

INSTRUCTOR'S HANDOUT "SUPPLEMENTAL": SOME IRRATIONAL NUMBERS

PETE L. CLARK

After I wrote up Handout 1 on the Fundamental Theorem of Arithmetic and its applications, I realized I had forgotten to include a very nice application: to irrationality proofs. I remembered this in time to lecture on it in class. Here are some notes based on my lectures. I could have changed the Handout 1 file by inserting these notes, but if you are printing out the notes it will be more useful to have a separate file.

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.

But now consider the equation

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

Thus $2|a^2$. It follows that $2|a$. Notice that this follows immediately from Euclid's Lemma – if $p|a^2$, $p|a$ or $p|a$. On the other hand, we can avoid EL by proving 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

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

so $2|b^2$ and reasoning as above, $2|b$. Thus 2 divides both a and b , but this is a contradiction.

Comment: This is a truly "classical" proof. In G.H. Hardy's seminal *A Mathematician's Apology* (apology being meant in the Socratic sense of *explanation*; he is not sorry to be a mathematician!), 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 proof is inevitably a proof by contradiction (unlike Euclid's proof, which really does construct a new prime for you in a perfectly explicit way). The original statement – that $\sqrt{2}$ is irrational – is logically more complicated than what we actually prove. Namely, 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 is the first instance of an "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.¹

Let us try to generalize this result: can we prove that $\sqrt{3}$ is irrational in the same way(s)? The proof with Euclid's Lemma certainly goes straight through to show that \sqrt{p} is irrational for any prime p : we 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 substituting we get $pb^2 = p^2A^2$, $b^2 = pA^2$, so $p|b^2$ and finally $p|b$, 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: $3|a^2 \implies 3|a$. 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. (There is more to notice from this calculation: taking a number which is either one more or one less than a multiple of 3 and squaring it, we get in both cases a number which is one more than a multiple of 3. Such observations will be of great importance to us later on.) 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 .

Another way to look at it is as a fact about arithmetic in the finite ring Z_p of integers modulo p : it is precisely the statement that 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. (The proof used, of course, Euclid's Lemma. We are just kicking the same idea around the mathematical landscape and watching different sides of it tumble into view.) Thus, although the full strength of $p|ab \implies p|a$ or $p|b$ holds *only* for primes, the special case $p|a^2 \implies p|a$ 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

¹Note that the above proof we gave is purely algebraic. It is therefore *not* the one the Greeks would have given. Mathematics related to this topic appear in several of Plato's dialogues: the Meno and the Theaetetus.

get one of these two limiting cases: namely, any n can be uniquely decomposed as

$$n = sN^2,$$

where s is squarefree. We leave this to the reader as an informal exercise. For instance, it works out nicely using the ord_p functions. 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 we have proven:

Theorem 3. *For any positive integer n , \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 very similar argument: suppose $\sqrt[3]{2} = \frac{a}{b}$, with a and b relatively prime. Then the usual algebra leads us to

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

and then $2|a^3 \implies 2|a$, and then $a = 3A$, so $2b^3 = 2^3A^3$, $b^3 = 2^2A^3$, so $2|b^3 \implies 2|b$, a contradiction, as before.

In fact, by decomposing an arbitrary integer into the product of a cube-free integer (i.e., an integer n with $\text{ord}_p(n) \leq 2$ for all primes p) and a perfect cube, one can prove that the cube root of n is irrational unless n is a perfect cube. For the sake of variety, we prove the general result in a different way, which makes more explicit use of the ord_p functions:

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

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

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

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 $k|\text{ord}_p(n)$, which is exactly what we assumed was not the case. Contradiction!

We remark that from a more advanced algebraic perspective, there is yet a further generalization to be made. Namely, recall that a complex number α is said to be an **algebraic number** if there exists a polynomial

$$P(X) = a_n X^n + \dots + a_1 X + a_0$$

with integer coefficients such that $P(\alpha) = 0$. It is said to be an **algebraic integer** if it satisfies such a polynomial P with $a_n = 1$ (a "monic polynomial"). For instance, $\frac{1}{2}$ is an algebraic number because it satisfies the polynomial $2X - 1$, and $\sqrt[5]{2}$ is an algebraic integer because it satisfied the polynomial $X^5 - 2$.

Theorem 5. *Suppose α is both a rational number and an algebraic integer. Then α is an integer.*

Proof: Suppose $\alpha = \frac{a}{b}$ (written in lowest terms, as usual!) satisfies a monic polynomial:

$$\left(\frac{a}{b}\right)^n + a_{n-1}\left(\frac{a}{b}\right)^{n-1} + \dots + a_1\left(\frac{a}{b}\right) + a_0 = 0.$$

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

$$a^n + ba_{n-1} \cdot a^{n-1} + \dots + b^{n-1}a_1 \cdot a + b^n a_0 = 0,$$

or

$$(1) \quad a^n = b(-a_{n-1} \cdot a^{n-1} - \dots - b^{n-2}a_1 \cdot a - b^{n-1}a_0).$$

If $b > 1$, there is some prime $p|b$, and then, since p divides the right-hand side of (1), it must divide the left-hand side, namely $p|a^n$, so by Euclid, $p|a$. But as usual this contradicts the fact that a and b were chosen to be relatively prime.

Remark: Unfortunately it was not clear from the definition whether $\frac{1}{2}$ is an algebraic integer: the polynomial $2X - 1$ is not monic, but maybe $\frac{1}{2}$ satisfies some *other* monic polynomial? Theorem 4 implies that the answer is negative: if so, it would be an ordinary integer, which it obviously isn't.

We can deduce Theorem 4 from Theorem 5 just by noticing that for any k and n , $\sqrt[k]{n}$ is a root of the monic polynomial $X^k - n$ so is an algebraic integer. On the other hand we know exactly when $\sqrt[k]{n}$ is an integer – quite tautologically, this is when n is a perfect k th power – so when n is not a perfect k th power it is an algebraic integer which is not an integer, so according to the theorem it cannot be a rational number.

Exercise: Prove the rational roots theorem from high school algebra: if

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

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

Final Remark: These irrationality proofs are also related to **Eisenstein's criterion** for irreducibility of an integer polynomial...