Solutions to In-Class Problems Week 1, Fri.

Problem 1.
Generalize the proof from lecture (reproduced below) that $\sqrt{2}$ is irrational, for example, how about $\sqrt[3]{2}$? Remember that an irrational number is a number that cannot be expressed as a ratio of two integers.

Theorem. *$\sqrt{2}$ is an irrational number.*

Proof. The proof is by contradiction: assume that $\sqrt{2}$ is rational, that is,

$$\sqrt{2} = \frac{n}{d}, \tag{1}$$

where n and d are integers. Now consider the smallest such positive integer denominator, d. We will prove in a moment that the numerator, n, and the denominator, d, are both even. This implies that

$$\frac{n/2}{d/2}$$

is a fraction equal to $\sqrt{2}$ with a smaller positive integer denominator, a contradiction.

Since the assumption that $\sqrt{2}$ is rational leads to this contradiction, the assumption must be false. That is, $\sqrt{2}$ is indeed irrational. This italicized comment on the implication of the contradiction normally goes without saying, but since this is the first 6.042 exercise about proof by contradiction, we've said it.

To prove that n and d have 2 as a common factor, we start by squaring both sides of (1) and get $2 = n^2/d^2$, so

$$2d^2 = n^2. \tag{2}$$

So 2 is a factor of n^2, which is only possible if 2 is in fact a factor of n.

This means that $n = 2k$ for some integer, k, so

$$n^2 = (2k)^2 = 4k^2. \tag{3}$$

Combining (2) and (3) gives $2d^2 = 4k^2$, so

$$d^2 = 2k^2. \tag{4}$$

So 2 is a factor of d^2, which again is only possible if 2 is in fact also a factor of d, as claimed. ■

Solution. *Proof.* We prove that for any $n > 1$, $\sqrt[n]{2}$ is irrational by contradiction.

Assume that $\sqrt[n]{2}$ is rational. Under this assumption, there exist integers a and b with $\sqrt[n]{2} = a/b$, where b is the smallest such positive integer denominator. Now we prove that a and b are both even, so that

$$\frac{a/2}{b/2}$$

is a fraction equal to $\sqrt[n]{2}$ with a smaller positive integer denominator, a contradiction.

$$\begin{aligned} \sqrt[n]{2} &= \frac{a}{b} \\ 2 &= \frac{a^n}{b^n} \\ 2b^n &= a^n. \end{aligned}$$

The lefthand side of the last equation is even, so a^n is even. This implies that a is even as well (see below for justification).

In particular, $a = 2c$ for some integer c. Thus,

$$\begin{aligned} 2b^n &= (2c)^n = 2^n c^n, \\ b^n &= 2^{n-1} c^n. \end{aligned}$$

Since $n - 1 > 0$, the righthand side of the last equation is an even number, so b^n is even. But this implies that b must be even as well, contradicting the fact that a/b is in lowest terms. ■

Now we justify the claim that if a^n is even, so is a.

There is a simple proof by contradiction: suppose to the contrary that a is odd. It's a familiar (and easily verified[1]) fact that the product of two odd numbers is odd, from which it follows that the product of *any* finite number of odd numbers is odd, so a^n would also be odd, contradicting the fact that a^n is even.

More generally for *any* integers $m, k > 0$, if m^k is divisible by a prime number, p, then m must be divisible by p. This follows from the factorization of an integer into primes (which we'll discuss further in a coming lecture): the primes in the factorization of m^k are precisely the primes in the factorization of m repeated k times, so if there is a p in the factorization of m^k it must be one of k copies of a p in the factorization of m. ■

Problem 2.
Here is a generalization of Problem 1 that you may not have thought of:

Lemma 2.1. *Let the coefficients of the polynomial $a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1} + x^m$ be integers. Then any real root of the polynomial is either integral or irrational.*

(a) Explain why Lemma (2.1) immediately implies that $\sqrt[m]{k}$ is irrational whenever k is not an mth power of some integer.

[1] Two odd integers can be written as $2x + 1$ and $2y + 1$ for some integers x and y. Then their product is also odd because it equals $2z + 1$ where $z = 2(2xy + x + y) + 1$.

Solution. Saying that an integer, k, is not the nth power of an integer, is equivalent to saying that the equation $x^M = k$ has no integer solutions. Another way to say this is that the polynomial $x^m - k$ has no integer root. Lemma (2.1) therefore implies that any root of $x^m - k$ is irrational. But $\sqrt[m]{k}$ is, by definition, a root of this polynomial, so it is irrational. ■

(b) Collaborate with your tablemates to write a clear, textbook quality proof of Lemma 2.1 on your whiteboard. (Besides clarity and correctness, textbook quality requires good English with proper punctuation. When a real textbook writer does this, it usually takes multiple revisions; if you're satisfied with your first draft, you're probably misjudging.) You may find it helpful to appeal to the following:

Lemma 2.2. *If a prime, p, is a factor of some power of an integer, then it is a factor of that integer.*

You may assume Lemma 2.2 without writing down its proof, but see if you can explain why it is true.

Solution. *Proof.* Let r be a real root of the polynomial, so that

$$a_0 + a_1 r + a_2 r^2 + \cdots + a_{m-1} r^{m-1} + r^m = 0.$$

There are three cases: either r is an integer, or r is irrational, or $r = s/t$ for integers s and t which have no common factors and such that $t > 1$. We want to eliminate the last case, so assume for the sake of contradiction that it held for some r.

Substituting s/t for r and multiplying both sides of the above equation by t^m yields:

$$a_0 t^m + a_1 s t^{m-1} + a_2 s^2 t^{m-2} + \cdots + a_{m-1} s^{m-1} t + s^m = 0, \tag{5}$$

$$a_0 t^m + a_1 s t^{m-1} + a_2 s^2 t^{m-2} + \cdots + s^{m-1} t = -s^m. \tag{6}$$

Now since $t > 1$, it must have a prime factor, p. The prime, p, therefore divides each term of the lefthand side of equation (6), so p also divides the righthand side, $-s^m$. This means that p divides s^m, so by Lemma 2.2, p is also a factor of s. So p is a common factor of s and t, contradicting the fact that s and t have no common factors. ■

Lemma 2.2 is a simple consequence of the *Fundamental Theorem of Arithmetic* which says that every integer > 1 factors into a product of primes that is *unique* except for the order in which the primes are multiplied.

For example, here are some ways to express 140 as a product of primes:

$$140 = 2 \cdot 2 \cdot 5 \cdot 7 = 2 \cdot 5 \cdot 7 \cdot 2 = 7 \cdot 5 \cdot 2 \cdot 2 = \cdots.$$

By the Fundamental Theorem, every such product will have exactly two occurrences of 2 and one each of 5 and 7. Next, we can obviously get a product of primes equal to, say, the third power of 140 by taking a product that equals 140 and repeating it three times. For example,

$$(140)^3 = 2 \cdot 2 \cdot 5 \cdot 7 \quad \cdot \quad 2 \cdot 2 \cdot 7 \cdot 5 \quad \cdot \quad 2 \cdot 2 \cdot 7 \cdot 5.$$

The Fundamental Theorem now says that *every* prime product equal to the third power of 60 must have the same primes as this repeated product, namely, six occurrences of 2 and three occurrences each of 5 and 7. In particular, the *only* primes that are factors of $(140)^3$ are the primes 2, 5 and 7 that are factors of 140. This reasoning applies equally well with any other integer greater than 1

in place of 140 and any power greater than 0 in place of 3, proving that if p is a prime factor of s^m, then p must have been a factor of s.

The Fundamental Theorem of Arithmetic is also know as the *Unique Prime Factorization Theorem*. It is one of those familiar mathematical facts that is not exactly obvious. We'll work out a proof of the Fundamental Theorem in a later chapter. ■

Problem 3.
If we raise an irrational number to an irrational power, can the result be rational? Show that it can by considering $\sqrt{2}^{\sqrt{2}}$ and arguing by cases.

Solution. We want to find irrational numbers a, b such that a^b is rational. We argue by cases.

Case 1: [$\sqrt{2}^{\sqrt{2}}$ is rational]. Let $a = b = \sqrt{2}$. a and b are irrational since $\sqrt{2}$ is irrational as we know. Also, a^b is rational by case hypothesis. So we have found the required a and b in this case.

Case 2: [$\sqrt{2}^{\sqrt{2}}$ is irrational]. Let $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$. Then a is irrational by case hypothesis, we know b is irrational, and

$$a^b = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^2 = 2,$$

which is rational. So we have found the required a and b in this case also.

So in any case, there will be irrational a, b such that a^b is rational. Note that we have no clue about which case is true, but that didn't matter.

■

Problem 4.
Here is a different proof that $\sqrt{2}$ is irrational, taken from the American Mathematical Monthly, v.116, #1, Jan. 2009, p.69:

Proof. Suppose for the sake of contradiction that $\sqrt{2}$ is rational, and choose the least integer, $q > 0$, such that $\left(\sqrt{2}-1\right)q$ is a nonnegative integer. Let $q' ::= \left(\sqrt{2}-1\right)q$. Clearly $0 < q' < q$. But an easy computation shows that $\left(\sqrt{2}-1\right)q'$ is a nonnegative integer, contradicting the minimality of q. ■

(a) This proof was written for an audience of college teachers, and is a little more concise than desirable at this point in 6.042. Write out a more complete version which includes an explanation of each step.

Solution. The points that need justification are:

1. Why is there a positive integer, q, such that $\left(\sqrt{2}-1\right)q$ is a nonnegative integer? *Answer:* Since $\sqrt{2}$ is rational, so is $\sqrt{2}-1$. So $\sqrt{2}-1$ can be expressed as an integer quotient with positive denominator; now just let q be that denominator.
2. Why is there such a *least* positive integer, q? *Answer:* As long as there is one such positive integer, there has to be a least one. This obvious fact is known as the *Well Ordering Principle*.

3. Why is $0 < q' < q$? *Answer:* We know that $1 < \sqrt{2} < 2$, so $0 < \sqrt{2} - 1 < 1$. Therefore, $0 < \left(\sqrt{2} - 1\right) r < r$ for any real number $r > 0$.
4. Why is $(\sqrt{2}-1)q'$ a nonnegative integer? *Answer:* It's actually positive, because it is a product of positive numbers. It's integer because

$$\left(\sqrt{2} - 1\right) q' = \left(\sqrt{2} - 1\right)^2 q = 2q - 2q\sqrt{2} + q = q - 2 \cdot \left[\left(\sqrt{2} - 1\right) q\right]$$

and the last term is of the form $\langle \text{integer} - 2 \cdot [\text{integer}] \rangle$.

■

(b) Now that you have justified the steps in this proof, do you have a preference for one of these proofs over the other? Why? Discuss these questions with your teammates for a few minutes and summarize your team's answers on your whiteboard.

Solution. Both proofs seem about equally easy to understand. The previous problems shows that the first proof generalizes pretty directly from square roots to kth roots, which doesn't seems as clear for the this second proof. On the other hand, the first proof requires appeal to Unique Prime Factorization, while the second just uses simple algebra. ■

6.042J / 18.062J Mathematics for Computer Science
Spring 2010