Math for CS 2015/2019 solutions to "In-Class Problems Week 1, Fri. (Session 2)"

https://github.com/spamegg1

October 18, 2022

Contents

1 Problem 1

Prove that if $a \cdot b = n$, then either a or b must be $\leq n$, where a, b, and n are nonnegative real numbers. Hint: by contradiction, Section 1.8 in the course textbook.

Proof. 1. Assume a, b, n are nonnegative real numbers, and $a \cdot b = n$.

2. Argue by contradiction. Assume $a > \sqrt{n}$ and $b > \sqrt{n}$.

3. Since all the numbers involved $a, b, n, \sqrt{n}$ are nonnegative, we can multiply the two inequalities in (2) to get: $a \cdot b > \sqrt{n} \cdot \sqrt{n}$.

4. Using (1) we can replace $a \cdot b$ with n, so (3) gives us: $n > n$, a contradiction.

5. Our assumption in (2) must be false, therefore either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$. □

2 Problem 2

Generalize the proof of Theorem 1.8.1 repeated below that $\sqrt{2}$ is irrational in the course textbook. For example, how about $\sqrt{3}$?

We want to prove:

Theorem 1. *$\sqrt{3}$ is an irrational number.*

First we will need another result:

Lemma 1. *Assume n is a positive integer. If 3 divides n^2, then 3 divides n.*

This is actually Problem 1.10 part (b) in the textbook! Prof. Meyer tells us to do it in the proof of $\sqrt{2}$ is irrational.

Proof. 1. Assume n is a positive integer and 3 divides n^2.

2. By definition of divisibility there exists an integer k such that $3k = n^2$ (we will need this later below).

3. Argue by contradiction and assume that 3 does not divide n.

4. By the Quotient-Remainder Theorem there exist integers q, r such that $n = 3q + r$ where $0 \leq r < 3$.

5. Since 3 does not divide n, r cannot be 0. So r must be 1 or 2.

6. **Case 1**. $r = 1$.

6.1. Then $n = 3q + 1$. So $n^2 = (3q + 1)^2 = 9q^2 + 6q + 1$.

6.2. So $3k = 9q^2 + 6q + 1$, dividing by 3 we get $k = 3q^2 + 2q + \frac{1}{3}$.

6.3. Moving terms, we get $k - 3q^2 - 2q = \frac{1}{3}$. This is a contradiction! Because the left-hand side $k - 3q^2 - 2q$ is an integer, but the right-hand side $\frac{1}{3}$ is not an integer.

7. **Case 2**. $r = 2$.

7.1. Then $n = 3q + 2$. So $n^2 = (3q + 2)^2 = 9q^2 + 12q + 4$.

7.2. So $3k = 9q^2 + 12q + 4$, dividing by 3 we get $k = 3q^2 + 4q + \frac{4}{3}$.

7.3. Moving terms, we get $k - 3q^2 - 4q = \frac{4}{3}$. This is a contradiction! Because the left-hand side $k - 3q^2 - 4q$ is an integer, but the right-hand side $\frac{4}{3}$ is not an integer.

8. The two cases in (6) and (7) are exhaustive of all possibilities, and in all cases we had a contradiction.

9. Therefore our assumption must have been false, so 3 divides n. □

Now we can begin the proof of the Theorem.

Proof. 1. Argue by contradiction and assume $\sqrt{3}$ is rational.

2. By the definition of a rational number, there exist integers n and d such that $\sqrt{3} = \frac{n}{d}$ where $d \neq 0$ and n and d have no common divisors greater than 1.

Without loss of generality, we may assume that both n and d are both positive, since $\sqrt{3}$ is positive.

3. Squaring both sides we get $3 = \frac{n^2}{d^2}$.

4. Multiplying both sides by d^2 we get $3d^2 = n^2$.

5. From this equation we notice that 3 divides n^2. (Because there exists an integer $k = d^2$ such that $n^2 = 3k$, which is the definition of divisibility).

6. By (5) and the Lemma, 3 divides n.

7. By (6) and the definition of divisibility, there exists an integer m such that $3m = n$.

8. Substituting (7) into (4) we get $3d^2 = (3m)^2 = 9m^2$.

9. Dividing by 3, we get $d^2 = 3m^2$. This means d is divisible by 3, which is a contradiction to the fact that n and d have no common divisors greater than 1.

10. Therefore our initial assumption was false, hence $\sqrt{3}$ is irrational. $\square$

2.1 Generalizing even further

This subsection is fairly hard and is optional.

How far can this Theorem be generalized? Is $\sqrt{4}$ irrational too? No, it's equal to 2. Where would the proof go wrong if we tried it on $\sqrt{4}$?

Let m vary over the positive integers, and consider the general statement: "$\sqrt{m}$ is irrational." Intuitively, it seems like this should be true as long as m itself is not a perfect square. If we go through the proof, we end up with a step where $md^2 = n^2$, and we notice m divides n^2. Then we would have to prove the Lemma, that is, if m divides n^2 then m divides n, and derive the contradiction similarly.

So, is it true that if m and n are positive integers, m **is not a perfect square**, and m divides n^2, then m divides n? Not quite. We can let $n = pq$ where p and q are two primes that are different from each other, and let $m = p^2q$. Then m divides $n^2 = p^2q^2$ but not $n = pq$. So we cannot use the same argument, with the same Lemma, to prove the Theorem for all m that are not perfect squares.

However, the Claim that if m divides n^2 then m divides n *should* hold true for all **prime** m. When $m = 3$ we had to consider two cases: where the remainder of dividing n by m was 1 or 2. In general there will be $m - 1$ cases! We cannot go through them one by one (we don't know how many there are, since we don't know the value of m), so we will have to "parametrize" all the cases and handle them in a generic way.

Lemma 2. *Assume m and n are positive integers and m is prime. If m divides n^2 then m divides n.*

Proof. 1. Assume m and n are positive integers, m is prime, and m divides n^2.

2. By definition of divisibility, there exists an integer k such that $mk = n^2$. (We notice that k must be positive.)

3. By the Quotient-Remainder theorem there exist integers q, r such that $n = qm + r$ where $0 \leq r < m$.

4. If $r = 0$ then $n = qm$ so m divides n, and we are done. So now consider the case $r > 0$.

5. Then $n^2 = (qm + r)^2 = q^2m^2 + 2qmr + r^2$.

6. By (2) and (4) we have $q^2m^2 + 2qmr + r^2 = mk$.

7. Dividing by m we get $q^2m + 2qr + \frac{r^2}{m} = k$.

8. Moving terms, we get $q^2m + 2qr - k = -\frac{r^2}{m}$.

9. Since m is prime and $0 < r < m$, r^2 is not divisible by m. **(We need to prove this!)**

10. So the LHS of (8) is an integer, while the RHS of (8) is not an integer (because $r \neq 0$), a contradiction.

11. Our initial assumption must have been false, therefore m divides n. □

Let's prove step (9). We have to use the Fundamental Theorem of Arithmetic and properties of prime numbers.

Claim 1. *Assume m is prime and $0 < r < m$ is an integer. Then m does not divide r^2.*

Proof. 1. Assume m is prime and $0 < r < m$ is an integer.

2. By the Fundamental Theorem of Arithmetic, there exist primes $p_1, \ldots, p_n$ and positive integers $a_1, \ldots, a_n$ such that

$$r = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_n^{a_n}$$

3. By (2), we have $p_i \leq r$ for all $i = 1, \ldots, n$.

4. Since $0 < r < m$, by (3) we have $p_i < m$ for all $i = 1, \ldots, n$.

5. Since m is prime, by (4) we have $m \nmid p_i$ for all $i = 1, \ldots, n$.

6. Since m is prime, by (5) m does not divide any product of the primes $p_1, \ldots, p_n$ either.

7. By (2) we have

$$r^2 = p_1^{2a_1} \cdot p_2^{2a_2} \cdot \ldots \cdot p_n^{2a_n}$$

so r^2 is a product of the primes $p_1, \ldots, p_n$.

8. By (7) and (6) m does not divide r^2. □

With Lemma 2, we are able to generalize the Theorem to square roots of any primes (just repeat the proof for $\sqrt{3}$ where m replaces 3, and use Lemma 2 in the place of Lemma 1):

Theorem 2. *Assume m is prime. Then $\sqrt{m}$ is irrational.*

Earlier we said that the theorem should hold not just for prime m, but any m that is not a perfect square itself. However proving this greater generalization would require more work.

3 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.

Proof. 1. **Case 1.** $\sqrt{2}^{\sqrt{2}}$ is rational.

1.1. We know that $\sqrt{2}$ is irrational (earlier Theorem from the lecture).

1.2. So in this case, an irrational, namely $\sqrt{2}$, raised to an irrational power, namely $\sqrt{2}$, gives us a rational number, namely $\sqrt{2}^{\sqrt{2}}$. Therefore we proved the claim in this case.

2. **Case 2.** $\sqrt{2}^{\sqrt{2}}$ is irrational.

2.1. By the law of exponents $(a^b)^c = a^{bc}$ we have:

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

2.2. So, in this case, once again we have an irrational, namely $\sqrt{2}^{\sqrt{2}}$, raised to an irrational power, namely $\sqrt{2}$, that results in a rational number, namely 2. So we proved the claim in this case too. □

4 Problem 4

The fact that that there are irrational numbers a, b such that a^b is rational was proved earlier by cases. Unfortunately, that proof was *nonconstructive*: it didn't reveal a specific pair, a, b with this property. But in fact, it's easy to do this: let $a ::= 2$ and $b ::= 2\log_2(3)$. We know a is irrational, and $a^b = 3$ by definition. Finish the proof that these values for a, b work by showing that $2\log_2(3)$ is irrational.

Proof. 1. Argue by contradiction and assume $2\log_2(3)$ is rational.

2. By the definition of a rational number, there exist integers n and d such that $2\log_2(3) = \frac{n}{d}$, where n and d have no common divisors greater than 1.

Without loss of generality we may assume $d > 0$.

3. Dividing both sides by 2, we get $\log_2(3) = \dfrac{n}{2d}$.

4. Using exponentiation with base 2 for both sides, we get $2^{\log_2(3)} = 2^{n/2d}$.

5. By the definition of $\log_2$, we get $3 = 2^{n/2d}$.

6. Raising both sides to the power $2d$ we get $3^{2d} = 2^n$.

7. Dividing, we get

$$\frac{3^{2d}}{2^n} = 1$$

8. Since 2 and 3 are different primes, 2^n cannot divide 3^{2d}, unless $n = 0$. So by (7) we have $n = 0$.

9. By (8) and (2) we have $2\log_2(3) = \frac{0}{d} = 0$ which is a contradiction. (Because for the $\log_2$ function, the only root is $x = 1$. So $\log_2(3) \neq 0$.)

10. Therefore $2\log_2(3)$ is irrational. $\square$