MOE H3 Math   Mathematical Proofs and Reasoning

Problem Set 2

1. Is each of the following statements true or false? Give a proof if it is true, and give a counter-example if it is false.

   (a) For each pair of real numbers x and y, if $x+y$ is irrational, then x is irrational and y is irrational.

   Solution: False.

   A counterexample is $x = \sqrt{2}$ and $y = 0$. Then $x + y = \sqrt{2}$ is irrational but not both x and y are irrational.

   (b) For each pair of real numbers x and y, if $x+y$ is irrational, then x is irrational or y is irrational.

   Solution: True.

   Prove by contrapositive: For every pair of real numbers x and y, if x is rational and y is rational, then $x+y$ is rational.

   This statement is true by closure property of rational numbers under addition.

   (Note that the closure property of rational number is a 'theorem' rather than an 'axiom'. It can be proven rather easily. Here you may assume it has been proven and use it without proving it again.)

   (c) For each pair of nonzero real numbers x and y, if x is rational and y is irrational, then xy is irrational.

   Solution: True. We will prove by contradiction.

   Write $x = \dfrac{a}{b}$ for some integers $a, b \in \mathbb{Z}$. Suppose xy is a rational number,

   $$xy = \frac{c}{d}$$

   for some integers $c, d \in \mathbb{Z}$. Then

   $$y = \frac{c}{d} \cdot x = \frac{c}{d} \cdot \frac{a}{b} = \frac{ac}{bd}$$

   is a rational number since $ac, bd \in \mathbb{Z}$. This means y is rational, contradicting the assumption that y is irrational.

   Therefore, our assumption is false, and xy must be irrational.

2. (Y2023 Q5)

   (a) Let p be a prime number greater than 2. Write down the possible remainders of p when divided by 4.

Solution: Possible remainders are 0, 1, 2, 3.

(b) Fermat's Little Theorem states that if p is prime and a is an integer which is not divisible by p, then $a^{p-1} \equiv 1$ (modulo p).
Use Fermat's Little Theorem to prove that if p is a prime number greater than 2, and there exists an integer z such that $z^2 \equiv -1$ (modulo p), then p is not congruent to 3 (modulo 4).

Solution: Use proof by contradiction. Suppose $p \equiv 3 \pmod 4$. This means that $p - 3 = 4k$ for some $k \in \mathbb{Z}$. Now If $z^2 \equiv -1 \pmod p$, then $p \nmid z$. So, by Fermat's little theorem, $z^{p-1} \equiv 1 \pmod p$. By assumption, $z^2 \equiv -1 \pmod p$ tells us that $z^4 \equiv 1 \pmod p$. Now

$$z^{p-3} = z^{4k} = (z^4)^k \equiv 1^k = 1 \pmod p.$$

Thus, by Fermat's little theorem

$$1 \equiv z^{p-1} = Z^{p-3}z^2 \equiv (1)(-1) = -1 \pmod p,$$

which is true only if $p = 2$, which is a contradiction. Hence, $p \not\equiv 3 \pmod 4$.

In fact, we know that since $p \neq 2$, $p \not\equiv 0, 2 \pmod 4$. That is, it must be the case that $p \equiv 1 \pmod 4$.

(c) Write down the possible remainders of w^2 when divided by 8 where w is an integer.

Solution: $1^2 \equiv 1 \pmod 8$, $2^2 \equiv 4 \pmod 8$, $3^2 \equiv 1 \pmod 8$, $4^2 \equiv 0 \mod 8$, $5^2 \equiv 1 \pmod 8$, $6^2 \equiv 4 \pmod 8$, $7^2 \equiv 1 \pmod 8$.

So, $w^2 \equiv 0, 1, 4 \pmod 8$.

3. Unique Factorization Theorem states that:
Every integer $n > 1$ has a unique standard factored form. i.e. there is exactly one way to express

$$n = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$$

where $p_1 < p_2 < \cdots < p_t$ are distinct primes and $k_1, k_2, \cdots, k_t$ are some positive integers.

Use the Unique Factorization Theorem to prove that, if a positive integer n is not a perfect square, then $\sqrt{n}$ is irrational.

Solution: Prove by contradiction.

Suppose n is not a perfect square and $\sqrt{n}$ is rational. Then $\sqrt{n} = \dfrac{a}{b}$ for some integers a, b. Squaring both sides and clearing denominator gives $nb^2 = a^2 - - - (*)$.

Consider the standard factored forms of n, a and b:

$$n = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$$

$$a = q_1^{e_1} q_2^{e_2} \cdots q_u^{e_u} \Rightarrow a^2 = q_1^{2e_1} q_2^{2e_2} \cdots q_u^{2e_u}$$
$$b = r_1^{f_1} r_2^{f_2} \cdots r_v^{f_v} \Rightarrow b^2 = r_1^{2f_1} r_2^{2f_2} \cdots r_v^{2f_v}$$

i.e. the powers of primes in the standard factored form of a^2 and b^2 are all even integers.

This means the powers k_i of primes p_i in the standard factored form of n are also even by Unique Factorization Theorem (UFT):

Note that all p_i appear in the standard factored form of a^2 with even power $2c_i$, because of $(*)$. By UFT, p_i must also appear in the standard factored form of nb^2 with the same even power $2c_i$.

If $p_i \nmid b$, then $k_i = 2c_i$ which is even. If $p_i \mid b$, then p_i will appear in b^2 with even power $2d_i$. So $k_i + 2d_i = 2c_i$, and hence $k_i = 2(c_i - d_i)$, which is again even.

Hence $n = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t} = \left(p_1^{k_1/2} p_2^{k_2/2} \cdots p_t^{k_t/2}\right)^2$.

Since $k_i/2$ are all integers, $p_1^{k_1/2} p_2^{k_2/2} \cdots p_t^{k_t/2}$ is an integer and n is a perfect square. This contradicts the given hypothesis that n is not a perfect square.

So we conclude that when a positive integer n is not a perfect square, then $\sqrt{n}$ is irrational.

4. Prove or disprove the statement

$$\text{If } a^2 \mid b^2, \text{ then } a \mid b \text{ for all integers } a, b.$$

Solution: Write $a = \prod_{i=1}^{n} p_i^{\alpha_i}$ and $b = \prod_{i=1}^{n} p_i^{\beta}$ be the prime factorization of a and b, where $p_i \neq p_j$ for $i \neq j$ (p_i are distinct), and $\alpha_i, \beta_i \geq 0$ for all $i = 1, ..., n$. Then since $a^2 \mid b^2$, it means that $2\alpha_i \leq 2\beta_i$ for all $i = 1, ..., n$. Hence, $\alpha_i \leq \beta_i$ for all $i = 1, ..., n$. Hence, $a \mid b$.

5. Determine whether each of the following real numbers is rational or irrational. Justify your answers.

(a) $\sqrt{3} + \sqrt{5}$;

Solution: $\sqrt{3} + \sqrt{5}$ is irrational.

Proof by contradiction.

Suppose $\sqrt{3} + \sqrt{5}$ is rational. Then we can write $\sqrt{3} + \sqrt{5} = \dfrac{m}{n}$ where $m, n \in \mathbb{Z}$. Squaring both sides gives

$$3 + 2\sqrt{3}\sqrt{5} + 5 = \frac{m^2}{n^2}.$$

This gives

$$\sqrt{15} = \frac{m^2}{2n^2} - 4 = \frac{2m^2 - n^2}{4n^2}$$

which implies $\sqrt{15}$ is a rational number.
However, since 15 is not a perfect square, $\sqrt{15}$ is an irrational number (by known result).

This gives a contradiction.

(b) $\sqrt{2} + \sqrt{8}$;

Solution: We can write $\sqrt{2} + \sqrt{8} = \sqrt{2}(1 + \sqrt{4}) = 3\sqrt{2}$.

Since 3 is a non-zero rational number, and $\sqrt{2}$ is irrational, the product $3\sqrt{2}$ is an irrational number.

(Here we use the known result that product of a non-zero rational number and an irrational number is irrational. This result itself can be proven using contradiction.)

(c) $\dfrac{1+\sqrt{2}}{1+\sqrt{3}}$.

Solution: $\dfrac{1+\sqrt{2}}{1+\sqrt{3}}$ is irrational. Proof by contradiction.

Suppose $\dfrac{1+\sqrt{2}}{1+\sqrt{3}}$ is rational. Then we can write $\dfrac{1+\sqrt{2}}{1+\sqrt{3}} = \dfrac{m}{n}$ where $m, n \in \mathbb{Z}$.

This can be rewritten as $n(1 + \sqrt{2}) = m(1 + \sqrt{3})$ and further as

$$n\sqrt{2} - m\sqrt{3} = m - n.$$

Squaring both sides gives

$$2n^2 - 2nm\sqrt{2}\sqrt{3} + 3m^2 = m^2 - 2mn + n^2.$$

This gives

$$\sqrt{6} = \frac{2m^2 + 2mn + n^2}{2nm}$$

which implies $\sqrt{6}$ is a rational number.
However, since 6 is not a perfect square, $\sqrt{6}$ is an irrational number (by known result).

This gives a contradiction.

6. Prove that there does not exists a smallest positive real number.

Solution: Suppose $r > 0$ is the smallest positive real number. Since $\dfrac{1}{2} \geq 0$, $\dfrac{r}{2} > 0$ too. Also,

$$r = \frac{r}{2} + \frac{r}{2} \implies \frac{r}{2} < r.$$

Thus $\dfrac{r}{2}$ is a positive real number that is strictly smaller than r, contradicting the minimality of r.

Therefore, no smallest positive real number exists.

7. Prove that each finite decimal may be written as an infinite decimal in two distinct ways:

$$a_0.a_1a_2\ldots a_{n-1}a_n \;=\; a_0.a_1a_2\ldots a_{n-1}a_n\widehat{0} \;=\; a_0.a_1a_2\ldots a_{n-1}(a_n-1)\widehat{9},$$

where $a_n > 0$ if $n > 0$. (Here $\widehat{0}$ means an infinite tail of 0's, and $\widehat{9}$ an infinite tail of 9's.)

Solution: Write

$$x = a_0.a_1a_2\ldots a_{n-1}a_n = \sum_{k=0}^{n} a_k\,10^{-k}.$$

Appending an infinite tail of zeros does not change the value: $a_0.a_1\ldots a_{n-1}a_n\widehat{0} = \sum_{k=0}^{n} a_k\,10^{-k} = x$.

For the $\widehat{9}$ representation (which requires $a_n \geq 1$ when $n > 0$), consider

$$a_0.a_1\ldots a_{n-1}(a_n-1)\widehat{9} = \sum_{k=0}^{n-1} a_k\,10^{-k} + (a_n-1)10^{-n} + \sum_{k=n+1}^{\infty} 9\cdot 10^{-k}.$$

The infinite tail sums to

$$\sum_{k=n+1}^{\infty} 9\cdot 10^{-k} = 9\cdot 10^{-(n+1)}\sum_{j=0}^{\infty} 10^{-j} = 9\cdot 10^{-(n+1)}\cdot\frac{1}{1-1/10} = 10^{-n}.$$

Hence the last two terms combine to $(a_n-1)10^{-n} + 10^{-n} = a_n10^{-n}$, giving the same value x. Thus both infinite decimals represent the original finite decimal.

8. Prove that each real number is represented by a unique infinite decimal unless it is representable by a finite decimal, in which case it is representable by precisely two infinite decimals as described in the previous problem.

Solution: Let two infinite decimals represent the same real number:

$$x = a_0.a_1a_2\ldots \qquad \text{and} \qquad x = b_0.b_1b_2\ldots$$

(so each $a_k, b_k \in \{0,1,\ldots,9\}$). Let $S_n = \sum_{k=0}^{n} a_k\,10^{-k}$ and $T_n = \sum_{k=0}^{n} b_k\,10^{-k}$. Then $x - S_n \in [0, 10^{-n})$ and $x - T_n \in [0, 10^{-n})$.

We prove by induction that $a_k = b_k$ for all k, unless one expansion ends in a tail $\widehat{9}$ and the other is the corresponding finite expansion.

Base $k = 0$: If $a_0 \neq b_0$, then $|S_0 - T_0| \geq 1$, contradicting $|x - S_0| < 1$ and $|x - T_0| < 1$ with the triangle inequality. Hence $a_0 = b_0$.

Inductive step: Assume $a_j = b_j$ for all $j < n$. If $a_n \neq b_n$, then

$$|S_n - T_n| = \left|(a_n - b_n)10^{-n}\right| \geq 10^{-n}.$$

But
$$|S_n - T_n| \le |x - S_n| + |x - T_n| < 10^{-n} + 10^{-n} = 2 \cdot 10^{-n}.$$
This only leaves two possibilities:

1) If $|S_n - T_n| > 10^{-n}$ we obtain a contradiction immediately.

2) If $|S_n - T_n| = 10^{-n}$, then necessarily $\{a_n, b_n\} = \{c, c-1\}$ for some c, and moreover the tails must satisfy
$$\sum_{k>n} a_k \, 10^{-k} + \sum_{k>n} b_k \, 10^{-k} = 10^{-n}.$$
This equality forces one tail to be all 9's and the other to be all 0's (indeed $\sum_{k>n} 9 \cdot 10^{-k} = 10^{-n}$). Thus one representation is finite (terminating with a 0-tail) and the other is obtained by decreasing the last nonzero digit by 1 and appending $\widehat{9}$, exactly as in the previous problem.

Therefore, unless the number has a finite decimal expansion (in which case it has exactly two infinite representations of the form described in the previous problem), the digits must agree at every place and the infinite decimal is unique.

9. Prove that if there are no nonzero integer solutions to the equation $x^n + y^n = z^n$, then there are no nonzero rational solutions.

Solution: We prove the contrapositive. Suppose there is a nonzero rational solution $(x, y, z) \in \mathbb{Q}^3$ to $x^n + y^n = z^n$.

Write
$$x = \frac{a}{b}, \qquad y = \frac{c}{d}, \qquad z = \frac{e}{f},$$
with integers a, b, c, d, e, f and $b, d, f \neq 0$. Then
$$\left(\frac{a}{b}\right)^n + \left(\frac{c}{d}\right)^n = \left(\frac{e}{f}\right)^n.$$

Multiplying both sides by $(bdf)^n$ gives
$$(adf)^n + (cbf)^n = (ebd)^n.$$

Set
$$A = adf, \qquad B = cbf, \qquad C = ebd,$$
which are all (nonzero) integers. Then
$$A^n + B^n = C^n,$$
exhibiting a nonzero integer solution, contradicting the hypothesis.

Hence no nonzero rational solution can exist.

Hints

1. *Hint for Question 2.* Do we have all conditions necessary to apply Fermat's Little Theorem? You may want to consider proof by contradiction or contrapositive.

2. *Hint for Question 3.* You may use the fact that n is a perfect square if and only if its standard factored form is $n = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$ where all the k_i's are even.

3. *Hint for Question 4.* Use prime factorization.

4. *Hint for Question 5.* May use the fact that if a positive integer n is not a perfect square, then $\sqrt{n}$ is irrational.

5. *Hint for Question 8.* Requires induction.