MOE H3 Math Mathematical Proofs and Reasoning

Problem Set 1

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

   (a) The set of prime numbers is closed under addition.

   Solution: False. Counter-example: $a = 3, b = 5$ but $a+b = 3+5 = 8$ which is not a prime.

   (b) The set of positive rational numbers is closed under division.

   Solution: True. Direct proof: Suppose a and b are positive rational numbers. Then there exists positive integers m, n, p, q such that $a = \frac{m}{n}$ and $b = \frac{p}{q}$.
   Then $a \div b = \frac{m}{n} \div \frac{p}{q} = \frac{mq}{np}$.
   Since mq and np are positive integers, so $a \div b$ is a positive rational number.
   Hence the set of positive rational numbers is closed under division.

2. Let a, b and c be nonzero integers. Use the definition of divisibility and write down a direct proof for each of the following statements. (Indicate every step clearly.)

   (a) If a divides b, then ac divides bc.

   Solution: Suppose $a \mid b$. (Starting with hypothesis)
   There exists an integer d such that $b = ad$. (Definition of divisibility)
   By multiplying c on both sides, we have $bc = (ad)c = d(ac)$. (Algebraic manipulation)
   This means $ac \mid bc$. (Definition of divisibility- conclusion)

   (b) If a divides b and b divides a, then $a = \pm b$.

   Solution: Suppose $a \mid b$ and $b \mid a$. (Starting with hypothesis)
   There exist integers c and d such that $b = ac$ and $a = bd$. (Definition of divisibility)
   So $b = ac = (bd)c = b(cd)$. Thus $cd = 1$. (Algebraic manipulation)
   This implies c, d are divisors of 1, (Definition of divisibility)
   and hence $c, d = \pm 1$ (by a proved theorem)
   This means $a = \pm b$. (Conclusion)

3. Show that 3 divides $n(n+1)(2n+1)$ for any integer n.

   Solution: We consider three cases:

   Case (i) $n = 3k$ for some integer k: so

   $$n(n+1)(2n+1) = 3k(n+1)(2n+1),$$

   which is divisible by 3.

Case (ii) $n = 3k + 1$ for some integer k: so

$$n(n+1)(2n+1) = n(n+1)(2[3k+1]+1) = n(n+1)(6k+3) = 3n(n+1)(2k+1),$$

which is divisible by 3.

Case (iii) $n = 3k + 2$ for some integer k: so

$$n(n+1)(2n+1) = n([3k+2]+1)(2n+1) = n(3k+3)(2n+1) = 3n(k+1)(2n+1),$$

which is divisible by 3.

We see that, for all the three cases, $n(n+1)(2n+1)$ is divisible by 3.

4. Prove that for all integers a, if the remainder is NOT 2 when a is divided by 4, then $4 \mid a^3 + 23a$.

Solution:

Since $a \neq 4k + 2$ for any integer k, we have three cases:

Case (i) $a = 4k$

$$a^3 + 23a = (4k)^3 + 23(4k) = 4[16k^3 + 23k]$$

which is divisible by 4.

Case (ii) $a = 4k + 1$

$$a^3 + 23a = (4k+1)^3 + 23(4k+1) = 4[16k^3 + 12k^2 + 26k + 6]$$

which is divisible by 4.

Case (iii) $a = 4k + 3$

$$a^3 + 23a = (4k+3)^3 + 23(4k+3) = 4[16k^3 + 36k^2 + 50k + 24]$$

which is divisible by 4.

We see that, for all three cases, $4 \mid a^3 + 23a$.

5. For any integer $n > 1$, let the standard factored form of n be given by

$$n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}.$$

Prove that n is a perfect square if and only if $k_1, k_2, \dots, k_r$ are all even integers.

Solution: ($\Leftarrow$) Suppose $k_1, k_2, \dots, k_r$ are all even integers. We can write $k_i = 2h_i$ for some integer h_i. Then $n = p_1^{2h_1} p_2^{2h_2} \dots p_r^{2h_r} = (p_1^{h_1} p_2^{h_2} \dots p_r^{h_r})^2$.

Let $m = p_1^{h_1} p_2^{h_2} \dots p_r^{h_r}$, which is an integer. So we have $n = m^2$, which is a perfect square.

($\Rightarrow$) Suppose n is a perfect square. We can write $n = m^2$ for some integer m. Since $n > 1$, we have $m > 1$, and since m is a divisor of n, it has a standard factored form

$$m = p_1^{h_1} p_2^{h_2} \dots p_r^{h_r} \quad \text{where} \quad 0 \le h_i \le k_i.$$

Then $n = (p_1^{h_1} p_2^{h_2} \dots p_r^{h_r})^2 = p_1^{2h_1} p_2^{2h_2} \dots p_r^{2h_r}$. By comparing with the standard factored form of n and the uniqueness of prime factorization, the prime power $k_i = 2h_i$ for all i. In other words, k_i are all even.

6. Prove the following bi-conditional statement:
For all integers a and b, $3 \mid ab$ if and only if $3 \mid a$ or $3 \mid b$.

Solution: ($\Leftarrow$) We are supposed to prove two cases: (i) If $3 \mid a$ then $3 \mid ab$; and (ii) If $3 \mid b$ then $3 \mid ab$. Without loss of generality, we just need to prove one case. (Notice by interchanging a and b, it will not change the statement.) So suppose $3 \mid a$. Then $a = 3k$ for some integer k. Then $ab = 3kb$ would imply $3 \mid ab$. This proved the 'If' part.

($\Rightarrow$) We prove this by contrapositive. Suppose $3 \nmid a$ and $3 \nmid b$, then $3 \nmid ab$. From the hypothesis, we have the following four cases:

Case (i) $a = 3k + 1$ and $b = 3h + 1$. Then

$$ab = (3k + 1)(3h + 1) = 9kh + 3(k + h) + 1 = 3(3kh + k + h) + 1.$$

The RHS has a remainder 1 when divided by 3. So $3 \nmid ab$.

Case (ii) $a = 3k + 2$ and $b = 3h + 1$. Then

$$ab = (3k + 2)(3h + 1) = 9kh + 3k + 6h + 2 = 3(3kh + k + 2h) + 2/$$

The RHS has a remainder 2 when divided by 3. So $3 \nmid ab$.

Case (iii) $a = 3k + 1$ and $b = 3h + 2$. Then

$$ab = (3k + 1)(3h + 2) = 9kh + 6k + 3h + 2 = 3(3kh + 2k + h) + 2/$$

The RHS has a remainder 2 when divided by 3. So $3 \nmid ab$.

Case (iv) $a = 3k + 2$ and $b = 3h + 2$. Then

$$ab = (3k + 2)(3h + 2) = 9kh + 6(k + h) + 4 = 3(3kh + 2k + 2h + 1) + 1.$$

The RHS has a remainder 1 when divided by 3. So $3 \nmid ab$.

In all cases, we have $3 \nmid ab$.

7. Is the following statement true?
If $\dfrac{n(n+1)}{2}$ is odd, then so is $\dfrac{(n+1)(n+2)}{2}$.

Solution: False. Consider $n = 6$. Then $\frac{6(6+1)}{2} = 21$ is odd, but $\frac{(6+1)(6+2)}{2} = 28$ is even.

8. Let a, j, r, s be fixed integers. Prove: if j divides $r + s$, then

$$\exists\, b \in \mathbb{Z}\ (a = bj + r) \iff \exists\, c \in \mathbb{Z}\ (a = cj - s).$$

Solution: Since $j \mid r + s$, there is an integer $k \in \mathbb{Z}$ such that $kj = r + s$.

($\Rightarrow$) Suppose $a = bj + r$ for some $b \in \mathbb{Z}$. Using $r = jk - s$,

$$a = bj + r = bj + (jk - s) = (b + j)j - s.$$

Let $c = b + j \in \mathbb{Z}$. Then $a = cj - s$.

($\Leftarrow$) Suppose $a = cj - s$ for some $c \in \mathbb{Z}$. Using $s = kj - r$ again,

$$a = cj - s = cj - (kj - r) = (c - k)j + r.$$

Let $b = c - k \in \mathbb{Z}$. Then $a = bj + r$.

9. Prove that, if $3 \nmid a$, then $3 \mid a^2 + 5$.

Solution: Since $3 \nmid a$, so its remainder is either 1 or 2 when divided by 3.

Consider two cases: (i) $a = 3k + 1$; and (ii) $a = 3k + 2$.

Case (i): If $a = 3k + 1$, then $a^2 + 5 = (3k + 1)^2 + 5 = 9k^2 + 6k + 6 = 3(3k^2 + 2k + 2)$.

Since $3k^2 + 2k + 2$ is an integer, we have $3 \mid a^2 + 5$.

Case (ii): If $a = 3k + 2$, then $a^2 + 5 = (3k + 2)^2 + 5 = 9k^2 + 12k + 9 = 3(3k^2 + 4k + 3)$.

Since $3k^2 + 4k + 3$ is an integer, we have $3 \mid a^2 + 5$.

Combining both cases, we conclude that, if $3 \nmid a$, then $3 \mid a^2 + 5$.

10. Prove the following statement:
If m and n are any two integers with the same parity, then $4 \mid m^2 - n^2$.

Solution: Consider two cases: (i) m, n both even; and (ii) m, n both odd.

Case (i): If m, n are even, then $m = 2h$ and $n = 2k$ for some integers h, k.
Then $m^2 - n^2 = (2h)^2 - (2k)^2 = 4(h^2 - k^2)$.

Since $h^2 - k^2$ is an integer, we have $4 \mid m^2 - n^2$.

Case (ii): If m, n are odd, then $m = 2h + 1$ and $n = 2k + 1$ for some integers h, k.
Then $m^2 - n^2 = (2h + 1)^2 - (2k + 1)^2 = 4(h^2 + h - k^2 - k)$.

Since $h^2 + h - k^2 - k$ is an integer, we have $4 \mid m^2 - n^2$.

Conclusion: In both cases, we have $4 \mid m^2 - n^2$.

Hints

1. *Hint for Question 3.* Consider cases: $n = 3k + r$, $r = 0, 1, 2$.
2. *Hint for Question 4.* Consider cases: $a = 4k + r$, $r = 0, 1, 3$.
3. *Hint for Question 5.* For the "only if" part, may use the uniqueness of prime factorization.
4. *Hint for Question 6.* For the "only if" part, consider prove by contrapositive.
5. *Hint for Question 9.* Consider cases for a.