MH1812 Tutorial
Chapter 1: Elementary Number Theory

Q1: Show that 2 is the only prime number which is even.

Solution: Take p a prime number. Then p has only 2 divisors, 1 and p. If p is even, then one of its divisors has to be 2, thus $p = 2$. $\square$

Q2: Show that if n^2 is even, than n is even, for n an integer.

Solution: An integer n is either even or odd, i.e., with the form $2k$ or $2k+1$, for some integer k. When $n = 2k+1$, $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, which is odd. While $n = 2k$, $n^2 = 4k^2$. The case where n^2 is even is thus when $n = 2k$. $\square$

Q3: The goal of this exercise is to show that $\sqrt{2}$ is irrational. We provide a step by step way of doing so.

1. Suppose by contradiction that $\sqrt{2}$ is rational, that is $\sqrt{2} = \frac{m}{n}$, for m and n integers with no common factor. Show that m has to be even.

   Solution: Since $\sqrt{2} = \frac{m}{n}$, hence $m^2 = 2n^2$, which is even. According to the conclusion of Q2, m must be even. $\square$

2. Compute m^2, and deduce that n has to be even too, a contradiction.

   Solution: Assume $m = 2k$ for some integer k, then $m^2 = 4k^2 = 2n^2$, hence $n^2 = 2k^2$, so n is even due to the conclusion from Q2. This contradicts the assumption that m and n have no common divisor because 2 divides both. $\square$

Q4: Show the following two properties of the integers modulo n:

1. $(a \bmod n) + (b \bmod n) \equiv (a+b) \bmod n$.

   Solution: Suppose $(a \bmod n) = a'$, that is $a = qn + a'$, and $(b \bmod n) = b'$, that is $b = rn + b'$, for some integer q, r. Then

   $$(a \bmod n) + (b \bmod n) = a' + b'$$

   and

   $$(a+b) = (qn + a' + rn + b') \equiv (a' + b') \bmod n.$$

   The result follows by combining the two equations. $\square$

2. $(a \bmod n) \cdot (b \bmod n) \equiv (a \cdot b) \bmod n$.

Solution: Suppose $(a \bmod n) = a'$, that is $a = qn + a'$, and $(b \bmod n) = b'$, that is $b = rn + b'$, for some integer q, r. Then

$$(a \bmod n) \cdot (b \bmod n) = a' \cdot b'$$

and

$$(a \cdot b) = (qn + a') \cdot (rn + b') = qrn^2 + qnb' + rna' + a'b' \equiv (a'b') \bmod n.$$

The result follows by combining the two equations. □

Q5: Compute the addition table and the multiplication tables for integers modulo 4.

Solution: We represent integers modulo 4 by the set of integers $\{0, 1, 2, 3\}$. Then

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Similarly

*	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

□

Q6: Show that $\frac{p(p+1)}{2} \equiv 0 \pmod p$ for p an odd prime.

Solution: When p is an odd prime, it can be written in the form of $2k+1$ for some positive integer k. Hence $\frac{p(p+1)}{2} = \frac{p(2k+2)}{2} = p(k+1)$ a multiple of p, the conclusion follows. □

Q7: Consider the following sets S, with respective operator Δ.

1. Let S be the set of rational numbers R, and Δ be the multiplication. Is S closed under Δ? Justify your answer.

Solution: Take two rational numbers m/n and m'/n', Then

$$\frac{m}{n} \cdot \frac{m'}{n'} = \frac{mm'}{nn'}$$

which is a rational number. Thus the answer is Yes. □

2. Let S be the set of natural numbers N, and Δ be the subtraction. Is S closed under Δ? Justify your answer.

   Solution: The subtraction of two natural numbers does not always given a number natural, for example
   $$5 - 10 = -5$$
   and -5 is not natural, hence S is not closed under subtraction. $\square$

3. Let S be the set of irrational numbers I, and Δ be the addition. Is S closed under Δ? Justify your answer.

   Solution: The addition of two irrational numbers does not always give an irrational number, for example
   $$\pi + (-\pi) = 0$$
   and 0 is not irrational number. Thus S is not closed under addition. Note we know π is irrational, and we are using the fact that $-\pi$ is irrational too. Indeed, if $-\pi$ was rational, then it can be represented as $\frac{m}{n}$, then $\pi = \frac{-m}{n}$ which is rational too, contradicting the fact that π is irrational. $\square$