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. $(a \bmod n) + (b \bmod n) \equiv a + b \pmod{n}$.

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

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

   and

   $$a + b \equiv (qn + a' + rn + b') \equiv a' + b' \pmod{n}.$$

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

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

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

$$a \cdot b \equiv (qn + a') \cdot (rn + b') \equiv qrn^2 + qnb' + rna' + a'b' \equiv a'b' \pmod{n}.$$

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

×	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: Find the last digit of 7^{9999}.

Solution: The question asks us to find $7^{9999} \bmod 10$. Observe that $7^4 \bmod 10 = 1$ and $9999 \bmod 4 = 3$, the answer to the problem is

$$7^3 \bmod 10 = 343 \bmod 10 = 3.$$

□

Q8: Find the last digit of 8^{9999}.

Solution: There are many different simple ways to do this. The following are just two examples.

[Solution 1:] The question asks us to find $8^{9999} \bmod 10 = 2^{9999 \cdot 3} \bmod 10$. Observe that $2^5 \bmod 10 = 2$, hence if $m = 5q + r$, then $2^m \equiv 2^{q+r} \pmod{10}$. Applying this rule repeatedly, we see that

$$\begin{aligned}
2^{9999\cdot 3} \bmod 10 &= 2^{29997} \bmod 10\\
&= 2^{5999+2} \bmod 10 = 2^{6001} \bmod 10\\
&= 2^{1200+1} \bmod 10 = 2^{1201} \bmod 10\\
&= 2^{240+1} \bmod 10 = 2^{241} \bmod 10\\
&= 2^{48+1} \bmod 10 = 2^{49} \bmod 10\\
&= 2^{9+4} \bmod 10 = 2^{13} \bmod 10\\
&= 2^{2+3} \bmod 10 = 2^{5} \bmod 10\\
&= 2.
\end{aligned}$$

[Solution 2:] Observe that (i) 8^n is an even integer for any integer $n > 0$ and so is $8^n \bmod 10$; (ii) $6k \bmod 10 = k$ for $k = 0, 2, 4, 6, 8$; (iii) $8^4 \bmod 10 = 6$; (iv) $6^2 \bmod 10 = 6$ and thus $6^n \bmod 10 = 6$ for all $n \geq 2$. Therefore

$$8^{9999} \bmod 10 = (8^4)^m 8^3 \bmod 10 = 6^m 8^3 \bmod 10 = 6 \cdot 8^3 \bmod 10 = 8^3 \bmod 10 = 2,$$

where m is an integer such that $9999 = 4m + 3$. $\square$

Q9: Consider the following sets S, with respective operator Δ.

1. Let S be the set of odd integers and Δ be the multiplication. Is S closed under Δ? Justify your answer.

   Solution: Take two odd integers $2p+1$ and $2q+1$, where p and q are integers. Then

   $$(2p+1)(2q+1) = 2(2pq + p + q) + 1$$

   which is an odd number. Thus the answer is Yes. $\square$

2. Let S be the set of nonzero rational numbers $\mathbb{Q} \setminus \{0\}$ and Δ be the division. Is S closed under Δ? Justify your answer.

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

   $$\frac{m}{n}\Big/\frac{m'}{n'} = \frac{mn'}{nm'}$$

   which is a rational number. Thus the answer is Yes. $\square$

3. Let S be the set of positive integers $\mathbb{Z}^+$ and Δ be the subtraction. Is S closed under Δ? Justify your answer.

   Solution: The subtraction of two natural numbers does not always give a natural number, for example

   $$5 - 10 = -5$$

   and -5 is not natural, hence S is not closed under subtraction. $\square$

4. Let S be the set of irrational numbers 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

$$\sqrt{2} + (-\sqrt{2}) = 0$$

and 0 is not irrational. Thus S is not closed under addition. Note we know $\sqrt{2}$ is irrational (see Q3), and we are using the fact that $-\sqrt{2}$ is irrational too. Indeed, if $-\sqrt{2}$ were rational, then it could be represented as $\frac{m}{n}$, then $\sqrt{2} = \frac{-m}{n}$ which would be rational too, contradicting the fact that $\sqrt{2}$ is irrational. $\square$