Chapter 11

Solutions to the Exercises

> *"Intuition comes from experience, experience from failure, and failure from trying."*

Exercises for Chapter 1

Exercise 1. 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 also even, then one of its divisors has to be 2, thus $p = 2$.

Exercise 2. Show that if n^2 is even, then n is even, for n an integer.

Solution. An integer n is either even, that is $n = 2n'$, for some integer n', or odd, that is $n = 2n' + 1$ for some integer n'. Thus n^2 is either $4(n')^2$ or $4(n')^2 + 4n' + 1$. The case where n^2 is even is thus when $n = 2n'$.

Exercise 3. 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, that is $m = 2k$.

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

Solution. 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. Then

$$2 = \frac{m^2}{n^2}$$

and thus $m^2 = 2n^2$, showing that m^2 is even, that is, using Exercise 2, m has to be even, say $m = 2k$ for k some integer.

2. Now $m^2 = (2k)^2 = 4k^2$. This tells us, combining with the first step of the exercise, that

$$m^2 = 4k^2 = 2n^2$$

which implies that $2k^2 = n^2$, that is n^2 is even and by again by Exercise 2, it must be that n is even. This is a contradiction, since we assumed that m and n have no commun factor.

Exercise 4. Let n be an integer greater than 1. Suppose that $a \equiv a' \mod n$ and $b \equiv b' \mod n$. Show that

1. $(a + b) \mod n \equiv (a' + b') \mod n$,
2. $(a \cdot b) \mod n \equiv (a' \cdot b') \mod n$.

Solution. Before solving this exercise, let us discuss its meaning. We know that $(a \mod n) + (b \mod n) \equiv (a + b) \mod n$, this is how addition mod n is defined. What this exercise shows is that if you take $a' \equiv a \mod n$ and $b' \equiv b \mod n$, summing them up gives the same result as summing $a \mod n$ and $b \mod n$ (the same principle is shown for multiplication).

1. Since $a \equiv a' \mod n$, then $a = qn + a'$, and since $b \equiv b' \mod n$, then similarly $b = rn + b'$, for some integers q, r. Then

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

2. Similarly

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

Exercise 5. 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

Note that these tables are great to observe the closure property! Elements computed in these tables are the same as those given as input.

Exercise 6. Show that $\frac{m(m+1)}{2} \equiv 0 \pmod{m}$ for m an odd number.

Solution. Suppose that m is an odd number. Then $m+1$ is even, thus divisible by 2, say $m+1 = 2k$ for some k. Now

$$\frac{m(m+1)}{2} = mk \equiv 0 \pmod{m}.$$

You may also observe that it is not always true for even numbers. If for example $m = 2$, this does not work, indeed $2 \cdot 3/2 = 3$ which is not 0 mod 2.

Exercise 7.

1. Compute $7 \cdot 8 \cdot 9 \cdot 10$ modulo 3.
2. Show that $n^3 - n$ is always divisible by 3, for n any positive integer.

Solution.

1. Since 3 divides 9, the result modulo 3 is 0.
2. We note that $n^3 - n = n(n^2 - 1) = n(n-1)(n+1)$. Now any positive integer n is either a multiple of 3, say $n = 3k$, or when divided by 3 there is a remainder of 1, say $n = 3k+1$, or a remainder of 2, $n = 3k+2$. If $n = 3k$, $n^3 - n = 3k(n-1)(n+1)$ is divisible by 3, if $n = 3k + 1$

then $n^3 - n = n(3k)(n+1)$ is divisible by 3 and if $n = 3k+2$, then $n^3 - n = n(n-1)(3k+3)$ is divisible by 3.

This can be rewritten by considering integers modulo 3, this is the same idea. To show that 3 divides $n^3 - n$ is the same thing has $n^3 - n \equiv 0 \pmod 3$. Then once one has the idea to look at integers modulo 3, write n as $3k$, $3k+1$, or $3k+2$, and compute $n^3 - n$ for each case, for example $(3k)^3 - (3k)$ is clearly divisible by 3, the same computation can be done to show that $n^3 - n$ is a multiple of 3 for $3k+1$ and $3k+2$.

Exercise 8. Compute 40^{1234} modulo 2.

Solution. We have that $40^{1234} \equiv 0$ modulo 2 because $40 = 2 \cdot 20 \equiv 0$ modulo 2.

Exercise 9. Consider the set S of odd natural numbers, with respective operator Δ.

- Let Δ be the multiplication. Is S closed under Δ? Justify your answer.
- Let Δ be the addition. Is S closed under Δ? Justify your answer.

Solution.

- The S of odd integer numbers is closed under multiplication. To see that, notice that an odd integer number is of the form $2a+1$ for a some integer number. Then $(2a+1)(2b+1) = 4ab + 2a + 2b + 1 = 2(2ab + a + b) + 1$ which is again an odd integer number.
- The S of odd integer numbers is not closed under addition. To see that, notice that an odd integer number is of the form $2a+1$ for a some integer number. Then $(2a+1) + (2b+1) = 2a + 2b + 2 = 2(a+b+1)$ which is even number. Alternatively, one example can do. For example, take 3 and 5, they are both odd, 3+5 is 8 which is even, thus S is not closed under addition.

Exercise 10. Consider the following sets S, with respective operator Δ.

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

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

Solution. • Take two rational numbers $\frac{m}{n}$ and $\frac{m'}{n'}$. Then

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

which is a rational number. Thus the answer is yes, S is closed under multiplication.

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

$$5 - 10 = -5.$$

Thus S is not closed under subtraction.

- The addition of two irrational numbers does not always give an irrational number, for example,

$$(2 + \sqrt{2}) + (2 - \sqrt{2})) = 4$$

and 4 is not an irrational number. Thus S is not closed under addition. Note that we are using here the claim that $2+\sqrt{2}$ is irrational. Indeed, suppose that $2 + \sqrt{2}$ were rational, that is $2 + \sqrt{2} = \frac{m}{n}$ for m, n some integers. Then

$$\sqrt{2} = \frac{m}{n} - 2 = \frac{m - 2n}{n}$$

which is a contradiction to the fact that $\sqrt{2}$ is irrational.

Exercises for Chapter 2

Exercise 11. Decide whether the following statements are propositions. Justify your answer.

1. $2 + 2 = 5$.
2. $2 + 2 = 4$.
3. $x = 3$.
4. Every week has a Sunday.