Group Theory – Introductory Exercises

In these exercises we will look at modular arithmetic.

You may also find it useful to refresh your GCSE set theory knowledge.

1. Introduction

We begin with a (fairly obvious) lemma.

Euclid's Division Lemma

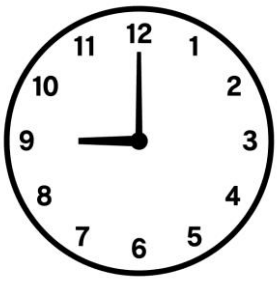
For every two positive integers a and b, $a \geq b$, there exists two unique integers q and r with $0 \leq r < b$, such that

$$a = qb + r$$

In short, this says we can divide any number by another and find a remainder.
For example, for $a = 7$, $b = 3$ we have

$$a = 2b + 1$$

Sometimes, we are only interested in the value of this remainder r.
Think of a 12 hour clock.



When it gets to "13 o'clock", the time on the clock returns to 1 o'clock.
If we hit the 25th hour, we would also return to 1 o'clock.

In this case, we are interested in the remainder r when dividing by $b = 12$.

$$13 = 1 \times 12 + \mathbf{1}$$
$$25 = 1 \times 12 + \mathbf{1}$$

This is a *modular* system and in the above example we are working in modulo 12.

We say that two numbers are *congruent modulo m* if they have the same remainder when dividing by m.

In the above example 13 and 25 are congruent modulo 12. We write this:

$$13 \equiv 25 \pmod{12}$$

If two numbers are congruent modulo m then their difference is divisible by m.
In the above example $25 - 13 = 12$ and this is clearly divisible by 12.

Definition

Let m be a positive integer. If a and b are integers, then we say a is congruent to b modulo m and write $a \equiv b \pmod{m}$ if m divides $(a - b)$.

Every number must be congruent to a number in the set $\{0, 1, \dots, m - 1\}$.
In this case, 13 and 25 are congruent to 1:

$$13 \equiv 1 \pmod{12}$$
$$25 \equiv 1 \pmod{12}$$

For simplicity, we are often only interested in these small values $< m$. Whilst it is true that $25 \equiv 13 \pmod{12}$, it is more useful to know that they are both congruent to 1 modulo 12.

We call the set of numbers congruent to a value $k < m$ a *congruence class*.

Example 1

Examples can help this make sense. Let's think about numbers modulo 3.

$$1 = 0 \times 3 + \mathbf{1}$$

So the remainder of 1 divided by 3 is 1, and we say 1 mod 3 is 1, or $1 \equiv 1 \pmod{3}$.

Similarly, it is easy to see that 2 mod 3 is 2.

$$3 = 1 \times 3 + \mathbf{0}$$

So $3 \equiv 0 \pmod{3}$. In fact, any multiple of 3 will have a zero remainder when divided by 3, and thus will be equal to 0 modulo 3.

Lets look at the next few numbers:

$$4 = 1 \times 3 + \mathbf{1}$$
$$5 = 1 \times 3 + \mathbf{2}$$
$$6 = 2 \times 3 + \mathbf{0}$$
$$7 = 2 \times 3 + \mathbf{1}$$
$$8 = 2 \times 3 + \mathbf{2}$$
$$9 = 3 \times 3 + \mathbf{0}$$

Each of the numbers is congruent to one of the numbers in the set {0,1,2}.

0 is always congruent to 0 modulo m for any m, and that is true for 3: $0 = 0 \times 3 + 0$.

Our congruence classes, therefore, would be:

$$[0] = \{0, 3, 6, \dots\}$$
$$[1] = \{1, 4, 7, \dots\}$$
$$[2] = \{2, 5, 8, \dots\}$$

Example 2

There are also some values of m which are easier to work with than others. Think about the number 10, for example.

What is 56 modulo 10? Well, $56 = 5 \times 10 + 6$, so $56 \equiv 6 \pmod{10}$.
What about 47? $47 = 4 \times 10 + 7$, so $47 \equiv 7 \pmod{10}$.
And 22? $22 = 2 \times 10 + 2$, so $22 \equiv 2 \pmod{10}$.

There is an obvious pattern here. Any number modulo 10 is just the digits value of the number.

Exercises

a) What is 7 modulo 4?
b) What is 93 modulo 8?
c) What is 41 modulo 6?
d) Write down the congruence classes for modulo 4 (like in Example 1).

---

2. Addition and Subtraction

We can add and subtract in a modular system.

Suppose we are looking at integers mod 5, and let's do $47 + 21 \pmod{5}$.
$47 + 21 = 68$ and $68 = 13 \times 5 + 3$, so 68 is congruent to 3 modulo 5.

However, we can do this another way.
$47 = 9 \times 5 + 2$, so $47 \equiv 2 \pmod{5}$.
$21 = 4 \times 5 + 1$, so $21 \equiv 1 \pmod{5}$.
Then we can just do $2 + 1 \pmod{5}$ and get the same answer, 3.

If we want to subtract we can use a similar method.

$47 - 21 = 26$, and $26 = 5 \times 5 + 1$, so $47 - 21 = 26 \equiv 1 \pmod{5}$.

Using the fact that $47 \equiv 2 \pmod{5}$ and $21 \equiv 1 \pmod{5}$ we could also find

$$2 - 1 = 1 \pmod{5}.$$

When working modulo n, adding by k is the same as subtracting by $n - k$, and vice versa.

Think again of our clock. If you move forward 1 hour you will be in the same place as if you moved back 11 hours, which is just $12 - 1$ hours.

We can also find modular values for negative numbers. In the above example, -11 is congruent to 1 modulo 12. We can also see this because $-11 = -1 \times 12 + 1$.

Exercises

a) What is $10 + 7$ modulo 4?
b) What is $82 - 17$ modulo 5?
c) It is currently 9 o'clock. What time will it be in 100 hours?

---

3. Multiplication

The last thing we will look at is multiplying numbers modulo m.

Multiplying numbers in a modular system is similar to adding and subtracting.

Say we have 15×12 and want to find the answer modulo 11.
$15 \times 12 = 180$, and $180 = 16 \times 11 + 4$, so the answer is $15 \times 12 = 180 \equiv 4 \bmod 11$.

Already this was quite difficult, and would only be more difficult for larger numbers. Instead lets try the same technique as before.

$15 = 1 \times 11 + 4$, and so $15 \equiv 4 \pmod{11}$.
$12 = 1 \times 11 + 1$, and so $11 \equiv 1 \pmod{11}$.

Then we can say that $15 \times 12 \equiv 4 \times 1 \equiv 4 \pmod{11}$, and this is much easier!

Example

What is 1837429×736523 modulo 10?

It would be very difficult to do this multiplication by hand, but we can see very quickly that $1837429 \equiv 9 \pmod{10}$ and $736523 \equiv 3 \pmod{10}$.

Instead we can do $9 \times 3 = 27$, and see that this is congruent to 7 modulo 10.

Therefore $1837429 \times 736523 \equiv 7 \pmod{10}$.

Exercises

a) What is 8×5 modulo 3?
b) What is 87×143 modulo 5?
c) What is 23×101 modulo 7?
d) Check your answers on a calculator.