Queen Mary University of London

MTH4104 **Introduction to Algebra**

Week 3 tutorial questions **w/c 7 February 2022**

This sheet contains questions for you to work through in your tutorial, singly or in a group.

It's important to work through lots of questions for practice. Remember that mathematics is not a spectator sport! If you want more questions, look at the "Extra questions" sheets on QMPlus.

Question 1 Write out addition and multiplication tables for $\mathbb{Z}_5$, like the ones for $\mathbb{Z}_4$ in the lecture notes.

That is, let $S := \{0,1,2,3,4\}$. For each pair of elements $a,b \in S$, your tables should give the integers $c,d \in S$ such that

$$[a]_5 + [b]_5 = [c]_5 \qquad \text{and} \qquad [a]_5[b]_5 = [d]_5.$$

Solution Let us make the addition table first. The *definition* of addition in modular arithmetic implies that

$$[a]_5 + [b]_5 = [a+b]_5$$

where $a+b$ inside the square brackets on the right hand side is ordinary addition of ordinary integers a and b. But we cannot simply take $c = a+b$ because then c will not *in general* be an element of S, and I requested elements of S in the tables.

Now since $a \leq 4$ and $b \leq 4$ always, $a+b$ is at most 8. If $a+b$ happens to be in S already then we can take $c = a+b$. Otherwise $5 \leq a+b \leq 8$, so the integer quotient of $a+b$ by 5 will be 1, and the division will give the remainder $a+b-5$, which *does* lie in S:

$$5 \leq a+b \leq 8 \quad \Rightarrow \quad a+b = 1\cdot 5 + (a+b-5).$$

If you prefer a formula to the above discussion, we can take

$$c = \begin{cases} a+b & \text{if} \quad a+b \leq 5 \\ a+b-5 & \text{if} \quad a+b \geq 5. \end{cases}$$

This leads to the following addition table for $\mathbb{Z}_5$:

$+$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[0]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[1]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$	$[0]_5$
$[2]_5$	$[2]_5$	$[3]_5$	$[4]_5$	$[0]_5$	$[1]_5$
$[3]_5$	$[3]_5$	$[4]_5$	$[0]_5$	$[1]_5$	$[2]_5$
$[4]_5$	$[4]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$

The second case of the rule above, where $c = a + b - 5$, is visible as the lower-right triangular chunk of the table, starting at the diagonal stripe of $[0]_5$.

For the multiplication table, we use the definition

$$[a]_5[b]_5 = [ab]_5,$$

and again we need to find a representative of $[ab]_5$ that is in S. There is less we can say in general about what the integer quotient of each product is, but we don't need to; it's enough to compute the remainder of each product $a \cdot b$ modulo 5 and record these in a table. Eventually the table we produce is the following.

$\cdot$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[0]_5$	$[0]_5$	$[0]_5$	$[0]_5$	$[0]_5$	$[0]_5$
$[1]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[2]_5$	$[0]_5$	$[2]_5$	$[4]_5$	$[1]_5$	$[3]_5$
$[3]_5$	$[0]_5$	$[3]_5$	$[1]_5$	$[4]_5$	$[2]_5$
$[4]_5$	$[0]_5$	$[4]_5$	$[3]_5$	$[2]_5$	$[1]_5$

Question 2 Find all solutions $X \in \mathbb{Z}_{10}$ to the equation $X^2 = [3]_{10} \cdot X$.

[Notation: X^2 means $X \cdot X$.]

Solution You can do this by brute force, that is, testing each of the 10 elements of $\mathbb{Z}_{10}$ to see whether it's a solution or not. In the table below I write all my congruence classes as $[a]_{10}$ for $0 \leq a < 10$; this makes it easy to tell when they are equal.

X	$[0]_{10}$	$[1]_{10}$	$[2]_{10}$	$[3]_{10}$	$[4]_{10}$	$[5]_{10}$	$[6]_{10}$	$[7]_{10}$	$[8]_{10}$	$[9]_{10}$
X^2	$[0]_{10}$	$[1]_{10}$	$[4]_{10}$	$[9]_{10}$	$[6]_{10}$	$[5]_{10}$	$[6]_{10}$	$[9]_{10}$	$[4]_{10}$	$[1]_{10}$
$[3]_{10} \cdot X$	$[0]_{10}$	$[3]_{10}$	$[6]_{10}$	$[9]_{10}$	$[2]_{10}$	$[5]_{10}$	$[8]_{10}$	$[1]_{10}$	$[4]_{10}$	$[7]_{10}$

By inspecting the table, there are exactly four solutions: $\boxed{X = [0]_{10}, [3]_{10}, [5]_{10}, [8]_{10}.}$

Question 3 Let m be a positive integer. Prove that the sum of all elements of $\mathbb{Z}_m$ equals $[0]_m$ if and only if m is odd.

Solution The list of all elements of $\mathbb{Z}_m$ is

$$[0]_m, [1]_m, [2]_m, \ldots, [m-1]_m.$$

Their sum is therefore

$$[0]_m + [1]_m + [2]_m + \cdots + [m-1]_m = [0 + 1 + 2 + \cdots + (m-1)]_m.$$

We know a formula for the sum inside the square brackets: it is $(m-1)m/2$. So the sum we seek is $[(m-1)m/2]_m$.

If m is odd, then $(m-1)/2$ is an integer, so $m \mid (m-1)m/2$, which implies $(m-1)m/2 \cong_m 0$ and therefore $[(m-1)m/2]_m = [0]_m$ by Corollary 1.8 from the notes. That's

the "if" direction of the statement to be proved. Instead of proving the converse, I will do the inverse, which is equivalent. Assume that m is even. Then $(m-2)/2$ is an integer, and

$$\frac{(m-1)m}{2} = \frac{m-2}{2} \cdot m + \frac{m}{2}.$$

Since $0 < m/2 < m$, the division rule says that, when $(m-1)m/2$ is divided by m, the quotient is $(m-2)/2$ and the remainder is $m/2$. So $[(m-1)m/2]_m = [m/2]_m \neq [0]_m$.

The above is a complete proof. But maybe you've seen Gauss' childhood trick for summing the integers from 1 to 100. It turns out you can use a similar trick here! I'd like to show you how.

If $[a]_m$ and its negative $[-a]_m$ are *different* elements of $\mathbb{Z}_m$, then when we sum up all the elements, both $[a]_m$ and $[-a]_m$ show up and cancel each other out in the sum. The only case in which we can't make the cancellation is $[-a]_m = [a]_m$; when these are the same element, it's only present in the sum once, and it would need to be there twice to be cancelled. So, after doing all these cancellations, what's left the sum of all elements $[a]_m$ of $\mathbb{Z}_m$ such that $[-a]_m = [a]_m$. An element $[a]_m$ satisfies this if and only if $-a \equiv_m a$, i.e. if and only if $m \mid a-(-a) = 2a$. As a takes the values $0, 1, \ldots, m-1$, the only ways $2a$ might be a multiple of m is if $2a = 0$ or $2a = m$; any other multiples of m are too big. The case $2a = 0$ always happens, when $a = 0$. But the case $2a = m$ only happens when m is even, when $a = m/2$. That is, when m is odd, the only non-cancelling term of our big sum is $[0]_m$. But when m is even, there are two non-cancelling terms, $[0]_m + [m/2]_m = [m/2]_m$, so the sum is not equal to $[0]_m$.

Question 4

(a) Write out the multiplication table for $\mathbb{Z}_6$. How many times does $[0]_6$ appear in each row of the table?

(b) Based on your answer to part (a) (and other examples, if it helps), write down a formula for how many times $[0]_m$ appears in the $[a]_m$ row of the multiplication table for $\mathbb{Z}_m$, for any integer a and natural number m. Can you explain why your formula works?

Solution (a) Here, without ado, is the times table for $\mathbb{Z}_6$:

$\cdot$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$
$[1]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[2]_6$	$[0]_6$	$[2]_6$	$[4]_6$	$[0]_6$	$[2]_6$	$[4]_6$
$[3]_6$	$[0]_6$	$[3]_6$	$[0]_6$	$[3]_6$	$[0]_6$	$[3]_6$
$[4]_6$	$[0]_6$	$[4]_6$	$[2]_6$	$[0]_6$	$[4]_6$	$[2]_6$
$[5]_6$	$[0]_6$	$[5]_6$	$[4]_6$	$[3]_6$	$[2]_6$	$[1]_6$

And here's a table of how often $[0]_6$ appears:

	$[a]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
number of $[0]_6$:s in row	$[a]_6$	6	1	2	3	2	1

(b) To see what's going on, it helps to expand the question a little bit using the definitions. If $[a]_m[b]_m = [0]_m$ is one of the multiplication facts that gives you a zero in the $[a]_m$ row, then $[ab]_m = [0]_m$, or in other words, ab is a multiple of m. For example, let's think about $a = 4$ in our $\mathbb{Z}_6$ example. For what numbers $b \in \{0,1,2,3,4,5\}$ is the product $4b$ a multiple of 6? Well, $6 = 2 \cdot 3$. Any product $4b$ is even, i.e. has a factor of 2, but the factor of 3 has to come from b, so the possibilities are $b = 0$ and $b = 3$. How this works in general is that, if $m \mid ab$, the factor $\gcd(m,a)$ of m comes from the "fixed" factor a, so the rest has to come from the "varying" factor b. Once you're there, thinking of the gcd, hopefully you spot that the function we have tabulated in part (a) is also $\gcd(a,6)$, so the general formula should be $\boxed{\gcd(a,m)}$.

(If you have read ahead a little to Theorem 2.10, you'll know that $[0]_m$ appears just once in the row for any element $[a]_m$ with a multiplicative inverse, because you can multiply both side of $[a]_m[b]_m = [0]_m$ by $[a]_m^{-1}$ to cancel the $[a]_m$. This would be another hint to be thinking of the gcd.)

The discussion in the first paragraph is halfway to a proof of the formula already. But let's write down a complete proof, in two steps.

Lemma. Given integers a, b and a natural number m, we have $m \mid ab$ if and only if $m/\gcd(a,m) \mid b$.

Proof of lemma. We know that $\gcd(a,m) \mid a$, that is, $a = k\gcd(a,m)$ for some integer k. So if $m/\gcd(a,m) \mid b$, that is $b = \ell \cdot m/\gcd(a,m)$ for some integer ℓ, then

$$ab = k\gcd(a,m) \cdot \ell \frac{m}{\gcd(a,m)} = k\ell m$$

is a multiple of m. For the converse, here is one way to argue using prime factorisations (other arguments are possible based on the ideas of Euclid's algorithm later in the chapter). Assume that $m \mid ab$. This means that every prime in the prime factorisation of m, including repetitions of the same prime, has to also appear in the prime factorisation of a or b. But the greatest common factor of a and m is $\gcd(a,m)$; this is the most we can get from a. So the rest of the primes in the factorisation of m, with product $m/\gcd(a,m)$, have to be factors of b instead.

I have stated the above argument informally. To make it more rigorous you could write it using the proposition in the "Greatest common divisors via prime factorisation" document on QMPlus. Try it!

Proposition. Given an integer a and a natural number m, there are $\gcd(a,m)$ different elements $[b]_m \in \mathbb{Z}_m$ such that $[a]_m[b]_m = [0]_m$.

Proof. By definition, $[a]_m[b]_m = [ab]_m$. By Corollary 1.8 from the notes, $[ab]_m = [0]_m$ if and only if $ab \cong_m 0$, and that in turn means $m \mid ab$. Using the lemma, $m \mid ab$ if and only if $m/\gcd(a,m) \mid b$.

So what we want to prove is that, among the numbers $b = 0, 1, \ldots, m-1$ that give us all the different elements $[b]_m \in \mathbb{Z}_m$, there are $\gcd(a,m)$ different multiples of $m/\gcd(a,m)$. The multiples of $m/\gcd(a,m)$ in this range are

$$0,\ \frac{m}{\gcd(a,m)},\ 2\frac{m}{\gcd(a,m)},\ \ldots,$$

and so on up to the largest multiple of $m/\gcd(a,m)$ less than m. But m itself is a multiple of $m/\gcd(a,m)$, namely $m = \gcd(a,m) \cdot m/\gcd(a,m)$. So the last multiple in our list is $(\gcd(a,m)-1) \cdot m/\gcd(a,m)$, and there are $\gcd(a,m)$ multiples overall.

Question 5 This question compares a naïve way to take the "sum" and "product" of two sets of integers to the definitions that we actually use in modular arithmetic.

(a) Prove that, for any integer $m > 0$, if X and Y are congruence classes of $\equiv_m$, then the set

$$S = \{x + y : x \in X, y \in Y\}$$

is a congruence class of $\mathbb{Z}_m$, and in fact equals the sum $X + Y$ within $\mathbb{Z}_m$.

(b) Give an example of an integer $m > 0$ and two congruence classes X, Y of $\equiv_m$ such that the set

$$P = \{xy : x \in X, y \in Y\}$$

is *not* the product XY within $\mathbb{Z}_m$.

Write down a general statement about P is related to XY.

Solution (a) The definitions of addition and multiplication in $\mathbb{Z}_m$ are framed in terms of representatives. So let's start by pick representatives for the congruence classes X and Y: let $X = [a]_m$ and $Y = [b]_m$. Now $X + Y = [a+b]_m$, and what we have to prove is

$$S = [a+b]_m.$$

This is an equality of sets, so we will prove it by showing each set is a subset of the other. Let's think about the $\subseteq$ direction first — by this I mean the subset statement

$$S \subseteq [a+b]_m.$$

A little reflection shows that this is a statement we have already proved, when we were proving that addition in $\mathbb{Z}_m$ is well-defined. By definition, $S = \{x + y : x \in [a]_m, y \in [b]_m\}$. What we showed is that if you took "different" representatives $a' \in [a]_m$ and $b' \in [b]_m$, then the sum $a' + b'$ was a representative of the same class that $a + b$ was a representative of, that is $a' + b' \in [a+b]_m$. Renaming a' to x and b' to y, this is exactly what we are asked to prove for the $\subseteq$ direction.

To prove the $\supseteq$ direction, that is,

$$S \supseteq [a+b]_m.,$$

what we have to show is that every element z of the class $[a+b]_m$ can be written as $x+y$ for some $x \in [a]_m$ and $y \in [b]_m$. Well, we get to pick x and y here, so there is lots of freedom: we may as well begin by taking $x = a$. That implies we must take $y = z - a$, so we have succeeded if $z - a$ is in the congruence class $[b]_m$.

In fact, we have succeeded. Since $z \in [a+b]_m$, we have $z \equiv_m a + b$, which means $m \mid z - (a+b)$. What we wish to show is that $z - a \in [b]_m$, that is $z - a \equiv_m b$, which means $m \mid (z-a) - b$; but this is our assumption. This completes the proof of the $\supseteq$ direction, and we are finished.

(b) There are many counterexamples. One of them occurs when $m = 5$, $X = [2]_5$ and $Y = [3]_5$. Then

$$XY = [2]_5[3]_5 = [6]_5 = [1]_5,$$

so $1 \in XY$. However, 1 is not an element of the set

$$P = \{xy : x \in [2]_5, y \in [3]_5\}$$

since the only ways to factor 1 as a product of two integers are $1 = 1 \cdot 1$ and $1 = (-1)(-1)$, and neither of these factorisations consists of an element of $[2]_5$ times an element of $[3]_5$.

The general statement that can be made relating the two is that

$$\boxed{P \subseteq XY}.$$

This is proved in a fashion exactly parallel to the proof of the $\subseteq$ inclusion in part (a).