MTH4104 **Introduction to Algebra**

Exercises 5 **For 28 February 2020**

There is no coursework question due on 28 February.

All the questions on this exercise sheet are there for additional practice. It's important to work through lots of questions—remember that mathematics is not a spectator sport!

1 [Question 4 from the 2019 resit exam.]

(a) Write down the *multiplicative inverse law*. Pay attention to the quantifiers ("for all", "there exists") and other conditions in the law.

(b) Use the Euclidean algorithm to show that $\gcd(45, 59) = 1$.

(c) Carrying on from part (b), use the extended Euclidean algorithm to compute the multiplicative inverse of $[45]_{59}$ in $\mathbb{Z}_{59}$.

(d) Find all solutions $x \in \mathbb{Z}_{31}$ to the equation

$$[16]_{31}\,x + [26]_{31} = [2]_{31}\,x + [3]_{31}.$$

Show your working. You are given that $[14]_{31}^{-1} = [20]_{31}$.

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

That is, let $S := \{0, 1, 2, 3, 4\}$ be the canonical set of representatives for $\mathbb{Z}_5$. For each pair of elements $a, b \in S$, your tables should give the integers $c, d \in S$ such that

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

3 (a) Explain why $[59]_{84}$ has a multiplicative inverse in $\mathbb{Z}_{84}$.

(b) Find a non-negative integer $b < 84$ such that $[59]_{84}^{-1} = [b]_{84}$.

4 Find $X, Y \in \mathbb{Z}_{11}$ that satisfy the simultaneous system of linear equations

$$\begin{aligned} [5]_{11}\,X + [2]_{11}\,Y &= [6]_{11} \\ [4]_{11}\,X + \phantom{[2]_{11}}\,Y &= [2]_{11}. \end{aligned}$$

5 How many of the elements of $\mathbb{Z}_{20}$ have multiplicative inverses? What about $\mathbb{Z}_{66}$?

Is there a way to calculate how many elements of $\mathbb{Z}_m$ have multiplicative inverses, without having to list and count them all? Hint: think about the prime factorisation of m.

6 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

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

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

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

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

Write down a general statement about how the above set is related to XY.

7 Let m and n be positive integers and a any integer.

(a) Prove that, as sets,

$$[a]_m \cap [a]_n = [a]_{\mathrm{lcm}(m,n)}.$$

(b) I have a secret integer a in mind. I don't tell you what a is, but I do tell you the remainders when a is divided by m and when a is divided by n. Explain why the equation in part (a) implies that you can work out what the remainder is[1] when a is divided by $\mathrm{lcm}(m,n)$.

[1]This principle, the *Chinese Remainder Theorem*, is used by several old riddles: see for example `https://www.cut-the-knot.org/blue/chinese.shtml`.