MATH 257 – HOMEWORK 0

The aim of this sheet is to cover some background material that we will be using in the course. You can read 0.2 and 0.3 in Dummit–Foote for more discussion.

Question 1. *Prove that, if m and n are integers with $n > 0$, then there are* unique *integers q and r with $0 \leq r < n$ such that $m = qn + r$.*

Find q and r for the following pairs (m, n): $(100, 7)$, $(-57, 16)$.

We call r the **remainder** on dividing m by n. Convince yourself that m is divisible by n if and only if $r = 0$.

The idea of **arithmetic modulo** n is to only remember the remainder that a number leaves when divided by n. So, modulo 2, all even numbers are the same and all odd numbers are the same and we have, for example, the rule 'odd plus odd equals even'. Modulo 10, two (positive) integers are the same if they have the same last digit, and we have, for example $5 + 7 = 2$ (the last digit of 12). Let's set this up precisely:

Question 2. *Let $n \in \mathbb{N}$. Define an equivalence relation $\equiv_n$ on $\mathbb{Z}$ by $a \equiv_n b$ if and only if $b - a$ is divisible by n (i.e. there exists an integer k such that $b - a = kn$).*

1. *Prove that this is an equivalence relation.*
2. *Prove that $a \equiv_n b$ if and only if they have the same remainder on division by n.*
3. *If $[i]$ is the equivalence class containing i, prove that the distinct equivalence classes are exactly $[0], [1], \ldots, [n-1]$.*
4. *Prove that, if $a \equiv_n a'$ and $b \equiv_n b'$ then $a + b \equiv_n a' + b'$ and $ab \equiv_n a'b'$.*

Let $\mathbb{Z}/n\mathbb{Z}$ be the set of equivalence classes for $\equiv_n$. Part 2 of the last question shows that $|\mathbb{Z}/n\mathbb{Z}| = n$.

Question 3. *Explain why the last part of the previous question allows us to define operations $+$ and $\times$ on $\mathbb{Z}/n\mathbb{Z}$ by*

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

and

$$[a] \times [b] = [a \times b].$$

Write out the addition table and multiplication table for $\mathbb{Z}/5\mathbb{Z}$ (i.e. the rows and columns of the table are labelled by the integers modulo 5, and the entries in the table show the result of adding/multiplying modulo 5).

Question 4. *By considering the following equations modulo carefully chosen n, show that they have no solutions in $\mathbb{Z}$:*

1. $x^2 - 2y^2 = 3$;
2. $x^2 - 3y^2 = 5$;
3. $x^3 - 6y^3 = 11$.

(hint: try small primes)

When $n = p$ is prime, $\mathbb{Z}/p\mathbb{Z}$ has special properties. You can assume the following **fact**: if p is a prime number and a and b are integers, then if a and b are not divisible by p, neither is ab. Equivalently, if p divides ab then it divides a or b. We will prove this fact next quarter, but if you are interested you can ask me or Michael.

Define $(\mathbb{Z}/p\mathbb{Z})^\times = \{[1], [2], \ldots, [p-1]\} \subset \mathbb{Z}/p\mathbb{Z}$: the integers not divisible by p, modulo p.

Question 5. *Use the above **fact** to prove that, if a is not divisible by p, then 'multiplication by $[a]$' is an* injective *function from $(\mathbb{Z}/p\mathbb{Z})^\times$ to itself.*

Show that any injective function from a finite set to itself is bijective. Deduce that there is $[b]$ in $(\mathbb{Z}/p\mathbb{Z})^\times$ such that $[a][b] = [1]$.

Question 6. *Prove that $\mathbb{Z}/p\mathbb{Z}$ is a field.*

Prove that, if n is not prime, then $\mathbb{Z}/n\mathbb{Z}$ is not a field.

When we are thinking of $\mathbb{Z}/p\mathbb{Z}$ as a field, we will often use the alternative notation $\mathbb{F}_p$, and $\mathbb{F}_p^\times$ for the non-zero elements of $\mathbb{F}_p$.

From now on, we will not write the square brackets around numbers, rather using '$\mod n$' to indicate that they are being considered modulo n: for example,

$$4 + 8 = 1 \mod 11.$$

The last four questions are not prerequisites for the course, but are here for you to do if you are interested!

Question 7. *Let $a \in \mathbb{F}_p^\times$. Show that $(a, 2a, 3a, \ldots, (p-1)a)$ is a rearrangement of $(1, 2, \ldots, p-1)$ (modulo p!!). By taking the product of each of these sequences, show that*

$$a^{p-1}(p-1)! = (p-1)! \mod p$$

and so prove that $a^{p-1} = 1 \mod p$.

This result is "Fermat's little theorem".

Question 8. *(harder) By considering a few cases, can you make a conjecture about the value of $(p-1)!$ modulo p? This result is "Wilson's theorem".*

Question 9. *(even harder!) Let p be a prime. Can you always find $g \in \mathbb{F}_p^\times$ such that $1, g, g^2, \ldots, g^{p-2}$ are the distinct elements of $\mathbb{F}_p^\times$? (such a g is called a **primitive root** mod p).*

Question 10. *(open ended) What can you say about the primes p for which 2 is a primitive root?*