MA10209 – Week 5 Tutorial

B3/B4, Andrew Kennedy

Top Tips (response to sheet 4)

- Try to think about whether answers make sense.
  - If you take the product of odd numbers and add 1 you get an even number. The smallest factor (greater than 1) of an even number is always 2. You can't write 2 in the form 4m+3.
- If you reach a contradiction, make sure you know what it contradicts and write your conclusion.
- Don't skip too many steps, especially when there aren't many to begin with.

Key concepts

- Euclid's algorithm
- (Divisors & Primes)
- $\mathbb{Z}_n$ & modular arithmetic

Euclid's algorithm

- To find gcd(a, b) where a>b:

  Find q, r such that

  $$a = qb + r \qquad \text{where } r \in \{0, 1, ..., b-1\}$$

  If $r \neq 0$,

  $$\text{relabel } a = b,\ b = r \text{ and begin again.}$$

- What is gcd(42,99)?
- Find integers λ_0 and μ_0 such that $42\lambda_0 + 99\mu_0 = 1$.

Modular arithmetic

- Write addition and multiplication tables for $\mathbb{Z}_3$.

$+$	$[0]$	$[1]$	$[2]$
$[0]$			
$[1]$			
$[2]$			

$\times$	$[0]$	$[1]$	$[2]$
$[0]$			
$[1]$			
$[2]$			

Modular arithmetic

- Write addition and multiplication tables for $\mathbb{Z}_3$.

$+$	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

$\times$	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

Modular Arithmetic

- Useful for eliminating possibilities in certain examples:
  - Is 167439203 a perfect square?

Modular Arithmetic

- Useful for eliminating possibilities in certain examples:

  - Is 167439203 a perfect square?
  - Work in $\mathbb{Z}_{10}$:
    - $[0]^2 = [0]$, $[1]^2 = [1]$, $[2]^2 = [4]$, $[3]^2 = [9]$, $[4]^2 = [6]$, $[5]^2 = [5]$, $[6]^2 = [6]$, $[7]^2 = [9]$, $[8]^2 = [4]$, $[9]^2 = [1]$,
    - Possibilities are [0], [1], [4], [5], [6], [9]
    - $n^2 = 167439203 \Rightarrow [n^2] = [3]$, or equivalently $n^2 \neq 167439203 \Leftarrow [n^2] \neq [3]$.

Modular Arithmetic

- Show that every square number $q > 3$ is of the form

$$4m \quad \text{or} \quad 4m + 1 \qquad \text{for some } m \in \mathbb{N}.$$

- Show that if we have two numbers of the form $4m + 1$, $m \in \mathbb{N}$, then their product must also be of that form.

- Show that a number of the form $4m + 3, m \in \mathbb{N}$ has at least one factor also in this form.
  - Do all its factors take this form?

Modular arithmetic

- What is the last digit of $3^{5^{17}}$ (written in decimal)?

Modular arithmetic

- What is the last digit of $3^{5^{17}}$ (written in decimal)?
  - Start by working in $\mathbb{Z}_{10}$.
  - Notice that $[3^4] = [1] \mod 10$.
  - Now find integers *k*, *s* such that $5^{17} = 4k + s$.
  - Write $3^{5^{17}} = 3^{4k+s}$ and calculate in $\mathbb{Z}_{10}$.

Exercise Sheet 5 - overview

- Q1 & 2 – Euclid's algorithm
  - Look at similar examples from notes/tutorial
  - Practice makes perfect ☺
  - See the Q1 & 2 helpful handout (on the course diary)
- Q4
  - If you're struggling to find the answers, try writing a list of factors of the first few numbers.
  - Explain answers.

Exercise Sheet 5 - overview

- Q6
  - (c) work in $\mathbb{Z}_8$.
- Q7
  - An equivalence relation must be reflexive, symmetric & transitive. Show all three.
- Q8
  - (b) work in $\mathbb{Z}_7$ - why does this work?

Bonus question

Let $x, y, z \in \mathbb{Z}$ be such that $x^2 + y^2 = z^2$.

Show that at least one of x, y, z is a multiple of 2.

Show that at least one of x, y, z is a multiple of 3.

Show that at least one of x, y, z is a multiple of 5.

Bonus question (part answer)

Let $x, y, z \in \mathbb{Z}$ be such that $x^2 + y^2 = z^2$.
Show that at least one of x, y, z is a multiple of 5.

Work in $\mathbb{Z}_5$. The square numbers are then $[0], [1], [4]$ (check).
Consider $[x^2] + [y^2]$ for all possible combinations of x and y:

[x²]+[y²]		[x²]		
		[0]	[1]	[4]
[y²]	[0]	[0]	[1]	[4]
	[1]	[1]	[2]	[0]
	[4]	[4]	[0]	[3]

By inspection, if $[x^2] + [y^2]$ is a square, then either $[x^2] = 0$, $[y^2] = 0$ or $[x^2] + [y^2] = 0$.

Then, $[a^2] = 0 \Leftrightarrow [a] = 0$, so one of $[x], [y], [z]$ is $[0]$.