MA10209 – Week 7 Tutorial

B3/B4, Andrew Kennedy

Top Tips (response to sheet 6)

- Don't panic! ☺ A lot of people struggled with Sheet 6, and if it helps, Sheet 7 isn't as bad.

- A few common problems:

Common problems on Sheet 6

- Don't assume groups are commutative:
  - When you multiply, multiply both sides of the equation by
    - the same element
    - applied to the same side
      (either pre- or post- multiply both sides)

- Multiplication by the inverse shouldn't be written like division
  - Some of the notation for division assumes that multiplication is commutative, which it isn't always. Even if it is commutative, stick to the usual notation for inverses unless you obviously mean division in the traditional sense.

Common problems on Sheet 6

- Be careful!
  - It's easy to get confused as to what's happening when
  - Write out every step, clearly and with reasons
  - If you can't give a reason, you probably don't understand what you're doing – go and look at notes

- Don't confuse associativity and commutativity:
  - Commutativity:
    - We can change the order of the elements we're multiplying
  - Associativity:
    - We can change the order in which we compute the multiplication
    - (Changing the order of the elements themselves may change the result)

Subgroups

- Let *G* be a group
- A subset *H* of *G* is a <u>subgroup</u> if the group operation of *G*, restricted to *H* causes *H* to be a group

- For *H* a subset of *G*, show the following are equivalent:
  - H is a subgroup of G.
  - $e \in H$ (where e is the identity element of G) and $\forall h, k \in H$ we have $hk^{-1} \in H$.

Chinese Remainder Theorem

Find an integer x such that $x \equiv 4 \mod 5$ and $x \equiv 2 \mod 4$.

- We can see that

$$1 = 5 \cdot 5 + (-6) \cdot 4$$

so that

$$5 \cdot 5 + (-6) \cdot 4 \equiv 1 \mod 4 \Rightarrow 2 \cdot 5 \cdot 5 + 4 \cdot (-6) \cdot 4 \equiv 2 \mod 4$$

and

$$2 \cdot 5 \cdot 5 + (-6) \cdot 4 \equiv 1 \mod 5 \Rightarrow 2 \cdot 5 \cdot 5 + 4 \cdot (-6) \cdot 4 \equiv 4 \mod 5$$

- -46 is one integer satisfying the conditions (there are infinitely many)

Exercise Sheet 7 - Overview

- Q1 – similar to tutorial example
- Q2 – 9 divides 2n+1 $\Longrightarrow$ 2n+1 = 0 mod 9

  $\Longrightarrow$ 2n = -1 mod 9
- Q3 – don't unpick Euclid if you can avoid it – try to spot a number that satisfies the conditions
- Q4 – we want to find a number *u* such that

  $n_i | u + i - 1$ for $i = 1, 2, 3, \ldots, 1000$

  where n_i is the product of 1000 prime numbers for each i.
- Q5 – *u*, *d* coprime, so there exist λ, μ such that

  $$1 = \lambda u + \mu d.$$

Exercise Sheet 7 - Overview

- Q6 – more general than the Chinese Remainder Theorem since we don't have *m*, *n* coprime.
  - How many elements of the domain map to each element in the image?
- Q7 – another question about groups – remember tips from the start of the tutorial
- Q8 – Euler function – look at its properties
- Q9 – sieve of Eratosthenes gives that $x \in S_2 \Rightarrow x+2, x+4, x+6, \ldots \in S_2, x-2, x-4, \ldots \in S_2$ and so on, provided that *x-a* > 0.