Section 1 Lecture 3 – Modular Arithmetic - Solutions

Part 1 (Essential exercises)

Q1)

(i) 5 = 1 x 3 + 2 so the remainder is 2, so 5 (mod 3) = 2

(ii) 43 = 8 x 5 + 3 so the remainder is 3, so 43 (mod 5) = 3

(iii) 17 = 8 x 2 + 1 so the remainder is 1, so 17 (mod 2) = 1

(iv) 18 = 3 x 6 + 0 so the remainder is 0, so 18 (mod 6) = 0

(v) 101 = 10 x 10 + 1 so the remainder is 1, so 101 (mod 10) = 1

(vi) 60 = 8 x 7 + 4 so the remainder is 4, so 60 (mod 7) = 4

(vii) 4 = 0 x 5 + 4 so the remainder is 4, so 4 (mod 5) = 4

(viii) 3 = 1 x 3 + 0 so the remainder is 0, so 3 (mod 3) = 0

(ix) 0 = 0 x 8 + 0 so the remainder is 0, so 0 (mod 8) = 0

Q2)

(i) 17 = 0 x 26 = 17 so the value is 17, which corresponds to R

(ii) 29 = 1 x 26 + 3 so the value is 3, which corresponds to D

(iii) 52 = 2 x 26 + 0 so the value is 0, which corresponds to A

(iv) 61 = 2 x 56 + 9 so the value is 9, which corresponds to J

Q3) Optional further questions:

(i) It will always be 0, there is no remainder when you divide by 1

(ii) Always 0, no remainder when you divide by itself

(iii) No – you cannot divide by 0

(iv) Open research – for example they are used heavily in the chromatic scale in music but there are many other examples!

(v) *Inverses for 1, 2, 3, 4 respectively are 1, 3, 2 and 4. It works whenever n is prime. If not, it won't work for all numbers (only those that do not share a factor in common with n which are called coprime to n – see later in the course when we do Euler's totient function!)*