**MA7010 – Week 5 Exercises**

**Perform the following calculations in the cyclic group G with generator g as specified below.**

**For a) – c) use the Baby Step Giant Step algorithm by hand calculation**

**For d) and e) use both Baby Step Giant Step and Pohlig Hellman algorithms using hand calculations**

**For f), g), h) and i) use just the Pohlig Hellman algorithm; use hand calculations and/or Maple as you see fit.**

1. a) Let G be <x | x40 = 1> and let g = x7 . Find the logarithm of the element h = x28

b) Let G be <x | x45 = 1> and let g = x11 . Find the logarithm of the element h = x34

c) Let G be <x | x72 = 1> and let g = x13 . Find the logarithm of the element h = x49

d) Let G be <x | x125 = 1> and let g = x17 . Find the logarithm of the element h = x19

e) Let G be <x | x81 = 1> and let g = x13 . Find the logarithm of the element h = x8

f) Let G be <x | x243 = 1> and let g = x19 . Find the logarithm of the element h = x18

g) Let G be <x | x1352 = 1> and let g = x37 . Find the logarithm of the element h = x68

h) Let G be <x | x432 = 1> and let g = x73 . Find the logarithm of the element h = x89

i) Let G be <x | x1404= 1> and let g = x67 . Find the logarithm of the element h = x118

2. Check your answers to a) – d) by performing modular exponentiation by hand.

Check your answers to e) – i) by calculating gx in Maple

3. Explore how the *ChineseRemainder* command in Maple evaluates the solution to the set of simultaneous linear congruences that you need to perform the Pohlig Hellman algorithm. You need to load the command using with(NumberTheory) to get access to this command.

4. Write a routine to populate the values in the Pollard Rho Table when you wish to find the logarithm x such that ax = b mod n. Test it by showing that it produces the correct answer for at least one of the values you have found in Q1. You may perform this question in any programming language you wish – refer to <https://en.wikipedia.org/wiki/Pollard%27s_rho_algorithm_for_logarithms>

if you need help getting started.