MA7010 – Number Theory for Cryptography

Assignment 2 – Discrete Logarithms and Associated Algorithms

The questions on page 2 need to be completed and uploaded to Weblearn no later than 3.00pm on Friday 12th January.

While you can talk about the assignment to other students om the module the final submission must be your own work and the University’s policy on plagiarism and assessment offences will be applied if necessary. For Questions 1-3 you may make use of the fragments of Maple code and procedures that have been developed in the workshops but will need to add to these with some additional code.

Questions 4 and 5 should be done as ‘hand calculation’ but you may use a programmable calculator to help you perform multiplication of large numbers.

Question 6 may require you to develop some code to calculate the values in Pollard Rho table

15% of the marks are reserved for your written explanations of your results which should form part of the same document as your results.

Each student will be allocated a different range of numbers so your answers should be individual. The number ranges are:

|  |  |  |
| --- | --- | --- |
| Name | Lower Range | Upper Range |
| Navjeet | 700 | 850 |
| Ajeesh | 600 | 750 |
| Stuart | 800 | 950 |

The questions will ask you about numbers in a range; you should give answers for all values between your lower and upper ranges inclusive.

Question 1 (10 marks)

Consider all the numbers n in your range. Divide the set into two subsets:

A – the subset consisting of all n where there is at least one primitive root modulo n;

B – the subset consisting of all n where no primitive roots exist modulo n.

Question 2 (12 marks)

1. Explain why we can always find a primitive root modulo p when p is a prime.
2. Express the number of primitive roots that exist modulo p using the Euler Totient function and show that your answer correctly predicts the number of primitive roots for all primes in your given range.
3. For the same range as Question 1 use the command *ifactors* in Maple to find the set C whose elements consist of numbers of the form pk (k > 1) or 2pk (k > 1).
4. Hence form a conjecture about when primitive roots do and don’t exist.

Question 3 (15 marks)

Suppose n has the form n = pq where p and q are different primes both > 2.

1. What is φ(n) in terms of p and q?
2. Suppose a is relatively prime to pq. Explain why
3. ap-1 = 1 mod p
4. aq-1 = 1 mod q
5. m = lcm(p-1, q-1) is < (p-1)(q-1)
6. am = 1 mod (p-1)(q-1)
7. Hence explain why numbers of the form n have no primitive roots.
8. Show that all numbers of the form n = pq (p and q both odd primes) in your range are included in set B.

Question 4 (18 marks)

4. Use the *BabyStepsGiantSteps* algorithm to find discrete logarithms x of b mod n for the primitive root a for each of the two examples assigned to you in the table below. Verify that your answer is correct by calculating ax mod m by hand using the method of modular exponentiation.

Question 5 (18 marks)

5. Use the Pohlig Helmann algorithm to find in the cyclic group of order n with the generating element a for both the examples assigned to you below. Verify your answer in Maple.

Question 6 (12 marks)

6. Use the Pollard Rho method to verify your answer to the first example you were allocated in Question 4.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | b | n | a | Method |
| Navjeet | 41 | 71 | 28 | BabyStepGiantStep |
| Navjeet | 34 | 53 | 18 | BabyStepGiantStep |
| Navjeet | x61 | 343 | x5 | Pohlig Hellman |
| Navjeet | x151 | 3267 | x17 | Pohlig Hellman |
| Ajeesh | 47 | 71 | 21 | BabyStepGiantStep |
| Ajeesh | 24 | 53 | 26 | BabyStepGiantStep |
| Ajeesh | x41 | 343 | x11 | Pohlig Hellman |
| Ajeesh | x157 | 3267 | x13 | Pohlig Hellman |
| Stuart | 37 | 71 | 33 | BabyStepGiantStep |
| Stuart | 29 | 53 | 14 | BabyStepGiantStep |
| Stuart | x97 | 343 | x13 | Pohlig Hellman |
| Stuart | x163 | 3267 | x19 | Pohlig Hellman |