MA7010 – Number Theory for Cryptography - Assignment 2

Ajeesh Thattukunnel Vijayan

January 11$^{\text{th}}$ 2024

1 Answers

1. Lower Range $= 600$, Upper Range $= 750$. 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

2. a. Explain why we can always find a primitive root modulo p when p is a prime.
   b. 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.
   c. 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 $p^k(p > 2, k \geq 1)$ or $2p^k(p > 2, k \geq 1)$
   d. Hence form a conjecture about when primitive roots do and don't exist

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

   (a) What is $\phi(n)$ in terms of p and q?
   (b) Suppose a is relatively prime to pq. Explain why
      i. $a^{p-1} \equiv 1 \mod p$
      ii. $a^{q-1} \equiv 1 \mod q$
      iii. $m = lcm(p-1, q-1)$ is less than $(p-1)(q-1)$
      iv. $a^m \equiv 1 \mod (p-1)(q-1)$
   (c) Hence explain why numbers of the form n have no primitive roots. check it out
   (d) Show that all numbers of the form $n = pq$ (p and q both odd primes) in your range are included in set B.

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 $a^x \mod m$ by hand using the method of modular exponentiation.

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.

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
Ajeesh	47	71	21	BabyStepGiantStep
Ajeesh	24	53	26	BabyStepGiantStep
Ajeesh	x^{41}	343	x^{11}	Pohlig Hellmen
Ajeesh	x^{157}	3267	x^{13}	Pohlig Hellmen

Table 1: List of composite numbers of the form P.Q

References

[1] C R Jordan & D A Jordan *MODULAR MATHEMATICS Groups* .

[2] Dr. Ben Fairbairn *GROUP THEORY Solutions to Exercises.*

[3] *https://github.com/Ssophoclis/AKS-algorithm/blob/master/AKS.py*