Assignment 1

Due: 23rd September 2020 at 5.00 p.m

Total: 70 marks

1. Using the theorem divisibility, prove the following
   a) If a|b , then a|bc $\forall \mathrm{a, b, c} \in \mathbb{Z}$ ( 5 marks)
   b) If a|b and b|c , then a|c (5 marks)
2. Using any programming language of choice (preferably python), implement the following algorithms
   a) Modular exponentiation algorithm (10 marks)
   b) The sieve of Eratosthenes (10 marks)
3. Write a program that implements the Euclidean Algorithm (10 marks)

4. Modify the algorithm above such that it not only returns the gcd of a and b but also the Bezouts coefficients x and y, such that $ax + by = 1$ (10 marks)

5. Let m be the gcd of 117 and 299. Find m using the Euclidean algorithm (5 marks)

6. Find the integers p and q , solution to $1002p + 71q = m$ (5 marks)

7. Determine whether the equation $486x + 222y = 6$ has a solution such that $x, y \in Z_p$ If yes, find x and y. If not, explain your answer. (5 marks)

8. Determine integers $x$ and $y$ such that $gcd(421, 11) = 421x + 11y$. (5 marks)

9. Explain the working mechanism of the following signature schemes (15 marks)

   - RSA signature scheme (10 mark)

   - Digital Signature Standard (10 mark)

   - Schnorr Signature Scheme(10 mark)