CMPSC 360 Discrete Mathematics for Computer Science
Fall 2024 Mahfuza Farooque

Worksheet 10

1. **Fermat's Little Theorem:** Simplify the following using Fermat's Little Theorem:
   (a) $5^{300} \bmod 13$
   (b) $3^{4^7} \bmod 7$
2. **Linear Congruence:**
   (a) Find all solutions, if possible to $6x \equiv 4 (\bmod 17)$
   (b) Find all solutions, if possible to $2x \equiv 5 (\bmod 8)$
   (c) Find all solutions, if possible to $3x \equiv 6 (\bmod 12)$
3. **Chinese Remainder Theorem:** Consider the following system of linear congruences:

$$x \equiv 2 \pmod 4$$

$$6x \equiv 3 \pmod{15}$$

   Solve for all solutions using CRT. (Hint: There are 3 unique solutions modulo 60)
4. **RSA:**
   (a) Given p = 23 and q = 19. Compute the public and the private keys.
   (b) Daniel wants to send the message M = 13 to Alice. Using Alice's public and private keys, calculate the ciphertext C, and the value for R when Alice recovers the message.