Worksheet 10 Solutions

1. **Fermat's Little Theorem:** Simplify the following using Fermat's Little Theorem:

   (a) 5^{300} mod 13

   (b) 3^{4^7} mod 7

   Answer:

   (a) According to FLT, $5^{12} \equiv 1$ mod 13
   300 mod 12 = 0
   Hence, $5^{300} \equiv 5^0 \equiv 1$ mod 13

   (b) According to FLT, $3^6 \equiv 1$ mod 7
   Now, consider 4 mod 6 $\equiv$ -2 mod 6
   Therefore, 4^7 mod 6 $\equiv -2^7$ mod 6 $\equiv$ -128 mod 6 $\equiv$ 4
   So, the question reduces to 3^4 mod 7 which is 4.

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 $3x \equiv 6 (\bmod 12)$

   Answer:

   (a)

   First, find the inverse of 6 modulo 17.
   Since $\gcd(6, 17) = 1$, the inverse exists.
   Using the extended Euclidean algorithm, we find that $6 \times 3 \equiv 1 \pmod{17}$.
   Multiplying both sides of the original equation by 3:
   $6x \times 3 \equiv 4 \times 3 \pmod{17}$
   $18x \equiv 12 \pmod{17}$
   $x \equiv 12 \pmod{17}$
   So, the solution is $x \equiv 12 \pmod{17}$.

   (b) $gcd(2, 8) = 2$, which does not divide 5. Thus, no solution exists.

   (c) $gcd(3, 12) = 3$. Thus, 3^{-1} mod 12 does not exist. However, there are still 3 solutions unique modulo 12. Notice that we can first simplify the congruence to $x \equiv 2$ mod 4. All the values of x that satisfy this and are less than 12 are: 2,6, and 10. Thus, the 3 solutions are:

   $$x \equiv 2 (\bmod 12)$$

$$x \equiv 6 (\bmod 12)$$

$$x \equiv 10 (\bmod 12)$$

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)
Answer:
The second congruence $6x \equiv 3 \pmod{15}$ has three solutions i.e., $x \equiv 3 \pmod{15}$ and $x \equiv 8 \pmod{15}$ and $x \equiv 13 \pmod{15}$. Based on these 3 solutions, we can generate three systems of linear congruences:

$$x \equiv 2 \pmod 4$$

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

and,

$$x \equiv 2 \pmod 4$$

$$x \equiv 8 \pmod{15}$$

and,

$$x \equiv 2 \bmod 4$$

$$x \equiv 13 \bmod 15$$

We can solve each of these systems of linear congruence independently using CRT. The common modulus m will be the same i.e., $m = 4 \times 15 = 60$. We get three solutions:

$$x \equiv 18 \pmod{60}$$

and,

$$x \equiv 38 \pmod{60}$$

and,

$$x \equiv 58 \pmod{60}$$

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.

Answer:

(a) $n = p * q = 23 * 19 = 437$
So, $k = (p-1)*(q-1) = 22*18 = 396$
We have to find an e such that $1 < e < k$ and $gcd(e,k) = 1$
If e=5, $e*d \equiv 1 mod k$ = $5*d \equiv 1 mod 396$
d=317
public key, (n,e)= (437, 5)
private key, (n,d)= (437, 317)

(b) Alice's public key is (437,5).
We need to find the remainder of when M^e is divided by 437.
$M^e = 13^5 = 371293$ is divided by 437, the remainder is 280. Daniel sent the Cipher text, C = 280.

We need to find the remainder of when C^d is divided by 437 to decrypt received ciphertext
$C^d = 280^{317}$ is divided by 437, the remainder is 13.