COMPSCI-1DM3: Assignment #2 CH 4-5

Author: Qusay Qadir
Instructor: Mahdee Jodayree
MacID: qadirq
Tut: T02

Due Date: July 21st, 2023

Contents

1 Question #1. [30 Marks]

Suppose that **a** and **b** are integers, $\boldsymbol{a} \equiv \mathbf{11(mod\ 19)}$, and $\boldsymbol{b} \equiv \mathbf{3(mod\ 19)}$. Find the integer $\boldsymbol{c}$ with $0 \leq c \leq 18$ such that

First we need to determine the value of a, which can be done by finding the remainder of 11 / 19. This would be as such that 11 = 19(0) + 11. Thus the lowest non-negative value of a that satisfies $a \equiv 11(\text{mod } 19)$ is 11

Second, we need to determine the value of b, which can be done so as finding the remainder of 3 / 19 which is 3 = 19(0) + 3. Thus the lowest non-negative value of b that satisfies $b \equiv 3(\text{mod } 19)$ is 3.

a) $c \equiv 13a(\text{mod } 19)$

$c \equiv (13)(11)(\text{mod}19)$

$c \equiv 143(\text{mod } 19)$

Therefore, the value of c is 10 such that the remainder of 143 / 19 is 10, 143 = 19(7) + 10

$c \equiv 10(\text{mod } 19)$

b) $c \equiv 8b(\text{mod } 19)$

$c \equiv (8)(3)(\text{mod}19)$

$c \equiv 24(\text{mod } 19)$

Therefore, the value of c is 5 such that the remainder of 24/ 19 is 5, 24 = 19(0) + 5

$c \equiv 5(\text{mod } 19)$

c) $c \equiv a$ - $b(\text{mod } 19)$

$c \equiv (11$ - $3)(\text{mod}19)$

$c \equiv 8(\text{mod } 19)$

Therefore, the value of c is 8 such that the remainder of 9 / 19 is 8, 8 = 19(0) + 8

$c \equiv 8(\text{mod } 19)$

d) $c \equiv 7a + 3b(\text{mod } 19)$

c ≡ 7(11) + 3(3)(mod19)

c ≡ 86(mod 19)

Therefore, the value of c is 10 such that the remainder of 86 / 19 is 10, 86 = 19(4) + 10

c ≡ 10(mod 19)

e) c ≡ $2a^2$ + $3b^2$(mod 19)

c ≡ $2(11)^2$ + $3(3)^2$(mod19)

c ≡ 269(mod 19)

Therefore, the value of c is 8 such that the remainder of 269 / 19 is 3, 269 = 19(14) + 3

c ≡ 3(mod 19)

f) c ≡ a^3 + $4b^3$(mod 19)

c ≡ $(11)^3$ + $4(3)^3$(mod19)

c ≡ 1439(mod 19)

Therefore, the value of c is 14 such that the remainder of 1439 / 19 is 14, 1439 = 19(75) + 14

c ≡ 14(mod 19)

2 Question #2. [20 Marks]

What are the quotient and remainder when

To solve the following questions take into consideration the division algorithm. a = dq + r where d represents the divisor, q represents the quotient, and r represents the remainder with r being $0 \leq r < d$

a) 19 is divided by 7

19 = 7(2) + 5

2 = 19 div 7

5 = 19 mod 7

b) -111 is divided by 11

-111 = 11(-11) + 10

-11 = -111 div 11

10 = -111 mod 11

c) 789 is divided by 23

789 = 23(34) + 7

34 = 789 div 23

7 = 789 mod 23

d) 1001 is divided by 13

1001 = 13(77) + 0

77 = 1001 div 13

0 = 1001 mod 13

3 Question #3. [30 Marks]

Find all the solutions of the congruence $x^2 \equiv$ **16(mod 105)**
The prime factorization of 105 is 3 * 5 * 7. Now we can solve the congruence modulo for each prime factor separately.

For modulo 3:
The solutions are x ≡ 1(mod 3) and x ≡ 2(mod 3) where x = 1 and x = 2

For modulo 5:
The solutions are x ≡ 1(mod 5) and x ≡ 4(mod 5) where x = 1 and x = 4

For modulo 7:
The solutions are x ≡ 3(mod 7) and x ≡ 4(mod 7) where x = 3 and x = 4

Since we only need to find 3 solutions of the 8, we only need to use 3 of the possibilities of the Chinese remainder theorem.

The first system for the Chinese remainder theorem looks like this:

1(mod 3)
1(mod 5)
3(mod 7)

The second system for the Chinese remainder theorem looks like this:

1(mod 3)
1(mod 5)
4(mod 7)

The third system for the Chinese remainder theorem looks like this:

1(mod 3)
4(mod 5)
4(mod 7)

Step 1: Find M_1, M_2 & M_3, for each individual value of the modulo

$$M_1 = 105 \ / \ 3 = 35$$
$$M_2 = 105 \ / \ 5 = 21$$
$$M_3 = 105 \ / \ 7 = 15$$

Step 2: Find the inverse of each of the M values above with there respective modulo and let them be dictated by y_1, y_2 , y_3

2 is the inverse of 35(mod 3) as 2*35 = 1(mod 3). Thus the value of y_1 is 2
1 is the inverse of 21(mod 5) as 1*(21) = 1(mod 5). Thus the value of y_2 is 1
1 is the inverse of 15(mod 7) as 1*(15) = 1 (mod 7). Thus the value of y_3 is 1

x = $a_1 M_1 y_1$ + $a_2 M_2 y_2$ + $a_3 M_3 y_3$

For the first system solution the values of a_1 = 1, a_2 = 1 and a_3 = 3. Where x:

= (1)(35)(2) + (1)(21)(1) + (3)(15)(1)
= 136
136 ≡ 31(mod 105)

For the second system solution the values of a_1 = 1, a_2 = 1 and a_3 = 4. Where x:

= (1)(35)(2) + (1)(21)(1) + (4)(15)(1)
= 151
151 ≡ 46(mod 105)

For the third system solution the values of a_1 = 1, a_2 = 4 and a_3 = 4.Where x:

= (1)(35)(2) + (4)(21)(1) + (4)(15)(1)
= 214

214 ≡ 4(mod 105)

Therefore 3 of 8 solutions of the congruence of x^2 ≡ **16(mod 105)** are
x = 31(mod 105), x = 46(mod 105), x = 4 (mod 105)

4 Question #4. [10 Marks]

Solve the congruence 2x = 7(mod 17) using the inverse of 2 modulo 17

First, since the gcd (2,17) = 1, we know these numbers are relatively prime. Next, we need to find the inverse of 2 modulo 17, this means 2*(some integer) = 1 (mod 17), and by inspection, we can determine that the integer must be 9, as 2(9) = 18 when divided by 17 gives remainder 1 thus 9 is the inverse of 2(mod 17) as 2*(9) = 1(mod 17)

Next, we can multiply both sides of the equation by 9 to 2x = 7(mod 17)

$$9*(2x) \equiv 7*(9) \text{ (mod 17)}$$
$$x \equiv 63 \text{ (mod 17)}$$
$$x = 12$$

Therefore, all solutions of x are in the form 12 + 17n
where n is any real integer

5 Question #5. [20 Marks]

6 Question #6. [20 Marks]

7 Question #7. [30 Marks]

8 Question #8. [30 Marks]

9 Question #9. [30 Marks]

10 Question #10. [10 Marks]

11 Question #11. [20 Marks]

12 Questions #12. [20 Marks]