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

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

Due Date: July 21st (23:59), 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 $\equiv$ 7(11) + 3(3)(mod19)

c $\equiv$ 86(mod 19)

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

c $\equiv$ 10(mod 19)

e) c $\equiv$ $2a^2$ + $3b^2$(mod 19)

c $\equiv$ $2(11)^2$ + $3(3)^2$(mod19)

c $\equiv$ 269(mod 19)

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

c $\equiv$ 3(mod 19)

f) c $\equiv$ a^3 + $4b^3$(mod 19)

c $\equiv$ $(11)^3$ + $4(3)^3$(mod19)

c $\equiv$ 1439(mod 19)

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

c $\equiv$ 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 = $a_1M_1y_1$ + $a_2M_2y_2$ + $a_3M_3y_3$

Finally:
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 $x^2 \equiv$ **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)

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

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

5 Question #5. [20 Marks]

$$\sum_{j=0}^{n}(\frac{-1}{2})^j = \frac{2^{(n+1)} + (-1)^n}{3 \cdot 2^n} \tag{1}$$

We must first prove that the basis step is true for n = 0

$$\sum_{j=0}^{0}\left(\frac{-1}{2}\right)^0 = \frac{2^{(0+1)}+(-1)^0}{3 \cdot 2^0}$$
$$1 = \frac{2^1+1}{3 \cdot 1}$$
$$1 = \frac{3}{3}$$
$$1 = 1$$

Therefore the basis step is true. Next, the inductive step, for the IH, we assume that P(k) holds true for any arbitrary positive integer k.

$$\sum_{j=0}^{k}(\frac{-1}{2})^j = \frac{2^{(k+1)} + (-1)^k}{3 \cdot 2^k} \tag{2}$$

We want to prove that P(k+1) is also true

$$\sum_{j=0}^{k+1}(\frac{-1}{2})^j = \frac{2^{(k+2)} + (-1)^{(k+1)}}{3 \cdot 2^{(k+1)}} \tag{3}$$

$$\sum_{j=0}^{k+1}\left(\frac{-1}{2}\right)^j = \sum_{j=0}^{k}\left(\frac{-1}{2}\right)^j + \left(\frac{-1}{2}\right)^{(k+1)}$$
$$= \frac{2^{(k+1)}+(-1)^k}{3 \cdot 2^k} + \frac{-1^{(k+1)}}{2^{(k+1)}}$$
$$= \frac{2^{(k+2)}+2(-1)^k}{3 \cdot 2^{(k+1)}} + \frac{(3)(-1)^{(k+1)}}{(3)2^{(k+1)}}$$
$$= \frac{2^{(k+2)}+(-1)^{(k+1)}}{3 \cdot 2^{(k+1)}}$$

Thus, P(k) $\rightarrow$ P(k+1), completing the basis step and the inductive step, proving by induction that P(n) is true for all positive integers n.

6 Question #6. [20 Marks]

Let P(n) be the statement that n! $< n^n$, where n is an integer greater than 1.

a) What is the statement P(2)?
2! $< 2^2$
$2 \cdot 1 < 2 \cdot 2$
$2 < 4$

b) Show that P(2) is true, completing the basis step of a proof by mathematical induction that P(n) is true for all integers n is greater than 1

The proof of the basis step is by plugging in the value of n = 2 into the inequality and determining whether it holds true or not

Since $2 < 4$, this is a true statement thus completing the basis step.

c) What is the inductive hypothesis of a proof by mathematical induction that P(n) is true for all integers n greater than 1?

The inductive step would be as follows: k! $< k^k$

d) What do you need to prove in the inductive step of a proof by mathematical induction that P(n) is true for all integers greater than 1.

Since we showed the basis step as P(2), for the inductive step we must show that for a value of k $\geq$ 2, the inductive step holds true for P(k +1)

We must show that (k+1)! $< (k+1)^{(k+1)}$ as this would indicate if
P(k) $\rightarrow$ P(k+1)

7 Question #7. [30 Marks]

Let P(n) be the statement that a postage of n cents can be formed using just 4-cent stamps and 7-cent stamps. The parts of this exercise outline a strong induction proof that P(n) is true for all integers n $\geq$ 18.

a) Show that the statements P(18), P(19), P(20), and P(21) are true, completing the basis step of a proof by strong induction that P(n) is true for all integers n $\geq$ 18.

Firstly P(18) is true because we can create 18 cents with 2 7-cent stamps and 1 4-cent stamps.

Secondly P(19) is true because we can create 19 cents with 3 4-cent stamps and 1 7-cent stamps.

P(20) is true because we can create 20 cents with 5 4-cent stamps.

P(21) is true because we can create 21 cents with 3 7-cent stamps.

b) What is the inductive hypothesis of a proof by strong induction that P(n) is true for all integers n $\geq$ 18?

The inductive hypothesis would be that for all j such that $18 \leq j \leq k$, j cents can be formed using just 4-cent and 7-cent stamps.

c) What do you need to prove in the inductive step of a proof that P(n) is true for all integers n $\geq$ 18?

It must be shown that P(k+1) is true under the assumption that P(k) holds true for all k $\geq$ 18, where we know the value holds up till P(21) through strong induction.

8 Question #8. [30 Marks]

Suppose that P(n) is a propositional function. Determine for which non-negative integers n the statement P(n) must be true if

a) P(0) is true; for all nonnegative integers n, if P(n) is true, then P(n+2) is true.

If P(0) is held true and we take into consideration that every P (n+2) is also true, if we consider that n = 0 proves the basis step, then the second value would be P(0 + 2) n =2, and the third value would be P (2 + 2) n=4 and P (4 + 2) n= 6 and so on, thus concluding that P(n) is true for all even positive integers, and it is not possible to demonstrate if P(n) is true for other non-even positive integers.

b) P(0) is true; for all nonnegative integers n, if P(n) is true, then P(n+3) is true.

If P(0) is held true and we take into consideration that every P (n+3) is also true, if we consider that n = 0 proves the basis step, then the second value would be P(0 + 3) n=3, and the third value would be P (3 + 3) n =6 , and P (6 + 3) n =9 and so on, thus concluding that P(n) is true for all n multiples of 3 and cannot demonstrate if P(n) is true for any other non-negative integers n.

9 Question #9. [30 Marks]

Find f(2), f(3), f(4), and f(5) if f is defined recursively by f(0) = f(1) = 1 and for n = 1,2, ...

a) f(n+1) = $f(n)^2 + f(n-1)^3$

f(2) = $f(1)^2 + f(0)^3$

f(2) = $1^2 + 1^3$

f(2) = 2

f(3) = $f(2)^2 + f(1)^3$

f(3) = 4 + 1

f(3) = 5

f(4) = $f(3)^2 + f(2)^3$

f(4) = $5^2 + 2^3$

f(4) = 33

f(5) = $f(4)^2 + f(3)^3$

f(5) = $33^2 + 5^3$

f(5) = 1214

b) f(n+1) = f(n) / f(n-1)

f(2) = f(1) / f(0)

f(2) = 1

f(3) = f(2) / f(1)

f(3) =1

Thus, from this pattern it is evident that for all value of n f(n) = 1.

Hence f(4) = f(5) = 1

10 Question #10. [10 Marks]

Trace Algorithm 3 when it finds gcd(12,17). That is, show all the steps used by Algorithm 3 to find gcd (12,17).

Let Algorithm 3 be expressed as:

procedure gcd (a,b: non-negative integers with a < b)
if a = 0 **then return** b
else return gcd (b mod a, a)
{output is gcd(a,b)}

The trace will be as follows with the input gcd (12, 17)
gcd (17 mod 12, 12) = gcd (5 ,12)
gcd (12 mod 5, 5) = gcd (2, 5)
gcd (5 mod 2, 2) = gcd(1, 2)
gcd (2 mod 1,1) = gcd (0,1)

Since a = 0 according to the algorithm it will return b, which is 1. Thus the gcd(12,17) = 1 where 12 and 17 are relatively prime.

11 Question #11. [20 Marks]

Devise a recursive algorithm for finding x^n mod m whenever n,x, and m are positive integers based on the fact that
x^n mod m = $(x^{(n-1)} mod m \cdot x mod m)$ mod m

procedure finding $x^n mod m$ (n, x, m: non-negative integers)
s **if** n = 1 then **return** x mod m
else return $(x^{(n-1)} mod m \cdot x mod m)$ mod m
output is x^n mod m

12 Questions #12. [20 Marks]

Prove that for every positive integer n,

$1 \cdot 2 \cdot 3 + 2 \cdot 3 \cdot 4 + ... + n(n+1)(n+2) = \frac{n(n+1)(n+2)(n+3)}{4}$

First step would be the basis step for n = 1.
6 = 1(2)(3)(4) / 4
6 = 6

Inductive Step:
Assume P(k) holds true for an arbitrary positive integer k.
$1 \cdot 2 \cdot 3 + 2 \cdot 3 \cdot 4 + ... + k(k+1)(k+2) = \frac{k(k+1)(k+2)(k+3)}{4}$

Under this assumption, we must show that P(k+1) is true, inductive hypothesis:
$1 \cdot 2 \cdot 3 + 2 \cdot 3 \cdot 4 + ... + k(k+1)(k+2) + (k+1)(k+2)(k+3) = \frac{(k+1)(k+2)(k+3)(k+4)}{4}$

We can show this by

$= \frac{(k)(k+1)(k+2)(k+3)}{4} + (k+1)(k+2)(k+3)$

$= \frac{(k)(k+1)(k+2)(k+3)}{4} + \frac{4(k+1)(k+2)(k+3)}{4}$

$= \frac{(k^4+10k^3+35k^2+50k+24)}{4}$, to simplify this further we will use the factor theorem on the numerator.

We will first use k = -1, we get the numerator to 0, this means that x+1 is a factor of the polynomial
We will then check k = -2, when we plug it in the polynomial we get 0 as well this means that x + 2 is a factor of the polynomial

We now know that both (k+2) and (k+1) are factors of the polynomial this means that $k^2 + 3k + 2$ is a factor of the polynomial.

If we apply long division, $(k^4+10k^3+35k^2+50k+24)/(k^2+3k+2) = (k^2+7k+12)$

If we factor $(k^2 + 7k + 12)$ we get $(k+3)(k+4)$ as factors. Thus demonstrating that factoring $(k^4 + 10k^3 + 35k^2 + 50k + 24)$ is (k+1)(k+2)(k+3)(k+4)

Going back to our inductive step:
$= \frac{(k^4+10k^3+35k^2+50k+24)}{4}$, this simplified is
$= \frac{((k+1)(k+2)(k+3)(k+4))}{4}$, thus showing that P(k) $\rightarrow$ P(k+1) , and concurrently by mathematical induction we now know that P(n) is true for all non-negative integers n