Problem 1. (4 pts)

Calculate the following:
a) $-22 \; mod \; 8$

1 pt $\quad -22 = -3 \times 8 + \boxed{2}$

b) Use the Euclidean Algorithm to find the gcd(302, 201).

1 pt

$302 = 1 \cdot 201 + 101$
$201 = 1 \cdot 101 + 100$
$101 = 1 \cdot 100 + \boxed{1}$ gcd
$100 = 1 \cdot 100 + 0$

Give $\frac{1}{2}$ pt if they get correct answer but don't use Euclidean Algorithm

c) Show that if $a \equiv c \bmod n$ and $b \equiv d \bmod n$ then $a + b \equiv c + d \bmod n$

2 pts

$a \equiv c \bmod n \Rightarrow a = c + k_1 n$

$b \equiv d \bmod n \Rightarrow b = d + k_2 n$

$\therefore \quad a + b = c + d + k_1 n + k_2 n$

$= c + d + (k_1 + k_2) n$

$\Rightarrow \quad a + b \equiv c + d \bmod n$

Problem 2. (4 pts)

a) Prove that if $f : A \to B$ is onto and $g : B \to C$ is onto, then $g \circ f : A \to C$ is onto.

2pts

Given $c \in C$ & Since g is onto there exists $b \in B$ with $g(b) = c$

Given b, Since f is onto, there exists $a \in A$ with $f(a) = b$

$\therefore$ $g \circ f(a) = g(f(a)) = g(b) = c$

So $g \circ f$ is onto

b) If $g \circ f$ and f are onto, does it follow that g is onto? Explain.

Yes, for if g not onto then $g(B) \neq C$

But f is onto, so $f(A) = B$

Hence $g(f(A)) \neq C$

So $g \circ f$ can't be onto

2 pts

1 pt for correct answer

1 pt for correct explanation

Problem 3. (4 pts)

a) Using the definition of f is O(g), show that $7x^2 + 3$ is big-O of x^3. be sure to specify the values of C and k from the definition.

2 pts

$7x^2+3 \leq 7x^2 + x^2$ if $x > 2$ (Since then $x^2 > 3$)

$\leq 8x^2 \leq 8x^3$ if $x > 2$

So $\underline{C = 8}$, $\underline{k = 2}$ (other choices of C, k are possible)

and $7x^2+3 \leq Cx^3$ if $x > 2$

So $7x^2+3$ is $O(x^3)$

b) Show x^3 is not big-O of $7x^2 + 3$

2 pts

If there exist constants C, k such that

$|x^3| \leq C(7x^2+3)$ for $x > k$

Then

$x^3 = |x|^3 \leq C \cdot 8x^2$ for $x > \max\{k, 2\}$

Therefore

$x = \frac{x^3}{x^2} \leq 8C$. for all $x > \max\{k, 2\}$ which is impossible

Thus x^3 is not $O(7x^2+3)$

Problem 4. (4 pts)

a) Find an inverse of 7 mod 5

1pt

$7 = 1 \cdot 5 + 2$

$5 = 2 \cdot 2 + 1$

$\Rightarrow 1 = 5 - 2 \cdot 2$

$= 5 - 2(7 - 5)$

$* \quad 1 = 3 \cdot 5 - 2 \cdot 7$

$\therefore$ inverse of 7 mod 5 is $\boxed{-2}$

b) Find an inverse of 5 mod 7.

1pt

by equation * we also see $\boxed{3}$ is an inverse for 5 mod 7

c)Find all solutions to the system of linear congruences

2 pts

$$x \equiv 3 \bmod 7$$

$$x \equiv 2 \bmod 5$$

1.5 pts if they only give one solution

By Chinese Remainder Thm

$M = 7 \cdot 5 = 35$

$M_1 = \frac{M}{7} = 5$ $\quad Y_1 =$ inverse of 5 mod 7 is 3

$M_2 = \frac{M}{5} = 7$ $\quad Y_2 =$ inverse of 7 mod 5 is -2

$a_1 = 3 \quad a_2 = 2$

$X = a_1 Y_1 M_1 + a_2 Y_2 M_2$

$= 3 \cdot 3 \cdot 5 + 2 \cdot (-2) \cdot 7$

$= 45 - 28 = 17 \bmod 35$

Any other solution is of the form

$\boxed{X + k35}$ k an integer

$\boxed{17 + k \cdot 35}$

Problem 5. 4 pts

a) What is the value of the variable "location" if the algorithm below is run with the list 5, 3, 6, 2, 7, 3 ,2 , 8

2 pts

```
procedure(a_1, ··· a_n: integers)
location := 0
i := 2
while i ≤ n  and location =0
begin
  j :=1
  while j < i and location =0
    if a_i = a_j the location :=i
    else j := j + 1
  i:= i+1
end
```

In grading consideration will be given to the confusion the addition of the line i:i=1 caused

i	j	Location
2	1	0
3	1	0
3	2	0
4	1	0
4	2	0
4	3	0
5	1	0
5	2	0
5	3	0
5	4	0
6	1	0
6	2	$\boxed{6}$ location

b) Give a worst case scenario big-O estrimate for this algorithm if it is run with a list of n integers.

2pts

In the worst case scenario, the outer loop executes from $i=2$ to n

For $i=2$ inner loop executes 1 time

$i=3$ " " " 2 times

$\vdots$

$i=n$ " " " $n-1$ times

Altogether, inner loop executes

$1+2+\cdots+n-1$ times

$$\leq \underbrace{n+n+\cdots+n}_{n-1} = n(n-1) \text{ which is } \boxed{O(n^2)}$$