Problem 1. (4 pts)

Calculate the following:

a) $-13 \; mod \; 6$

1pt

$$-13 = -3 \times 6 + \boxed{5}$$

b) Use the Euclidean Algorithm to find the gcd(34, 21).

1pt

$\frac{1}{2}$ pt for correct answer but don't use Euclidean Algorithm

$$34 = 1 \cdot 21 + 13$$
$$21 = 1 \cdot 13 + 8$$
$$8 = 1 \cdot 5 + 3$$
$$5 = 1 \cdot 3 + 2$$
$$3 = 1 \cdot 2 + \boxed{1}$$
$$2 = 1 \cdot 2 + 0$$

c) Show that if $a \equiv b$ mod n and $b \equiv c$ mod n then $a \equiv c$ mod n

2pts

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

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

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

$= c + (k_1 + k_2) n$

$\Rightarrow \quad a \equiv c \bmod n$

Problem 2. (4 pts)

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

2pts

If $g \circ f(x) = g \circ f(y)$

then $g(f(x)) = g(f(y))$

But since g is 1-1, this implies

$f(x) = f(y)$

and since f is 1-1, this implies

$x = y$

$\therefore$ $g \circ f$ is 1-1

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

2pts

1 pt for correct answer

1 pt for correct explanation

Yes.

For if f not 1-1, then

$f(x) = f(y)$ for some $x \neq y$

$\therefore$ $g(f(x)) = g(f(y))$ for some $x \neq y$

$\therefore$ $g \circ f(x) = g \circ f(y)$ for some $x \neq y$

and $g \circ f$ can't be 1-1

Problem 3. (4 pts)

a) Using the definition of f is O(g), show that $5x^2 + 2$ is big-O of x^3. Be sure to specify the values of C and k from the definition.

2pts

$5x^2+2 \le 5x^2 + x^2$ if $x > 2$

$\le 6x^2 \le 6x^3$ if $x > 2$

So $\underline{C=6}$, $\underline{k=2}$ will work

(as will other values of C, k)

$\le Cx^3$ if $x > 2$

So $5x^2+2$ is $O(x^3)$

b) Show x^3 is not big-O of $5x^2 + 2$

2pts

If there exist C, k such that

$x^3 \le C(5x^2+2)$ for all $x > k$, then

$x^3 \le C \cdot 6x^2$ for all $x > \max\{k, 2\}$ by part a)

$\therefore$ $x = \frac{x^3}{x^2} \le 6 \cdot C$ for all $x > \max\{k, 2\}$

which is impossible. Thus x^3 is <u>not</u> $O(5x^2+2)$

Problem 4. (4 pts)

a) Find an inverse of 5 mod 7.

1pt

$7 = 1 \cdot 5 + 2$

$5 = 2 \cdot 2 + 1$

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

$= 5 - 2(7 - 5)$

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

$\therefore \boxed{3}$ is an inverse of 5 mod 7

b) Find an inverse of 7 mod 5

1pt

Also, by equation $*$

$\boxed{-2}$ is an inverse for 7 mod 5

c) Find all solutions to the system of linear congruences

2 pts

$$x \equiv 2 \bmod 7$$

$$x \equiv 3 \bmod 5$$

1.5 pts if they only give one solution

By Chinese Remainder Thm

$M = 5 \cdot 7$

$M_1 = \frac{M}{7} = 5$

$M_2 = \frac{M}{5} = 7$

Y_1 = inverse of M_1 mod 7 $= 3$

Y_2 = inverse of M_2 mod 5 $= -2$

$a_1 = 2, \; a_2 = 3$

$$x = a_1 Y_1 M_1 + a_2 Y_2 M_2$$
$$= 2 \cdot 3 \cdot 5 + 3 \cdot (-2) \cdot 7$$
$$= 30 - 42 = \boxed{-12 \bmod 35}$$

Any other solution is of the form

$\boxed{x + k \cdot 35}$ k integer

2pts

Problem 5. 4 pts

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

```
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
```

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	$\boxed{5}$ Location

In marking consideration will be given to confusion the addition of the line i:i+1 Created

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

2 pts

In the worst case scenario, the outer loop executes for $i = 2$ 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

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