CS 2214B
Assignment 4

Student name: Ashna Mittal
Student number: 251206758

Problem 1:

(a) Euclidean Algorithm: greatest common divisor of 23805 and 123

To find: gcd(23805, 123)

The GCD of 23805 and 123 is 3.

Using: Let a and b be integers with $a = bq + r$ by Euclidean division.

Thus, $0 \leq r < b$. we get: $gcd(a,b) = gcd(b,r)$

Therefore, we repeat the Euclidean Division.

1. $23805 = 123 \times 193 + 66$
   $= 23805 \bmod 123$ is 66
2. $123 = 66 \times 1 + 57$
   $= 123 \bmod 66$ is 57
3. $66 = 57 \times 1 + 9$
   $= 66 \bmod 57$ is 9
4. $57 = 9 \times 6 + 3$
   $= 57 \bmod 9$ is 3.
5. $9 = 3 \times 3 + 0$
   $= 9 \bmod 3$ is 0

Since, we cannot divide by 0 in next step, the process terminates. We get: $gcd(23805, 123) = gcd(123, 66) = gcd(66, 57) = gcd(57, 9) = gcd(9, 3) = gcd(3, 0) = 3$.

__/__/____

(b) Backward-substitution method :

$$\gcd(a,b) = sa + tb$$

where s, t are bezout coefficients of a, b.

We have, $\gcd(23805, 123) = 3$

To show, $23805s + 123t = 3$.

Using the back-substitute one equation ⇒

$$3 = 57 - 6 \times 9$$
$$3 = 57 - 6(66 - 1 \times 57)$$
$$3 = 57 \times 7 - 6 \times 66$$
$$3 = 7(123 - 1 \times 66) - 6 \times 66$$
$$3 = 7 \times 123 - 13 \times 66$$
$$3 = 7 \times 123 - 13(23805 - 193 \times 123)$$
$$3 = 7 \times 123 - 13 \times 23805 + 2509 \times 123$$
$$3 = 2516 \times 123 - 13 \times 23805$$

Hence, $\gcd(23805, 123) = -13(23805) + 2516(123)$

$\Rightarrow s = -13, \quad t = 2516$

(c) To determine if we can compute a multiplicative inverse, we find gcd(135, 489)

$$489 = 135 \times 3 + 84$$
$$135 = 84 \times 1 + 51$$
$$84 = 51 \times 1 + 33$$
$$51 = 33 \times 1 + 18$$
$$33 = 18 \times 1 + 15$$
$$18 = 15 \times 1 + 3$$
$$15 = 3 \times 5 + 0$$

Since, $\gcd(135, 489) \neq 1$ but equal 3, Hence (a) 135 is the zero divisor for arithmatic modulo (m) 489. Hence, there is no multiplicative inverse.

Problem 2 :-

(a) $-13 \leq x \leq 250$ and $67x + 12 \equiv 78 \bmod 89$

Simplifying the congruence :

$$67x + 12 \equiv 78 \bmod 87$$

(subtracting 12 from both sides :)

$$67x \equiv 66 \bmod 87$$

Using Euclidean Algorithm to find the inverse of 67 modulo 89 -

$$89 = 67 \times 1 + 22$$
$$67 = 22 \times 3 + 1$$
$$22 = 1 \times 22 + 0$$

Since, the $\gcd(67, 89) = 1$, a modular inverse exists

Using Backward - Substitution method to find the bézout's coefficients -

$$1 = 67 - 3 \times 22$$
$$1 = 67 - 3(89 - 1 \times 67)$$
$$1 = 4 \times 67 - 3 \times 89$$

The inverse of 67 modulo 89 is 4, which gives:

$$67x \equiv 66 \bmod 89$$
$$4(67x) \equiv 4 \times 66 \bmod 89$$
$$1 \cdot x \equiv 264 \bmod 89$$
$$x \equiv 86 \bmod 89$$

Since x is of the form: $x = 86 + 89k$ and $-13 \leq x \leq 250$, we can find the smallest and largest k : $-13 \leq 86 + 89K \leq 250$

$\Rightarrow -99 \leq 89K \leq 164$ $\Rightarrow -1 \leq K \leq 1$

possible values : $x = 86 + 89(-1), 86 + 89(0), 86 + 89(1)$

Values of $x = -3, 86, 175$

__/__/____

(b) $\begin{cases} x \equiv 8 \mod 13 \\ x \equiv 15 \mod 17 \end{cases}$

The Chinese Remainder Theorem states that Let m, n be two co-prime integers > 1,

$\begin{cases} x \equiv a \mod m \\ x \equiv b \mod n \end{cases}$

then the above congruences has a unique solution modulo $m \times n$.

Since 13 has 1 and 13 as factors and 17 has 1 and 17 as factors, 13 and 17 are co-prime. Hence, by Chinese Remainder Theorem, there exists a unique solution modulo 221 $\{13 \times 17 = 221\}$.

Hence, there is exactly one solution 'x' which is $0 \leq x \leq 221$.

By Bezout Theorem, there exists s, t such that, $sm + tn = 1$

Applying Euclidean Algorithm, we get $s = 4$ and $t = -3$ such that $13s + 17t = 1$

Since $x = bsm + atn$, we get:

$x = bsm + atn$

$x = bsm + a(1 - sm) = b(1 - tn) + atn$

$x = bsm + a - asm = b - btn + atn$

$x = (15 \times 4 \times 13) + 8 - (8 \times 4 \times 13) = 15 - (15 \times -3 \times 17) + (8 \times -3 \times 17$

$x = 788 - 416 = 780 - 408$

$x = 372 = 372 \mod (221)$

$= 151$ Ans

To Verify : $13 \mid 151 - 8 = 143$ and

$17 \mid 151 - 15 = 136$

(c) $\begin{cases} 4x - y \equiv 9 \mod 67 & -① \\ x + 2y \equiv 16 \mod 67 & -② \end{cases}$

Multiplying ① by '2' and solving ① and ② simultaneously:

$$\begin{array}{rl} 8x - 2y \equiv 18 \mod 67 & \\ x + 2y \equiv 16 \mod 67 & \\ \hline 9x \equiv 34 \mod 67 & \end{array}$$

Using Euclidean Algorithm to find the inverse of 9 modulo 67:

$$67 = 9 \times 7 + 4$$
$$9 = 2 \times 4 + 1$$
$$4 = 4 \times 1 + 0$$

Hence, gcd of (9, 67) is 1 and a modular inverse exists. Using Backward substitution to find the Bézout's coefficients:

$$1 = 9 - 2 \times 4$$
$$1 = 9 - 2(67 - 7 \times 9)$$
$$1 = 15 \times 9 - 2 \times 67$$

The inverse of 9 modulo 67 is 15 which gives: $9x \equiv 34 \mod 67$

$$15(9x) \equiv 15 \times 34 \mod 67$$
$$x \equiv 510 \mod 67$$
$$x \equiv 41 \mod 67$$

Since $x = 37$, $y \Rightarrow 4(41) - 8y \equiv 9 \mod 67$

$\Rightarrow 164 - y \equiv 9 \mod 67$

$\Rightarrow 30 - y \equiv 9 \mod 67$

$\Rightarrow \quad +y \equiv +21 \mod 67$

Hence, $x = 41 \mod 67$

$y = 21 \mod 67$.

Problem 3 :-

To prove : $\gcd(3n+2, 5n+3) = 1$
where n is a positive integer.
Proof : Direct Proof using Euclid.

Using Euclidean Algorithm :

- $5n+3 = 1 \cdot (3n+2) + 2n-1$

$\{(5n+3) \bmod (3n+2)$ is $(2n-1)\}$.
Since, n is a $\mathbb{Z}^+$, therefore, $2n-1 \neq 0$ and so we continue the division by procedure.

- $(3n+2) = 1 \cdot (2n-1) + n+3$.

$\{(3n+2) \bmod (2n-1)$ is $(n+3)\}$.
Similarly, we continue ; because $n+3 \neq 0$.

- $2n-1 = 1 \cdot (n+3) + (n-4)$

$\{(2n-1) \bmod (n+3)$ is $(n-4)\}$
we continue since $n-4 \neq 0$.

- $n+3 = 1 \cdot (n-4) + 7$

Since, we got a constant value '7', let the $\gcd(3n+2, 5n+3) = k$.
Since $3n+2$ and $5n+3$ are divisible by k, so should their linear combinations $(2n-1)$, $(n+3)$, $(n-4)$ and 7.
Hence, by direct proof, we can say that there can be only one number which is '1' that divides all these above terms. So, $k = 1$
Hence, $\gcd(3n+2, 5n+3) = 1$.

Problem 4 :-

(a) $a = 8, \quad c = 5, \quad m = 14, \quad x_0 = 1$

Using the linear Congruential method's recurrence relation : $x_{n+1} = ax_n + c \bmod m$

$x_0 = 1$

$x_1 = 8(1) + 5 \bmod 14 = 13$

$x_2 = 8(13) + 5 \bmod 14 = 109 \% 14 = 11$

$x_3 = 8(11) + 5 \bmod 14 = 93 \% 14 = 9$

$x_4 = 8(9) + 5 \bmod 14 = 77 \% 14 = 7$

$x_5 = 8(7) + 5 \bmod 14 = 61 \% 14 = 5$

$x_6 = 8(5) + 5 \bmod 14 = 45 \% 14 = 3$

$x_7 = 8(3) + 5 \bmod 14 = 29 \% 14 = 1$

$x_8 = 8(1) + 5 \bmod 14 = 13$

$x_9 = 8(13) + 5 \bmod 14 = 11$

$x_{10} = 8(11) + 5 \bmod 14 = 9$

$x_{11} = 8(9) + 5 \bmod 14 = 7$

$x_{12} = 8(7) + 5 \bmod 14 = 5$

$x_{13} = 8(5) + 5 \bmod 14 = 3$

$x_{14} = 8(3) + 5 \bmod 14 = 1$

Hence, the sequence : $\{1, 13, 11, 9, 7, 5, 3, 1, 13, 11, \ldots\}$
It repeats after the first seven elements, since they are always periodic. However, with $m = 14$, we might expect that the period be 14, since there are 14 integers in the range $\{0, 1, 2 \ldots 12, 13\}$

(b) $m = 8$

Assuming $a = 1$, $c = 1$

$x_0 = 1$

$x_1 = 1(1) + 1 \mod 8 = 2$

$x_2 = 1(2) + 1 \mod 8 = 3$

$x_3 = 1(3) + 1 \mod 8 = 4$

$x_4 = 1(4) + 1 \mod 8 = 5$

$x_5 = 1(5) + 1 \mod 8 = 6$

$x_6 = 1(6) + 1 \mod 8 = 7$

$x_7 = 1(7) + 1 \mod 8 = 0$

Hence, for $a = 1, c = 1$, $x_0 \ldots x_7$ gives all possible values $\{0, 1 \ldots 7\}$. However, it is given that $2 \leq a \leq m$, and so we cannot take $a = 1$. This case is therefore not valid.

Assuming $a = 5$, $c = 1$

$x_0 = 1$

$x_1 = 5(1) + 1 \mod 8 = 6$

$x_2 = 5(6) + 1 \mod 8 = 7$

$x_3 = 5(7) + 1 \mod 8 = 4$

$x_4 = 5(5) + 1 \mod 8 = 5$

$x_5 = 5(5) + 1 \mod 8 = 2$

$x_6 = 5(2) + 1 \mod 8 = 3$

$x_7 = 5(3) + 1 \mod 8 = 0$

Hence, for $a = 5$, $c = 1$, $x_0 \ldots x_7$ give all possible values $\{0, 1 \ldots 7\}$

Hence, the valid pair is $(a = 5, c = 1)$.

(C) $x_{n+1} = 65539\, x_n \bmod 2^{31}$

Let $x_0 = 1$

$x_1 = 65539$ { $2^{16} + 3$ }

$x_2 = 393225$

$x_3 = 1769499$

$x_4 = 7077969$

$x_{i+1} = (2^{16}+3)x_i \bmod 2^{31}$

$x_{i+2} = (2^{16}+3)\, x_{i+1} \bmod 2^{31}$

$x_{i+2} = (2^{16}+3)(2^{16}+3)\, x_i \bmod 2^{31}$

$x_{i+2} = (2^{32} + 6 \times 2^{16} + 9)\, x_i \bmod 2^{31}$

$x_{i+2} = 6(2^{16}+3)x_i \bmod 2^{31} - 9x_i \bmod 2^{31}$

$\therefore x_{i+2} = 6x_{i+1} - 9x_i$

Therefore, modulo 2^{31}, purely multiplicative generator $x_{n+1} = 65539 x_n \bmod 2^{31}$ is equivalent to the recurrence relation $x_{i+1} = 6x_{i+1} - 9x_i$, assuming that the x_0 value is same { i.e., 1 }.