Midterm 2 / 2023.3.31 / MAT 1313.002 / Algebra and number systems

1. Find all integer solutions $[x, y]$ to the linear Diophantine equation $15x - 24y = 9$

gcd$(15, 24) = 3$, $3 | 9$ so Cancel: $5x - 8y = 3$

Extended Euclid's algorithm for 8 and 5:

$8 = 5 + 3$ so $1 = 3 - 2 = 3 - (5-3) = -5 + 2 \cdot 3 = -5 + 2(8-5) = 2 \cdot 8 - 3 \cdot 5$
$5 = 3 + 2$
$3 = 2 + 1$ Thus $5(-3) - 8 \cdot (-2) = 1$

Mul. by 3: $5 \cdot (-9) - 8 \cdot (-6) = 3$

Gen. sol.: $[x, y] = \{ [-9 - 8n, -6 - 5n] : n \in \mathbb{Z} \}$

2. Find the general simultaneous solution to the system of linear modular equations

$$7x \equiv 3 \bmod 11$$
$$5x \equiv 2 \bmod 13$$

First solve the individual equations for x:

Reciprocals of $7 \bmod 11$, $5 \bmod 13$

$11 = 7 + 4$ $\quad 1 = 4 - 3 = 4 - (7-4) = -7 + 2 \cdot 4 = -7 + 2(11-7)$
$7 = 4 + 3$ $\quad = 2 \cdot 11 - 3 \cdot 7$ so $7^{-1} \equiv -3 \equiv 8 \bmod 11$
$4 = 3 + 1$

$13 = 2 \cdot 5 + 3$ $\quad 1 = 3 - 2 = 3 - (5-3) = -5 + 2 \cdot 3 = -5 + 2(13 - 2 \cdot 5)$
$5 = 3 + 2$ $\quad = 2 \cdot 13 - 5 \cdot 5$ so $5^{-1} \equiv -5 \equiv 8 \bmod 13$
$3 = 2 + 1$

$x \equiv -3 \cdot 3 \equiv -9 \equiv 2 \bmod 11$
$x \equiv -5 \cdot 2 \equiv -10 \equiv 3 \bmod 13$

System: $x \equiv 2 \bmod 11$ and $x \equiv 3 \bmod 13$ $\iff$

$x = 2 + 11y = 3 + 13z$ for some $y, z \in \mathbb{Z}$

Solve for y: $11y = 1 + 13z$, $11y \equiv 1 \bmod 13$

$13 = 11 + 2$ $\quad 1 = 11 - 5\cdot 2 = 11 - 5(13-11) = -5\cdot 13 + 6\cdot 11$

$11 = 5\cdot 2 + 1$ $\quad$ so $11^{-1} \equiv 6 \bmod 13$, i.e. $y \equiv 6 \bmod 13$

i.e. $\exists$ (new) $z \in \mathbb{Z}$ $\; y = 6 + 13z$

Plug in: $x = 2 + 11(6 + 13z) = 68 + 143z$

By the Chinese remainder theorem the gen. sol. is $x \equiv 68 \bmod 143$

Alt: Chinese remainder formula: $M = 11\cdot 13 = 143$

$x = M_1 b_1 a_1 + M_2 b_2 a_2$ where $M_i b_i \equiv 1 \bmod m_i$ and $a_i =$ r.h.s.

m_i	M_i	b_i	a_i	$M_i b_i a_i$
11	$13 \equiv 2$	6	2	$13\cdot 6\cdot 2 = 156 \equiv \underline{13} \bmod 143$ $(156 = 143 + 13)$
13	$11 \equiv -2$	-7	3	$11\cdot(-7)\cdot 3 = -231 \equiv \underline{55} \bmod 143$ $(-231 = -2\cdot 143 + 55)$

Total: $68 \bmod 143$

3. Let x_n be the sequence of integers recursively defined by

$$x_0 = 0$$
$$x_1 = -3$$
$$x_n = 5x_{n-1} - 4x_{n-2} \text{ for } n > 1$$

Prove by induction on n that $x_n = 1 - 4^n$ for all $n \geq 0$

Basis: $n = 0$: $1 - 4^0 = 1 - 1 = 0$, $n = 1$: $1 - 4^1 = 1 - 4 = -3$ ☺

For $n > 1$ assume $0 \leq k < n \Rightarrow x_k = 1 - 4^k$

In particular $x_{n-1} = 1 - 4^{n-1}$, $x_{n-2} = 1 - 4^{n-2}$

$x_n = 5x_{n-1} - 4x_{n-2} = 5(1 - 4^{n-1}) - 4(1 - 4^{n-2})$

$= 5 - 5\cdot 4^{n-1} - 4 + \underbrace{4\cdot 4^{n-2}}_{4^{n-1}} = 1 - 4\cdot 4^{n-1} = 1 - 4^n$ ☺