DMA Practice problems: Equations (diophantine, modular)

Exercise 1: Find all solutions $(x, y) \in \mathbb{Z}^2$ for the following diophantine equations:
(i) $819x + 315y = 126$; (ii) $10x - 15y = 131$; (iii) $6x + 9y = 204$.

Exercise 2: Solve the following congruences:
(i) $84x \equiv -56 \pmod{308}$; (ii) $3x \equiv 7 \pmod{10}$; (iii) $12x \equiv 0 \pmod{20}$.

Exercise 3: Solve the following equations in the given $\mathbb{Z}_n$:
(i) $84x = 126$ v $\mathbb{Z}_{210}$; (ii) $10x = 0$ v $\mathbb{Z}_{35}$; (iii) $8x = 10$ v $\mathbb{Z}_{12}$.

Exercise 4: Solve the following systems of congruences:

(i) $x \equiv 0 \pmod 3$, $x \equiv 1 \pmod 4$, $x \equiv 2 \pmod 5$;

(ii) $x \equiv 4 \pmod 2$, $x \equiv -4 \pmod 3$, $x \equiv 4 \pmod 5$;

(iii) $x \equiv 1 \pmod 7$, $x \equiv 0 \pmod 9$, $x \equiv -1 \pmod{11}$;

(iv) $x \equiv 3 \pmod 5$, $x \equiv 4 \pmod 4$, $x \equiv 5 \pmod 3$.

Solution 1: (i): $\gcd(819,315) = 63 = 2\cdot 819 + (-5)\cdot 315$, 63 divides 126 so there is a solution. Multiply Bezout's identity by 2: $819\cdot 4 + 315\cdot(-10) = 126$. Solution $x = 4$, $y = -10$.
Homogeneous eq.: $819x + 315y = 0$ cancels to $13x + 5y = 0$, so $x_h = -5k$, $y_h = 13k$. Solution is $x = 4 - 5k$, $y = 13k - 10$ for $k \in \mathbb{Z}$, or $(x,y) = (4-5k, -10+13k)$ for $k \in \mathbb{Z}$.
(ii): We guess $\gcd(10,-15) = 5$, this does not divide 131. No solution.
(iii): We guess $\gcd(6,9) = 3$, so instead of the Euclid algorithm we try just cancelling in the equation: $2x + 3y = 68$. We easily guess that $\gcd(3,2) = 1 = 1\cdot 3 + (-1)\cdot 2$, multiply to get 68: $2\cdot(-68) + 3\cdot 68 = 68$. Thus particular solution $x = -68$, $y = 68$.
Homogeneous case: $2x + 3y = 0$ yields $x_h = -3k$, $y_h = 2k$, so the general solutions is $x = 3k - 68$, $y = 68 - 2k$ for $k \in \mathbb{Z}$, or also $(x,y) = (-68+3k, 68-2k)$ for $k \in \mathbb{Z}$.

Solution 2: (i): $-56 = 84x + 308n$, Euclid: $\gcd(308,84) = 28 = (-1)\cdot 308 + 4\cdot 84$. Since $\frac{-56}{28} = -2 \in \mathbb{Z}$, the equation is solvable. Multiplying the Bezout identity by that -2 we obtain $-56 = 84\cdot(-8) + 2\cdot 308$, so $x = -8$ is a solution.
Hom. case: $84x + 308n = 0$ cancels to $3x + 11n = 0$, hence $x_h = 11k$. We get the solution $x = -8 + 11k$, $k \in \mathbb{Z}$. I prefer $x = 3 + 11k$, $k \in \mathbb{Z}$.
(ii): $7 = 3x + 10n$, obviously $\gcd(3,10) = 1 = (-3)\cdot 3 + 1\cdot 10$ (we guess), multiply this by seven to get $7 = 3\cdot(-21) + 7\cdot 10$, hence $x = -21$ is a solution.
Hom. case: $3x + 10n = 0$ gives $x_h = 10k$ (nothing to cancel), hence the given equation has solution $x = -21 + 10k$, $k \in \mathbb{Z}$. I prefer $x = 9 + 10k$, $k \in \mathbb{Z}$.
(iii): Obviously $\gcd(12,20) = 4$, we cancel: $3x + 5n = 0$ has the solution $x = 5k$, $k \in \mathbb{Z}$.

Solution 3: (i): $126 = 84x + 210n$, Euklid's algorithm: $\gcd(210,84) = 42 = 1\cdot 210 + (-2)\cdot 84$, equation has a solution as $\frac{126}{42} = 3 \in \mathbb{Z}$. Multiplying Bezout's identity by 3 we obtain $126 = 84\cdot(-6) + 210\cdot 3$, hence $x = -6$ is a solution.
Hom. case: $84x + 210n = 0$ cancels to $3x + 5n = 0$, hence $x_h = 5k$ and $x = -6 + 5k$ solves the congruence. There are $\gcd(210,84) = 42$ solutions in $\mathbb{Z}_{210}$: $x = 4 + 5k$ for $k = 0, 1, \dots, 41$, that is, $\{4, 9, 14, 19, \dots, 204, 209\}$.
(ii): We solve $10x + 35n = 0$, we guess $\gcd(35,10) = 5$, divide the equation: $2x + 7n = 0$, so the congruency has the solution $x = 7k$. There are $\gcd(35,10) = 5$ solutions in $\mathbb{Z}_{35}$, namely $x = 7k$ for $k = 0,1,2,3,4$, that is, $\{0, 7, 14, 21, 28\}$.
(iii): $10 = 8x + 12n$, we can guess $\gcd(12,8) = 4 = 1\cdot 12 + (-1)\cdot 8$, no solution since 4 does not divide 10.

Solution 4: (i): $n = 60$, $N_1 = 20$, inverse element in $\mathbb{Z}_3$ is $x_1 = -1$; $N_2 = 15$, inverse element in $\mathbb{Z}_4$ is $x_2 = -1$; $N_3 = 12$, inverse element in $\mathbb{Z}_5$ is $x_3 = -2$. $x = 0\cdot 20\cdot(-1) + 1\cdot 15\cdot(-1) + 2\cdot 12\cdot(-2) = -63 \equiv 57 \pmod{60}$. General solution is $x = 60k - 63$ (I prefer $57 + 60k$) for $k \in \mathbb{Z}$.
(ii): $n = 30$, $N_1 = 15$, inverse element in $\mathbb{Z}_2$ is $x_1 = 1$; $N_2 = 10$, inverse element in $\mathbb{Z}_3$ is $x_2 = 1$; $N_3 = 6$, inverse element in $\mathbb{Z}_5$ is $x_3 = 1$. $x = 4\cdot 15\cdot 1 + (-4)\cdot 10\cdot 1 + 4\cdot 6\cdot 1 = 44 \equiv 14 \pmod{30}$. General solution is $x = 44 + 30k$ (I prefer $14 + 30k$) for $k \in \mathbb{Z}$.
(iii): $n = 693$, $N_1 = 99$, inverse element in $\mathbb{Z}_7$ is $x_1 = 1$; $N_2 = 77$, inverse element in $\mathbb{Z}_9$ is $x_2 = 2$; $N_3 = 63$, inverse element in $\mathbb{Z}_{11}$ is $x_3 = -4$. $x = 1\cdot 99\cdot 1 + 0\cdot 77\cdot 2 + (-1)\cdot 63\cdot(-4) = 351$. General solution is $x = 351 + 693k$ for $k \in \mathbb{Z}$.
(iv): Rewrite as $x \equiv 3 \pmod{5}$, $x \equiv 0 \pmod{4}$, $x \equiv 2 \pmod{3}$. $n = 60$, $N_1 = 12$, inverse element in $\mathbb{Z}_5$ is $x_1 = 3$; we need not worry about N_2; $N_3 = 20$, inverse element in $\mathbb{Z}_3$ is $x_3 = 2$. $x = 3\cdot 12\cdot 3 + 0 + 2\cdot 20\cdot 2 = 188$. General solution is $x = 188 + 60k$ (I prefer $x = 8 + 60k$) for $k \in \mathbb{Z}$.