4.4 Linear Congruences

Note Title 3/21/2005

Note that since $\{0, 1, \ldots, n-1\}$ is a complete set of residues mod n, Then $\{0, c\cdot 1, c\cdot 2, \ldots, c\cdot(n-1)\}$ is also a complete set mod n if $\gcd(c,n)=1$, by prob. 10, p. 69

$\therefore$ for $cx \equiv r \pmod{n}$, to find a solution, you can just test for $x = 0, 1, \ldots, n-1$, since r must be congruent to one of $0, c, \ldots, c\cdot(n-1)$ if $\gcd(c,n)=1$.

$\therefore$ When solving for $Nx = 1 \pmod{n_K}$, you can try $x = 0, 1, \ldots, n_K - 1$ to find one solution, provided $\gcd(N, n_K) = 1$.

1. (a). $25x \equiv 15 \pmod{29}$

$\gcd(25, 29) = 1$, $\therefore$ solution exists

$-4x \equiv -14$ (adding -29)

$2x \equiv 7$ ($\gcd(2, 29) = 1$)

$30x \equiv 105$ (mult. by 15)

$x \equiv 76$ (adding -29)

$\therefore x \equiv 18 \pmod{29}$ (adding -58 on right)

(b) $5x \equiv 2 \pmod{26}$

$\gcd(5,26)=1$, $\therefore$ solution exists.

$25x \equiv 10$ (mult. by 5)

$25x - 26x \equiv 10 - 26 \pmod{26}$

$-x \equiv -16$

$\therefore x \equiv 16 \pmod{26}$

(c) $6x \equiv 15 \pmod{21}$

$\gcd(6,21)=3$, $3 \mid 15$, $\therefore$ solution exists.

$2x \equiv 5 \pmod 7$ (divide by 3)

$2x \equiv 12 \pmod 7$ (add 7)

$x \equiv 6 \pmod 7$ ($\gcd(2,7)=1$, divide by 2)

$\therefore x = 6 + 7t$

Since $\gcd(6,21)=3$, there are 3 mutually incongruent solutions, by Th. 4.7, and by Th. 4.7, they are $t = 0, 1, 2$.

$\therefore x \equiv 6, 13, 20 \pmod{21}$

(d) $36x \equiv 8 \pmod{102}$

$\gcd(36,102)=6$, and $6 \nmid 8$, $\therefore$ no solution

(e) $34x \equiv 60 \pmod{98}$

$\gcd(34,98)=2$, $2 \mid 60$, $\therefore$ solution exists.

$102x \equiv 180$ (mult. by 3)

$102x - 98x \equiv 180 - 2\cdot 98 \pmod{98}$

$4x \equiv -16 \pmod{98}$

$2x \equiv -8 \pmod{49}$

$x \equiv -4 \pmod{49}$ $(\gcd(2,49) = 1)$

$\therefore x = -4 + 49t$

By Th. 4.7, two incongruent solutions exist.

$\therefore t = 0, 1 \Rightarrow x \equiv -4, 45$, or

$x \equiv 45, 98 \pmod{98}$.

(f). $140x \equiv 133 \pmod{301}$

$140 = 2^2 \cdot 5 \cdot 7$, $301 = 7 \times 43$, $\therefore \gcd(140, 301) = 7$

and $7 | 133$. $\therefore$ 7 incongruent solutions exist.

$20x \equiv 19 \pmod{43}$ (divide by 7)

$40x \equiv 38$ (multiply by 2)

$43x - 40x \equiv 43 - 38 \pmod{43}$

$3x \equiv 5 \pmod{43}$

$42x \equiv 70 \pmod{43}$ (mult. by 14)

$43x - 42x \equiv 86 - 70 \pmod{43}$

$x \equiv 16 \pmod{43}$

$\therefore x = 16 + 43t$, $\therefore$ set $t = 0, 1, 2, 3, 4, 5, 6$

$\therefore x \equiv 16, 59, 102, 145, 188, 231, 274 \pmod{301}$

2.(a). $4x + 51y = 9$

$$4x \equiv 9 \pmod{51}$$
$$52x \equiv 117 \quad (\text{mult. by } 13)$$
$$x \equiv 15 \quad (\text{subtract } 51x,\ 102)$$
$$\therefore x = 15 + 51t$$

$$51y \equiv 9 \pmod{4}$$
$$17y \equiv 3 \pmod{4} \qquad (\gcd(51,4)=1, \text{ divide by } 3)$$
$$17y - 16y \equiv 3 \pmod{4}$$
$$y \equiv 3 \pmod{4}$$
$$\therefore y = 3 + 4s$$

$$\therefore 4x + 51y = 4(15+51t) + 51(3+4s)$$
$$= 60 + 204t + 153 + 204s$$
$$\therefore 9 = 213 + 204t + 204s$$
$$\therefore -204 = 204t + 204s$$
$$-1 = t + s$$
$$s = -1 - t$$

$$\therefore x = 15 + 51t$$
$$y = 3 + 4(-1-t) = -1 - 4t$$

(b) $12x + 25y = 331$

$12x \equiv 331 \pmod{25}$

$24x \equiv 662$

$25x - 24x \equiv 662 - 650 \pmod{25}$

$x \equiv 12 \pmod{25}$

$\therefore x = 12 + 25t$

$25y \equiv 331 \pmod{12}$

$25y - 24y \equiv 331 - 324 \pmod{12}$

$y \equiv 7 \pmod{12}$

$\therefore y = 7 + 12s$

$\therefore 12x + 25y = 12(12 + 25t) + 25(7 + 12s)$

$= 144 + 300t + 175 + 300s$

$\therefore 331 = 319 + 300t + 300s$

$12 = 300t + 300s$

$1 = 25t + 25s$

$\therefore 25t = 1 - 25s$

$\therefore x = 12 + 25t = 13 - 25s$

$\therefore x = 13 - 25s$

$y = 7 + 12s$

(c) $5x - 53y = 17$

$5x \equiv 17 \pmod{53}$

$55x \equiv 187 \quad$ (mult. by 11)

$55x - 53x \equiv 187 - 3 \cdot 53 \pmod{53}$

$2x \equiv 28 \pmod{53}$

$x \equiv 14 \pmod{53} \quad$ (gcd(2,53) = 1, divide by 2)

$\therefore x = 14 + 53t$

$-53y \equiv 17 \pmod{5}$

$-53y + 50y \equiv 17 \pmod{5}$

$-3y \equiv 17 \pmod{5}$

$-9y \equiv 51 \pmod{5} \quad$ (mult. by 3)

$y \equiv 51 \pmod{5} \quad$ (add 10y)

$\therefore y = 51 + 5s$

$\therefore 5x - 53y = 5(14 + 53t) - 53(51 + 5s)$

$17 = 70 + 265t - 2703 - 265s$

$2650 = 265t - 265s$

$10 = t - s, \quad s = t - 10$

$\therefore y = 51 + 5(t - 10) = 5t + 1$

$\therefore x = 14 + 53t$

$y = 1 + 5t$

3. Find all solutions to: $3x - 7y \equiv 11 \pmod{13}$

$3x \equiv 7y + 11 \pmod{13}$

$\gcd(3,13)=1$, so $1 \mid (7y+11)$. There are 13 incongruent possibilities for y $(0, 1, \ldots, 12)$

$\therefore$

$y \equiv 0$: $3x \equiv 11 \pmod{13}$
$12x \equiv 44$
$12x - 13x \equiv 44 - 3\cdot 13$
$-x \equiv 5$, $x \equiv -5+13$
$x \equiv 8$

$y \equiv 1$: $3x \equiv 18 \pmod{18}$
$12x \equiv 72$
$-x \equiv 72 - 5\cdot 13$
$x \equiv -7+13$
$x \equiv 6$

$y \equiv 2$: $3x \equiv 25 - 26 \pmod{13}$
$12x \equiv -4$
$12x - 13x \equiv -4$
$x \equiv 4$

$y \equiv 3$: $3x \equiv 32 \pmod{18}$
$12x \equiv 4(32 - 3\cdot 13)$
$12x - 13x \equiv -28 + 26$
$x \equiv 2$

$y \equiv 4$: $3x \equiv 37 \pmod{13}$
$12x \equiv 4\cdot(39 - 3\cdot 13)$
$-x \equiv 0$
$x \equiv 0$

$y \equiv 5$: $3x \equiv 46 \pmod{13}$
$12x \equiv 4(46 - 39)$
$-x \equiv 28 - 26 = 2$
$x \equiv -2$, $x \equiv 11$

$\therefore$ From pattern, all $\pmod{13}$

$y \equiv 0$, $x \equiv 8$
$y \equiv 1$, $x \equiv 6$
$y \equiv 2$, $x \equiv 4$
$y \equiv 3$, $x \equiv 2$
$y \equiv 4$, $x \equiv 0$
$y \equiv 5$, $x \equiv 11$
$y \equiv 6$, $x \equiv 9$
$y \equiv 7$, $x \equiv 7$
$y \equiv 8$, $x \equiv 5$
$y \equiv 9$, $x \equiv 3$
$y \equiv 10$, $x \equiv 1$
$y \equiv 11$, $x \equiv 12$ $(\equiv -1)$
$y \equiv 12$, $x \equiv 10$

4. (a). $x \equiv 1 \pmod 3$

$x \equiv 2 \pmod 5$

$x \equiv 3 \pmod 7$

$N = 3 \cdot 5 \cdot 7 = 105$

$N_1 = \frac{105}{3} = 35$, $N_2 = \frac{105}{5} = 21$, $N_3 = \frac{105}{7} = 15$

$35x \equiv 1 \pmod 3$ $\quad$ $21x \equiv 1 \pmod 5$ $\quad$ $15x \equiv 1 \pmod 7$

$35x - 36x \equiv 1$ $\quad$ $21x - 20x \equiv 1$ $\quad$ $15x - 14x \equiv 1$

$-x \equiv 1$ $\quad$ $x \equiv 1 \pmod 5$ $\quad$ $x \equiv 1 \pmod 7$

$x \equiv -1 \pmod 3$

$\therefore x_1 = -1, x_2 = 1, x_3 = 1$

$\therefore a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 =$

$1 \cdot 35 \cdot (-1) + 2 \cdot 21 \cdot 1 + 3 \cdot 15 \cdot 1 = 52$

$\therefore x \equiv 52 \pmod{105}$

(b). $x \equiv 5 \pmod{11}$

$x \equiv 14 \pmod{29}$

$x \equiv 15 \pmod{31}$

$N = 11 \cdot 29 \cdot 31 = 9889$

$N_1 = 29 \cdot 31 = 899$, $N_2 = 11 \cdot 31 = 341$, $N_3 = 11 \cdot 29 = 319$

$899x \equiv 1 \pmod{11}$ $\quad$ $341x \equiv 1 \pmod{29}$ $\quad$ $319x \equiv 1 \pmod{31}$

$899x - 81 \cdot 11x \equiv 1$ $\quad$ $341x - 12 \cdot 29x \equiv 1$ $\quad$ $319x - 310x \equiv 1$

$899x - 891x \equiv 1$ $\quad$ $341x - 348x \equiv 1$ $\quad$ $9x \equiv 1$

$8x \equiv 1$ $\quad$ $-7x \equiv 1$ $\quad$ $63x \equiv 7$

$32x \equiv 4$ $\quad$ $-28x \equiv 4$ $\quad$ $x \equiv 7$

$32x - 33x \equiv 4$ $\quad$ $x \equiv 4$

$x \equiv -4 \pmod{11}$

$\therefore x_1 = -4, \; x_2 = 4, \; x_3 = 7$

$\therefore q_1 N_1 x_1 + q_2 N_2 x_2 + q_3 N_3 x_3 =$
$5 \cdot 899 \cdot (-4) + 14 \cdot 341 \cdot 4 + 15 \cdot 319 \cdot 7 = 34{,}611$

$\therefore x \equiv 34{,}611 \equiv 34{,}611 - 3 \cdot 9889 \equiv 4{,}944$
$\pmod{9889}$

(c) $x \equiv 5 \pmod{6}$ $\quad$ $N = 6 \cdot 11 \cdot 17 = 1122$

$x \equiv 4 \pmod{11}$ $\quad$ $N_1 = 11 \cdot 17 = 187$

$x \equiv 3 \pmod{17}$ $\quad$ $N_2 = 6 \cdot 17 = 102$

$N_3 = 6 \cdot 11 = 66$

$187x \equiv 1 \pmod{6}$ $\quad$ $102x \equiv 1 \pmod{11}$ $\quad$ $66x \equiv 1 \pmod{17}$

$187x - 186x \equiv 1$ $\quad$ $102x - 99x = 3x \equiv 1$ $\quad$ $66x - 68x = -2x \equiv 1$

$x \equiv 1$ $\quad$ $21x \equiv 7$ $\quad$ $18x \equiv -9$

$21x - 22x \equiv -x \equiv 7$ $\quad$ $18x - 17x = x \equiv -9$

$\therefore x_1 = 1,\ x_2 = -7,\ x_3 = -9$

$\therefore a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 =$
$5 \cdot 187 \cdot 1 + 4 \cdot 102 \cdot (-7) + 3 \cdot 66 \cdot (-9) = -3703$

$\therefore x \equiv -3703 + 4 \cdot 1122 = 785 \pmod{1122}$

(d). $2x \equiv 1 \pmod 5$: $4x \equiv 2,\ 4x - 5x = -x,\ x \equiv -2 \pmod 5$
$3x \equiv 9 \pmod 6$: $x \equiv 3 \pmod 2$
$4x \equiv 1 \pmod 7$: $8x \equiv 2,\ 8x - 7x = x,\ x \equiv 2 \pmod 7$
$5x \equiv 9 \pmod{11}$: $10x \equiv 18,\ 10x - 11x = -x,\ x \equiv -18 \pmod{11}$

$N = 5 \cdot 2 \cdot 7 \cdot 11 = 770$ $\quad N_1 = 2 \cdot 7 \cdot 11 = 154$ $\quad N_3 = 5 \cdot 2 \cdot 11 = 110$
$N_2 = 5 \cdot 7 \cdot 11 = 385$ $\quad N_4 = 5 \cdot 2 \cdot 7 = 70$

$154 x_1 \equiv 1 \pmod 5$ $\qquad 385 x_2 \equiv 1 \pmod 2$
$x_1 \equiv -1$ $\qquad x_2 \equiv 1$

$110 x_3 \equiv 1 \pmod 7$ $\qquad 70 x_4 \equiv 1 \pmod{11}$
$110 x_3 - 7 \cdot 15 x_3 = 5 x_3 \equiv 1$ $\qquad 70 x_4 - 66 x_4 = 4 x_4 \equiv 1$
$15 x_3 \equiv 3$ $\qquad 12 x_4 \equiv 3$
$x_3 \equiv 3$ $\qquad x_4 \equiv 3$

$\therefore a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 + a_4 N_4 x_4 =$
$(-2)(154)(-1) + 3 \cdot 385 \cdot 1 + 2 \cdot 110 \cdot 3 + (-18) \cdot 70 \cdot 3 = -1657$
$\therefore x \equiv -1657 + 3 \cdot 770 = 653 \pmod{770}$

5. $17x \equiv 3 \pmod{2\cdot 3\cdot 5\cdot 7}$

$17x \equiv 3 \pmod{2} \Leftrightarrow x \equiv 1 \pmod{2} \Leftrightarrow x \equiv 1 \pmod{2}$
$17x \equiv 3 \pmod{3} \Leftrightarrow 2x \equiv 0 \pmod{3} \Leftrightarrow x \equiv 0 \pmod{3}$
$17x \equiv 3 \pmod{5} \Leftrightarrow 2x \equiv 3 \pmod{5} \therefore 4x \equiv 6,\ x \equiv -6 \pmod{5}$
$17x \equiv 3 \pmod{7} \Leftrightarrow 3x \equiv 3 \pmod{7} : 6x \equiv 6,\ x \equiv -6 \pmod{7}$

$N = 2\cdot 3\cdot 5\cdot 7 = 210$ $\quad N_1 = 3\cdot 5\cdot 7 = 105$ $\quad N_3 = 2\cdot 3\cdot 7 = 42$
$N_2 = 2\cdot 5\cdot 7 = 70$ $\quad N_4 = 2\cdot 3\cdot 5 = 30$

$105x_1 \equiv 1 \pmod{2}$
$x_1 \equiv 1$

$70x_2 \equiv 1 \pmod{3}$
$70x_2 - 69x_2 = x_2 \equiv 1$

$42x_3 \equiv 1 \pmod{5}$
$84x_3 \equiv 2$
$84x_3 - 85x_3 \equiv 2$
$x_3 \equiv -2$

$30x_4 \equiv 1 \pmod{7}$
$90x_4 \equiv 3$
$90x_4 - 7\cdot 13x_4 = -x_4 \equiv 3$
$x_4 \equiv -3$

$\therefore a_1N_1x_1 + a_2N_2x_2 + a_3N_3x_3 + a_4N_4x_4 =$
$1\cdot 105\cdot 1 + 0\cdot 70\cdot 1 + (-6)(42)(-2) + (-6)(30)(-3) = 1149$

$\therefore x \equiv 1149 - 5\cdot 210 = 99 \pmod{210}$

6. Find smallest integer $a > 2$ s.t.
$2 \mid a,\ 3 \mid a+1,\ 4 \mid a+2,\ 5 \mid a+3,\ 6 \mid a+4$

This is equivalent to:

$a \equiv 0 \pmod{2}$ or $a \equiv 0 \pmod{2}$ [1]
$a+1 \equiv 0 \pmod{3}$ $a \equiv -1 \pmod{3}$ [2]
$a+2 \equiv 0 \pmod{4}$ $a \equiv -2 \pmod{4}$ [3]
$a+3 \equiv 0 \pmod{5}$ $a \equiv -3 \pmod{5}$ [4]
$a+4 \equiv 0 \pmod{6}$ $a \equiv -4 \pmod{6}$ [5]

Note that $\gcd(2,4) = 2$. So eliminate #1, since if [3] is true, [1] is automically true.

Also, $\gcd(3,6) \neq 1$. Multiply [2] by 2 and get

$$(a+1)\cdot 2 \equiv 0\cdot 2 \pmod{3\cdot 2}, \text{ or}$$
$$2a+2 \equiv 0 \pmod{6}$$

Combine this with [5] and get

$$2a+2 \equiv 0 \equiv a+4 \pmod{6}$$
$$\therefore \quad a \equiv 2 \pmod{6}$$

$\therefore$ If this is true, then [2] and [5] will be true.

$\therefore$ So far, we have
$a \equiv -2 \pmod{4}$ [1]'
$a \equiv -3 \pmod{5}$ [2]'
$a \equiv 2 \pmod{6}$ [3]'

Note $\gcd(4,6) \neq 1$. $\therefore$ Combine
[1]' becomes $3a \equiv -6 \pmod{12}$

[3]' becomes $2a \equiv 4 \pmod{12}$

$\therefore \quad 3a + 12 \equiv -6 + 12 = 6 \pmod{12}$

$\quad 2a + 2 \equiv 4 + 2 = 6 \pmod{12}$

$\therefore \quad 3a + 12 \equiv 2a + 2 \pmod{12}$, or

$\quad a \equiv -10 \pmod{12}$

$\therefore$ The system reduces to:

$$a \equiv -3 \pmod{5}$$
$$a \equiv -10 \pmod{12}$$

$\therefore \quad N = 5 \cdot 12 = 60 \qquad N_1 = 12, \; N_2 = 5$

$\therefore \quad 12x_1 \equiv 1 \pmod{5} \qquad 5x_2 \equiv 1 \pmod{12}$

$\quad 24x_1 \equiv 2 \qquad 25x_2 \equiv 5$

$\quad 24x_1 - 25x_1 = -x_1 \equiv 2 \qquad 25x_2 - 24x_2 = x_2 \equiv 5$

$\quad \therefore \; x_1 \equiv -2$

$\therefore \quad a_1 N_1 x_1 + a_2 N_2 x_2 =$

$(-3)(12)(-2) + (-10)(5)(5) = 72 - 250 = -178$

$\therefore \quad a \equiv -178 \pmod{60}$, or $a \equiv 2 \pmod{60}$

$\therefore \quad a \equiv 62 \pmod{60}. \qquad \therefore \; \underline{a = 62}$

7. (a). Obtain three consecutive integers, each having a square factor.

An integer a satisfying the hint will do.

$a \equiv 0 \pmod{2^2}$ $\quad a+1 \equiv 0 \pmod{3^2}$ $\quad a+2 \equiv 0 \pmod{5^2}$

Note $2^2, 3^2, 5^2$ are relatively prime, so can use Chinese Remainder Theorem.

$\therefore\ a \equiv 0 \pmod 4$ $\qquad N = 4 \cdot 9 \cdot 25 = 900$

$a \equiv -1 \pmod 9$ $\qquad N_1 = 9 \cdot 25 = 225$

$a \equiv -2 \pmod{25}$ $\qquad N_2 = 4 \cdot 25 = 100$

$N_3 = 4 \cdot 9 = 36$

$225x_1 \equiv 1 \pmod 4$ $\qquad 100x_2 \equiv 1 \pmod 9$ $\qquad 36x_3 \equiv 1 \pmod{25}$

$225x_1 - 224x_1 = x_1$ $\qquad 100x_2 - 99x_2 = x_2$ $\qquad 72x_3 \equiv 2$

$x_1 \equiv 1$ $\qquad x_2 \equiv 1$ $\qquad 72x_3 - 75x_3 = -3x_3$

$3x_3 \equiv -2$

$24x_3 \equiv -16$

$24x_3 - 25x_3 = -x_3$

$x_3 \equiv 16$

$\therefore\ a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 =$

$0 + (-1)(100)(1) + (-2)(36)(16) = -1252$

$\therefore\ x \equiv -1252 + 2 \cdot 900 = 548 \pmod{900}$

$\therefore$ 548, 549, 550

(6). Obtain three consecutive integers, the first of which is divisible by a square, the second by a cube, and the third by a fourth power.

Consider
$$a \equiv 0 \pmod{5^2}$$
$$a+1 \equiv 0 \pmod{3^3}$$
$$a+2 \equiv 0 \pmod{2^4}$$

Choose reverse order to get small # for n^4

$2^2, 3^3, 5^4$ are relatively prime, so can use Chinese Remainder Theorem.

$\therefore$
$$a \equiv 0 \pmod{25} \qquad N = 25 \cdot 27 \cdot 16 = 10{,}800$$
$$a \equiv -1 \pmod{27} \qquad N_1 = 27 \cdot 16 = 432$$
$$a \equiv -2 \pmod{16} \qquad N_2 = 25 \cdot 16 = 400$$
$$N_3 = 25 \cdot 27 = 675$$

$$432x_1 \equiv 1 \pmod{25}$$
$$432x_1 - 425x_1 = 7x_1$$
$$7x_1 \equiv 1, \quad 49x_1 \equiv 7$$
$$-x_1 \equiv 7, \quad x_1 \equiv -7$$

$$400x_2 \equiv 1 \pmod{27}$$
$$400x_2 - 15 \cdot 27x_2 = -5x_2$$
$$-55x_2 \equiv 11, \quad -x_2 \equiv 11$$
$$x_2 \equiv -11$$

$$675x_3 \equiv 1 \pmod{16}$$
$$675x_3 - 42 \cdot 16x_3 = 3x_3$$
$$15x_3 \equiv 5, \quad -x_3 \equiv 5$$
$$x_3 \equiv -5$$

$\therefore\ a_1 M_1 x_1 + a_2 M_2 x_2 + a_3 M_3 x_3 =$

$0 + (-1)(400)(-11) + (-2)(675)(-5) = 11150$

$\therefore\ 11{,}150 - 10{,}800 = 350$

$\therefore\ 11{,}150 \equiv 350 \pmod{25 \cdot 27 \cdot 16}$

$\therefore\ 350, 351, 352$

8. Eggs removed from a basket

Eggs removed from a basket	Remaining Eggs
2 at a time	1
3 at a time	2
4 "	3
5 "	4
6 "	5
7 "	0

Find smallest number of eggs in basket.

$x \equiv 1 \pmod{2}$ [1]
$x \equiv 2 \pmod{3}$ [2]
$x \equiv 3 \pmod{4}$ [3]
$x \equiv 4 \pmod{5}$ [4]
$x \equiv 5 \pmod{6}$ [5]
$x \equiv 0 \pmod{7}$ [6]

Need to eliminate the non-relatively prime conditions!

If [3] is true, then $x = 3 + 4n = 1 + 2 + 4n =$
$1 + (1+2n) \cdot 2$, so $x \equiv 1 \pmod{2}$.
$\therefore$ Eliminate [1]

Now look at [2] since $\gcd(3,6) \neq 1$

Multiply [2] by 2 and get $2x \equiv 4 \mod (3 \cdot 2)$

Combine with [5]

$\therefore 2x - 4 \equiv x - 5 \pmod{6}$

$\therefore x \equiv -1 \pmod{6}$

$\therefore$ If [5'] is true, [2] and [5] will be true.

$\therefore$ We now have

$$x \equiv 3 \pmod{4} \quad [3]$$
$$x \equiv 4 \pmod{5} \quad [4]$$
$$x \equiv -1 \pmod{6} \quad [5']$$
$$x \equiv 0 \pmod{7} \quad [6]$$

But $\gcd(4,6) \neq 1$. $\therefore$ multiply [3] by 3 and [5'] by 2. $\therefore$ $3x \equiv 9 \pmod{12}$

$2x \equiv -2 \pmod{12}$

$\therefore 3x - 9 \equiv 2x + 2 \pmod{12}$

$x \equiv 11 \pmod{12}$

$\therefore$ Everything reduces to:

$$x \equiv 4 \pmod{5} \quad [4]$$
$$x \equiv 11 \pmod{12} \quad [5'']$$
$$x \equiv 0 \pmod{7} \quad [6]$$

5, 12, 7 are relatively prime, so now can use Chinese Remainder Theorem.

$N = 5 \cdot 12 \cdot 7 = 420$
$N_1 = 12 \cdot 7 = 84$
$N_2 = 5 \cdot 7 = 35$
$N_3 = 5 \cdot 12 = 60$

$\therefore\ 84x_1 \equiv 1 \pmod 5$ $\quad 35x_2 \equiv 1 \pmod{12}$
$84x_1 - 85x_1 = -x_1 \equiv 1$ $\quad 35x_2 - 36x_2 = -x_2 \equiv 1$
$x_1 \equiv -1$ $\quad x_2 \equiv -1$

$60x_3 \equiv 1 \pmod 7$
$60x_3 - 56x_3 = 4x_3 \equiv 1$
$8x_3 \equiv 2$, $8x_3 - 7x_3 = x_3$
$x_3 \equiv 2$

$\therefore\ a_1N_1x_1 + a_2N_2x_2 + a_3N_3x_3 =$
$4 \cdot 84 \cdot (-1) + 11 \cdot 35 \cdot (-1) + 0 = -721$
$-721 + 2 \cdot 420 = 119$

$\therefore$ 119 eggs in the basket

9. Basket-of-eggs problem: One egg remains when the eggs are removed from the basket 2, 3, 4, 5, or 6 at a time; but no eggs remain if removed 7 at a time. Find smallest number of eggs in the basket.

$x \equiv 1 \pmod{2}$ [2]
$x \equiv 1 \pmod{3}$ [3]
$x \equiv 1 \pmod{4}$ [4]
$x \equiv 1 \pmod{5}$ [5]
$x \equiv 1 \pmod{6}$ [6]
$x \equiv 0 \pmod{7}$ [7]

Need to consolidate since $\gcd(2,4) \neq 1$, $\gcd(3,6) \neq 1$, $\gcd(4,6) \neq 1$

If [4] is true, Then $x = 1 + 4n = 1 + 2(2n)$, and so [2] must be true. $\therefore$ Elimate [2].

If [6] is true, Then $x = 1 + 6n = 1 + 3(2n)$, and so [3] is true. $\therefore$ Eliminate [3]

Now multiply [4] by 3 and [6] by 2 to get:

$3x \equiv 3 \pmod{3 \cdot 4} = 3 \pmod{12}$ [4']
$2x = 2 \pmod{2 \cdot 6} = 2 \pmod{12}$ [6']

$\therefore$ $3x - 3 \equiv 2x - 2 \pmod{12}$
$x \equiv 1 \pmod{12}$ [12]

If [12] is true, then so must [4] and [6]
$\therefore$ Now have:

$x \equiv 1 \pmod{5}$
$x \equiv 0 \pmod{7}$
$x \equiv 1 \pmod{12}$

5, 7, 12 relatively prime

$\therefore N = 5 \cdot 7 \cdot 12 = 420$ $\quad N_1 = 7 \cdot 12 = 84$

$N_2 = 5 \cdot 12 = 60$

$N_3 = 5 \cdot 7 = 35$

$\therefore 84x_1 \equiv 1 \pmod 5$

$84x_1 - 85x_1 = -x_1 \equiv 1$

$x_1 \equiv -1 \pmod 5$

$35x_3 \equiv 1 \pmod{12}$

$35x_3 - 36x_3 = -x_3 \equiv 1$

$x_3 \equiv -1 \pmod{12}$

$60x_2 \equiv 1 \pmod 7$

irrelevant since $a_2 = 0$

$$a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 = 1 \cdot 84 \cdot (-1) + 0 + 1 \cdot 35 \cdot (-1)$$
$$= -84 - 35$$
$$= -119$$

$\therefore -119 + 420 = 301$

$\therefore$ 301 eggs in basket.

10\. **10.** (Ancient Chinese Problem.) A band of 17 pirates stole a sack of gold coins. When they tried to divide the fortune into equal portions, 3 coins remained. In the ensuing brawl over who should get the extra coins, one pirate was killed. The wealth was redistributed, but this time an equal division left 10 coins. Again an argument developed in which another pirate was killed. But now the total fortune was evenly distributed among the survivors. What was the least number of coins that could have been stolen?

$x \equiv 3 \pmod{17}$

$x \equiv 10 \pmod{16}$

$x \equiv 0 \pmod{15}$

17, 16, 15 are relatively prime.

$N = 17 \cdot 16 \cdot 15 = 4080$ $\quad N_1 = 16 \cdot 15 = 240$

$N_2 = 17 \cdot 15 = 255$

$N_3 = 17 \cdot 16 = 272$

$240x_1 = 1 \pmod{17}$

$240x_1 - 14 \cdot 17x_1 = 2x_1$

$2x_1 \equiv 1, \ 18x_1 \equiv 9$

$\therefore x_1 \equiv 9 \pmod{17}$

$255x_2 \equiv 1 \pmod{16}$

$255x_2 - 16 \cdot 16x_2 = -x_2$

$\therefore x_2 \equiv -1 \pmod{16}$

$N_3 x_1 \equiv 1 \pmod{15}$

irrelevant since $a_3 = 0$

$\therefore a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 = 3 \cdot 240 \cdot 9 + 10 \cdot 255 \cdot (-1) + 0$
$= 3930$

$\therefore$ 3930 coins.

The solutions manual uses different approach.

$x \equiv 3 \pmod{17} \Rightarrow x = 3 + 17t$

$x \equiv 10 \pmod{16} \Rightarrow 3 + 17t \equiv 10 \pmod{16}$, or

$17t \equiv 7 \pmod{16}$, $\therefore 17t - 16t = t \equiv 7 \pmod{16}$

$\Rightarrow t = 7 + 16k$

$\therefore x = 3 + 17(7 + 16k) = 122 + 272k$

The third condition means $122 + 272k \equiv 0 \pmod{15}$,

$122 + 272k - 18 \cdot 15k \equiv 0$, or $122 + 2k \equiv 0 \pmod{15}$,

$122 - 8 \cdot 15 + 2k \equiv 0$, $2k \equiv -2$, $2k \equiv 13 \pmod{15}$,

$16k \equiv 104$, $\therefore k \equiv 14 \pmod{15}$, $\therefore k = 14 + 15r$

$\therefore x = 122 + 272(14 + 15r) = 3930 + 4080r$

11. Prove $x \equiv a \pmod{n}$ and $x \equiv b \pmod{m}$ admit a simultaneous solution $\Leftrightarrow$ $\gcd(n,m) \mid a-b$; if a solution exists, confirm it is unique modulo $\operatorname{lcm}(n,m)$.

Pf: (1) Suppose a solution exists for x.

Let $d = \gcd(n,m)$. $\therefore n = dr,\ m = ds$

$x \equiv a \pmod{n} \Rightarrow x = a + nt$, some integer t
$x \equiv b \pmod{m} \Rightarrow x = b + mk$, some integer k

$\therefore a + nt = b + mk$, or $nt - mk = b - a$

Substituting for n and m,
$drt - dsk = b - a$,
$d(sk - rt) = a - b$. $\therefore d = \gcd(n,m) \mid a-b$

(2) Let $d = \gcd(n,m)$, and suppose $d \mid a-b$

$\therefore dt = a - b$, some integer t.
By Th. 2.3, There are integers x_0 and y_0 s.t. $nx_0 + my_0 = d$

$\therefore dt = nx_0t + my_0t = a - b$

$\therefore m y_0 t + b = a - x_0 t n$

Let $x = a + (-x_0 t) n = b + (y_0 t) m$

$\therefore$ $x \equiv a \pmod{n}$ So there is a
$x \equiv b \pmod{m}$ simultaneous solution.

Now let y be any other solution

$\therefore$ $x \equiv a \pmod{n}$ and $y \equiv a \pmod{n}$
$x \equiv b \pmod{m}$ $y \equiv b \pmod{m}$

$\therefore$ $x \equiv y \pmod{n}$
$x \equiv y \pmod{m}$

By Section 4.2, problem 13, p. 69,

$x \equiv y \pmod{\operatorname{lcm}(n,m)}$

12. $x \equiv 5 \pmod{6}$ and $x \equiv 7 \pmod{15}$

$\gcd(6,15) = 3$. Since $3 \nmid (7-5)$, there is no solution.

13. If $x \equiv a \pmod{n}$, prove either $x \equiv a \pmod{2n}$ or
$x \equiv a + n \pmod{2n}$

Pf: $x \equiv a \pmod{n} \Rightarrow x = a + kn$, some k.

If k is even, then $k = 2r$, some r.
$\therefore x = a + r(2n) \Rightarrow x \equiv a \pmod{2n}$

If k is odd, then $k = 2r+1$, some r.
$\therefore x = a + (2r+1)n = a + n + r2n \Rightarrow$
$x \equiv a + n \ (2n)$

14. $x \equiv 1 \pmod{9}$ and $1 < x < 1200$
$x \equiv 2 \pmod{11}$
$x \equiv 6 \pmod{13}$

9, 11, 13 are rel. prime, so can use Chinese Remainder Theorem.

$N = 9 \cdot 11 \cdot 13 = 1287$
$N_1 = 11 \cdot 13 = 143$ $\quad N_2 = 9 \cdot 13 = 117$ $\quad N_3 = 9 \cdot 11 = 99$

$143 x_1 \equiv 1 \pmod{9}$
$143 x_1 - 9 \cdot 15 x_1 \equiv 8 x_1$
$8x_1 - 9x_1 = -x_1 \equiv 1$
$x_1 \equiv -1$

$117 x_2 \equiv 1 \pmod{11}$
$117 x_2 - 121 x_2 = -4x_2$
$-12 x_2 \equiv 3$, $-x_2 \equiv 3$
$x_2 \equiv -3$

$99x_3 \equiv 1 \pmod{13}$

$99x_3 - 8\cdot 13x_3 = -5x_3$

$-15x_3 \equiv 3$, $-2x_3 \equiv 3$

$-12x_3 \equiv 18$

$x_3 \equiv 18$

$\therefore a_1N_1x_1 + a_2N_2x_2 + a_3N_3x_3 =$
$1\cdot 143\cdot(-1) + 2\cdot 117\cdot(-3) + 6\cdot 99(18) = 9847$

$9847 - 7\cdot 1287 = 838$

$\therefore \underline{838}$

15. (a). Find an integer having the remainders 1, 2, 5, 5 when divided by 2, 3, 6, 12 respectively.

$x \equiv 1 \pmod 2$ [2] divisors not relatively prime,
$x \equiv 2 \pmod 3$ [3] so simplify
$x \equiv 5 \pmod 6$ [6]
$x \equiv 5 \pmod{12}$ [12]

$\gcd(3,6) \neq 1$, so multiply [3] by 2

$\therefore 2x \equiv 4 \pmod 6$
$x \equiv 5 \pmod 6$

$\therefore 2x - 4 \equiv x - 5 \pmod 6$, or $x \equiv -1 \pmod 6$ [6']

$\therefore$ if [6'] is true, then so is [6] and [3]
But [6'] is the same as $x \equiv -1+6=5 \pmod 6$, which is [6]. $\therefore$ can drop [3]

$\gcd(6,12) \neq 1$, so multiply [6] by 2
$\therefore 2x \equiv 10 \pmod{12}$
$x \equiv 5 \pmod{12}$
$\therefore x \equiv 5 \pmod{12}$, which is [12].
$\therefore$ if [12] is true, so is [6], and so is [3]
$\therefore$ can drop [3] and [6].

$\therefore x \equiv 1 \pmod 2$ [2]
$x \equiv 5 \pmod{12}$ [12]

But $\gcd(2,12) \neq 1$. $\therefore$ multiply [2] by 6.
$\therefore 6x \equiv 6 \pmod{12}$
$x \equiv 5 \pmod{12}$
$\therefore 5x \equiv 1 \pmod{12}$
$7 \cdot 5x \equiv 7$, or $35x \equiv 7$
$35x - 36x = -x \equiv 7$
$x \equiv -7+12 = 5$
$\therefore x \equiv 5 \pmod{12}$
$\therefore x = 5 + 12k$
Since want $x > 12$, choose $x = 5+12 = \underline{17}$

(6) Find an intiger with remainders 2, 3, 4, 5 when divided by 3, 4, 5, 6 respectively.

$x \equiv 2 \pmod 3$ [3]
$x \equiv 3 \pmod 4$ [4]
$x \equiv 4 \pmod 5$ [5]
$x \equiv 5 \pmod 6$ [6]

Divisors not relatively prime, so simplify.

Multiply [3] by 2: $2x \equiv 4 \pmod 6$
$x \equiv 5 \pmod 6$ [6]

$\therefore$ $x \equiv -1 \pmod 6$, or
$x \equiv 5 \pmod 6$, which is [6]

$\therefore$ [3] is superfluous since if [6] is true, so is [3]

Now examine [4] and [6]. Multiply [4] by 3 and [6] by 2.

$\therefore$ $3x \equiv 9 \pmod{12}$
$2x \equiv 10 \pmod{12}$

$\therefore$ $x \equiv -1$, or $x \equiv 11 \pmod{12}$ [12]

$\therefore$ if [12] is true, so is [4] and [6]

$\therefore$ $x \equiv 4 \pmod 5$
$x \equiv 11 \pmod{12}$

$\gcd(5, 12) = 1$, $\therefore$ use Chinese Remainder Th.

$N = 5 \cdot 12 = 60 \quad N_1 = 12 \quad N_2 = 5$

$12x_1 \equiv 1 \pmod 5$ $\qquad$ $5x_2 \equiv 1 \pmod{12}$

$24x_1 \equiv 2$ $\qquad$ $25x_2 \equiv 5$

$24x_1 - 25x_1 = -x_1$ $\qquad$ $25x_2 - 24x_2 \equiv 5$

$-x_1 \equiv 2, \ x_1 \equiv -2$ $\qquad$ $x_2 = 5$

$x_1 \equiv -2+5 = 3$

$\therefore a_1 N_1 x_1 + a_2 N_2 x_2 = 4 \cdot 12 \cdot 3 + 11 \cdot 5 \cdot 5 = 419$

$\therefore x \equiv 419 \pmod{60}$, or $x \equiv 419 - 6 \cdot 60$

$x \equiv 59 \pmod{60}$

$\therefore x = \underline{59}$

(c) Find an integer having remainders 3, 11, 15 when divided by 10, 13, 17 respectively.

$x \equiv 3 \pmod{10}$
$x \equiv 11 \pmod{13}$
$x \equiv 15 \pmod{17}$

All divisors or relatively prime. $\therefore$ Use Chinese Remainder Th.

$N = 10 \cdot 13 \cdot 17 = 2210$

$N_1 = 13 \cdot 17 = 221$
$N_2 = 10 \cdot 17 = 170$
$N_3 = 10 \cdot 13 = 130$

$221 x_1 \equiv 1 \pmod{10}$ $\quad$ $170 x_2 \equiv 1 \pmod{13}$

$221 x_1 - 220 x_1 = x_1$ $\quad$ $170 x_2 - 13 \cdot 13 x_2 = x_2$

$x_1 \equiv 1$ $\quad$ $x_2 \equiv 1$

$130 x_3 \equiv 1 \pmod{17}$

$130 x_3 - 8 \cdot 17 x_3 = -6 x_3$

$-6 x_3 \equiv 1, \quad 18 x_3 \equiv -3$

$18 x_3 - 17 x_3 = x_3$

$\therefore x_3 \equiv -3$

$\therefore a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 =$

$3 \cdot 221 \cdot 1 + 11 \cdot 170 \cdot 1 + 15 \cdot 130 \cdot (-3) = -3317$

$\therefore -3317 + 2 \cdot (2210) = 1103$

$\therefore x = \underline{1103}$

16. Let t_n be the n^{th} triangular number. For which values of n does t_n divide $t_1^2 + t_2^2 + \cdots + t_n^2$?

$$t_1^2 + t_2^2 + \ldots + t_n^2 = t_n (3n^3 + 12n^2 + 13n + 2)/30$$

Pf: By induction, if $n = 1$, $t_1 = \frac{n(n+1)}{2} = 1$

$\therefore t_1^2 = 1$, $\quad t_n (3n^3 + 12n^2 + 13n + 2)/30 =$

$1(3 + 12 + 13 + 2)/30 = 1$

Now suppose, for $k > 1$,

$$t_1^2 + \dots + t_k^2 = t_k(3k^3 + 12k^2 + 13k + 2)/30 \quad [1]$$

$$\therefore t_1^2 + \dots + t_k^2 + t_{k+1}^2 =$$

$$t_k(3k^3 + 12k^2 + 13k + 2)/30 + \left[\frac{(k+1)(k+2)}{2}\right]^2$$

$$= \frac{k(k+1)}{2}\left(\frac{3k^3 + 12k^2 + 13k + 2}{30}\right) + \frac{(k+1)^2(k+2)^2}{2^2}$$

$$= \frac{(k+1)}{2}\left[\frac{k(3k^3 + 12k^2 + 13k + 2)}{30} + \frac{(k+1)(k+2)^2}{2}\right]$$

$$= \frac{(k+1)}{2}\left[\frac{3k^4 + 12k^3 + 13k^2 + 2k}{30} + \frac{k^3 + 5k^2 + 8k + 4}{2}\right]$$

$$= \frac{(k+1)}{2}\left[\frac{3k^4 + 27k^3 + 88k^2 + 122k + 60}{30}\right] \quad [2]$$

Now look at right side of [1] using $k+1$.

$$t_{k+1}\left(3(k+1)^3 + 12(k+1)^2 + 13(k+1) + 2\right)/30$$

$$= \frac{(k+1)(k+2)}{2}\left[\frac{3k^3 + 9k^2 + 9k + 3 + 12k^2 + 24k + 12 + 13k + 15}{30}\right]$$

$$= \frac{(k+1)}{2}(k+2)\left[\frac{3k^3+21k^2+46k+30}{30}\right]$$

$$= \frac{(k+1)}{2}\left[\frac{3k^4+21k^3+46k^2+30k+6k^3+42k^2+92k+60}{30}\right]$$

$$= \frac{(k+1)}{2}\left[\frac{3k^4+27k^3+88k^2+122k+60}{30}\right] \quad [3]$$

$\therefore$ $[2] = [3]$, so $k \Rightarrow k+1$

$\therefore t_1^2 + \dots + t_n^2 = t_n(3n^3+12n^2+13n+2)/30$

$\therefore t_n \mid (t_1^2 + \dots + t_n^2) \Leftrightarrow \frac{(3n^3+12n^2+13n+2)}{30}$ is

an integer, i.e.,

$(3n^3+12n^2+13n+2) \equiv 0 \pmod{30}$, or

$(3n^3+12n^2+13n+2) \equiv 0 \pmod{2\cdot 3\cdot 5}$, or

$(3n^3+12n^2+13n+2) \equiv 0 \pmod{2}$ [2]
$(3n^3+12n^2+13n+2) \equiv 0 \pmod{3}$ [3]
$(3n^3+12n^2+13n+2) \equiv 0 \pmod{5}$ [4]

since unique solutions are $\equiv \pmod{30}$ by

Chinese Remainder Theorem.

For [2], $3n^3 - 2n^3 + 12n^2 - 6\cdot 2n^2 + 13n - 2\cdot 6n + 2 - 2 =$

$$n^3 + n = n(n^2+1) \equiv 0 \pmod{2}$$

If n is even, then $n(n^2+1)$ is even, and so $n^2(n+1) \equiv 0 \pmod{2}$

If n is odd, n^2 is odd, and n^2+1 is even, so $n(n^2+1)$ is even, so $n(n^2+1) \equiv 0 \pmod{2}$

So [2] puts no restrictions on n.

For [3], $3n^3 - 3n^3 + 12n^2 - 3\cdot 4n^2 + 13n - 3\cdot 4n + 2 =$

$$n + 2 \equiv 0 \pmod{3}$$

$$\therefore n \equiv 1 \pmod{3}$$

For [5], $3n^3 + 12n^2 - 5\cdot 2n^2 + 13n - 5\cdot 2n + 2 =$

$$3n^3 + 2n^2 + 3n + 2 =$$

$$n^2(3n+2) + 3n+2 = (n^2+1)(3n+2) \equiv 0 \pmod{5}$$

$$\therefore (n^2+1) \equiv 0 \pmod{5} \text{ or } (3n+2) \equiv 0 \pmod{5}$$

(using $ab \equiv 0 \pmod{p}$, p prime, $\Rightarrow a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$ — see comments at end of section 4.2, and proof of Theorem 2 in Problems 4.2).

$\therefore$ Problem reduces to $\boxed{n \equiv 1 \pmod{3}}$

and $(n^2+1) \equiv 0 \pmod{5}$ or $(3n+2) \equiv 0 \pmod{5}$

$3n+2 \equiv 0 \pmod 5$

$3n \equiv -2,\ 6n \equiv -4$

$n \equiv -4,\ n \equiv 1$

$\therefore n \equiv 1 \pmod 5$

$n \equiv 1 \pmod 5 \Rightarrow 3n \equiv 3 \pmod{15}$

$n \equiv 1 \pmod 3 \Rightarrow 5n \equiv 5 \pmod{15}$

$\therefore 5n-3n \equiv 5-3 \pmod{15}$

$2n \equiv 2 \pmod{15}$

$\underline{n \equiv 1 \pmod{15}}$

$n^2+1 \equiv 0 \pmod 5$

$n^2 \equiv -1,\ n^2 \equiv 4$

$\therefore n \equiv 2$, or $n \equiv -2$

$\therefore n \equiv 2 \pmod 5$

or $n \equiv 3 \pmod 5$

$n \equiv 2 \pmod 5 \Rightarrow 3n \equiv 6 \pmod{15}$

$n \equiv 1 \pmod 3 \Rightarrow 5n \equiv 5 \pmod{15}$

$\therefore 5n - 3n \equiv 5-6,\ 2n \equiv -1,$

$2n \equiv -1+15,\ 2n \equiv 14,$

$\therefore \underline{n \equiv 7 \pmod{15}}$

$n \equiv 3 \pmod 5 \Rightarrow 3n \equiv 9 \pmod{15}$

$n \equiv 1 \pmod 3 \Rightarrow 5n \equiv 5 \pmod{15}$

$5n-3n \equiv 5-9 = -4,\ 2n \equiv -4,$

$n \equiv -2,\ n \equiv -2+15,$

$\underline{n \equiv 13 \pmod{15}}$

$\therefore n \equiv 1$, or 7, or $13 \pmod{15}$

17. Find solutions of

$$3x+4y \equiv 5 \pmod{13} \quad [1]$$
$$2x+5y \equiv 7 \pmod{13} \quad [2]$$

Mult. [1] by 5: $15x+20y \equiv 25 \pmod{13}$ [1']

Mult. [2] by 4: $8x+20y \equiv 28 \pmod{13}$ [2']

$[1'] - [2']: \quad 7x \equiv -3 \pmod{13}$

$\therefore \quad 14x \equiv -6$

$14x - 13x \equiv -6 + 13$

$x \equiv 7 \pmod{13} \qquad [3']$

Substitue $[3']$ into $[1]$: $\quad 3x \equiv 21 \pmod{13} \quad [3']$

$3x \equiv 5 - 4y \pmod{13} \quad [1]$

$\therefore \quad 21 \equiv 5 - 4y \pmod{13}$

$16 \equiv -4y$

$48 \equiv -12y$

$48 - 3 \cdot 13 \equiv -12y + 13y$

$9 \equiv y \pmod{13}$

$\therefore \quad x \equiv 7 \pmod{13}$

$y \equiv 9 \pmod{13}$

18. Obtain the two incongruent solutions mod 210 of the system:

$2x \equiv 3 \pmod{5} \qquad [5]$

$4x \equiv 2 \pmod{6} \qquad [6]$

$3x \equiv 2 \pmod{7} \qquad [7]$

From $[5]$: $\quad 4x \equiv 6$

$4x - 5x \equiv 6 - 5$

$-x \equiv 1$

$x \equiv -1 + 5$

$x \equiv 4 \pmod{5}$

From [6]: $4x/2 \equiv 2/2 \pmod{6/2}$

$$2x \equiv 1 \pmod 3$$
$$4x \equiv 2$$
$$4x - 3x = x \equiv 2 \pmod 3, \therefore x \equiv 2 \pmod 6$$

Since $\gcd(4,6) = 2$, Th. 4.7 says the 2 incongruent solutions are x_0, $x_0 + \frac{6}{2}$, where x_0 is a solution. $x = 2$ is a solution, so $2 + \frac{6}{2} = 5$ is the other.
$\therefore$ $x \equiv 5 \pmod 6$ is the other.

From [7]: $6x \equiv 4 \pmod 7$

$$6x - 7x \equiv 4 - 7$$
$$-x \equiv -3$$
$$x \equiv 3 \pmod 7$$

$$\therefore \quad x \equiv 4 \pmod 5$$
$$x \equiv 2 \pmod 6 \quad \text{or} \quad x \equiv 5 \pmod 6$$
$$x \equiv 3 \pmod 7$$

$N = 5 \cdot 6 \cdot 7 = 210$

$N_1 = 6 \cdot 7 = 42$
$N_2 = 5 \cdot 7 = 35$
$N_3 = 5 \cdot 6 = 30$

$\therefore\ 42x_1 \equiv 1 \pmod 5$
$42x_1 - 40x_1 = 2x_1 \equiv 1$
$6x_1 \equiv 3,\ 6x_1 - 5x_1 = x_1$
$\therefore\ x_1 \equiv 3 \pmod 5$

$35x_2 \equiv 1 \pmod 6$
$35x_2 - 36x_2 = -x_2$
$\therefore\ x_2 \equiv -1 + 6 = 5$
$x_2 \equiv 5 \pmod 6$

$30x_3 \equiv 1 \pmod 7$
$30x_3 - 28x_3 = 2x_3$
$2x_3 \equiv 1,\ 8x_3 \equiv 4$
$8x_3 - 7x_3 = x_3 \equiv 4$
$\therefore\ x_3 \equiv 4 \pmod 7$

$\therefore\ a_1N_1x_1 + a_2N_2x_2 + a_3N_3x_3 =$

$4(42)(3) + 2(35)(5) + 3(30)(4) = 1214$
or $4(42)(3) + 5(35)(5) + 3(30)(4) = 1739$

$\therefore\ x \equiv 1214 \pmod{210} \Rightarrow \boxed{x \equiv 164 \pmod{210}}$
or $x \equiv 1739 \pmod{210} \Rightarrow \boxed{x \equiv 59 \pmod{210}}$

19. Obtain the 8 incongruent solutions of $3x + 4y \equiv 5 \pmod 8$.

Set $3x \equiv 5 - 4y \pmod 8$. Since $\gcd(3,8) = 1$, and $1 \mid (5-4y)$, Th. 4.7 says there is one solution for any value of y. Since there

are 8 incongruent values of $5-4y$ $(y=0,1,\ldots,7)$
solve for each value of y.

$\therefore\ 3x \equiv 5 \pmod 8$ $\quad 15x \equiv 25,\ 15x-16x \equiv 25-24$

$x \equiv -1,\ x \equiv 7$

$\therefore\ x \equiv 7,\ y \equiv 0 \pmod 8$

$3x \equiv 1 \pmod 8$ $\quad 15x \equiv 5,\ -x \equiv 5,\ x \equiv -5,$

$x \equiv 3$

$\therefore\ x \equiv 3,\ y \equiv 1 \pmod 8$

$3x \equiv -3 \pmod 8$ $\quad 15x \equiv -15,\ -x \equiv 1,\ x \equiv -1,$

$x \equiv 7$

$\therefore\ x \equiv 7,\ y \equiv 2 \pmod 8$

$3x \equiv -7 \pmod 8,$ $\quad 3x \equiv 1,\ 15x \equiv 5,\ -x \equiv 5,$

$x \equiv 3$

$\therefore\ x \equiv 3,\ y \equiv 3 \pmod 8$

$3x \equiv -11 \pmod 8,$ $\quad 3x \equiv 5,\ 15x \equiv 25,\ -x \equiv 1$

$x \equiv -1,\ x \equiv 7$

$\therefore\ x \equiv 7,\ y \equiv 4 \pmod 8$

$3x \equiv -15 \pmod 8,$ $\quad 3x \equiv 1,\ 15x \equiv 5,\ -x \equiv 5,$

$x \equiv -5,\ x \equiv 3$

$\therefore\ x \equiv 3,\ y \equiv 5 \pmod 8$

$3x \equiv -19 \pmod 8$, $3x \equiv -3$, $x \equiv 7$ from above
$\therefore x \equiv 7$, $y \equiv 6 \pmod 8$

$3x \equiv -23 \pmod 8$, $3x \equiv 1$, $\therefore x \equiv 3$ from above
$\therefore x \equiv 3$, $y \equiv 7 \pmod 8$

20. Find solutions to the following systems.

(a). $5x + 3y \equiv 1 \pmod 7$ [1]
$3x + 2y \equiv 4 \pmod 7$ [2]

$10x + 6y \equiv 2 \pmod 7$ [1'] = [1] × 2
$9x + 6y \equiv 12 \pmod 7$ [2'] = [2] × 3

$x \equiv -10 \pmod 7$ [1'] - [2']
$x \equiv -10 + 14 = 4$
$x \equiv 4 \pmod 7$ [3]

$5x \equiv 20 \pmod 7$ [3'] = [3] × 5
$\therefore 1 - 3y \equiv 20 \pmod 7$ [3'] in [1]
$-3y \equiv 19 - 14 = 5$
$-6y \equiv 10$
$-6y + 7y \equiv 10$
$y \equiv 10 \pmod 7$

$\therefore x \equiv 4 \pmod 7$
$y \equiv 10 \pmod 7$

(b) $7x + 3y \equiv 6 \pmod{11}$ [1]

$4x + 2y \equiv 9 \pmod{11}$ [2]

$14x + 6y \equiv 12 \pmod{11}$ [1'] = [1] × 2

$12x + 6y \equiv 27 \pmod{11}$ [2'] = [2] × 3

$2x \equiv -15 \pmod{11}$ [1'] − [2']

$2x \equiv -15 + 22 = 7$

$10x \equiv 35$

$10x - 11x \equiv 35 - 3 \cdot 11$

$-x \equiv 2, \quad x \equiv -2$

$x \equiv -2 + 11 = 9$ [3]

$4x \equiv 36 \pmod{11}$ [3] × 4

$4x \equiv 36 - 33 = 3 \pmod{11}$ [3']

$3 \equiv 9 - 2y \pmod{11}$ [3'] in [2]

$-2y \equiv -6$

$-10y \equiv -30$

$-10y + 11y \equiv -30 + 3 \cdot 11$

$y \equiv 3 \pmod{11}$

$\therefore x \equiv 9 \pmod{11}$

$y \equiv 3 \pmod{11}$

(c) $11x + 5y \equiv 7 \pmod{20}$ [1]

$6x + 3y \equiv 8 \pmod{20}$ [2]

$$33x + 15y \equiv 21 \pmod{20} \qquad [1'] = [1] \times 3$$
$$30x + 15y \equiv 40 \pmod{20} \qquad [2'] = [2] \times 5$$

$$3x \equiv -19 \pmod{20} \qquad [3] = [1'] - [2']$$
$$3x \equiv -19 + 20 = 1 \qquad [3']$$
$$21x \equiv 7 \qquad [3'] \times 7$$
$$21x - 20x \equiv 7$$
$$x \equiv 7 \pmod{20} \qquad [4]$$

$$6x \equiv 42 \pmod{20} \qquad [4'] = [4] \times 6$$
$$\therefore 42 \equiv 8 - 3y \pmod{20} \qquad [4'] \text{ in } [2]$$
$$-3y \equiv 34 - 20 = 14 \qquad [4'']$$
$$-21y \equiv 98 \qquad [5] = [4''] \times 7$$
$$-21y + 20y \equiv 98 - 5 \cdot 20$$
$$-y \equiv -2$$
$$y \equiv 2$$

$$\therefore \quad x \equiv 7 \pmod{20}$$
$$y \equiv 2 \pmod{20}$$