MTH 4436 Homework Set 4.4; p. 82 #1, 3, 4, 8, 9, 10, 17, 19, 20

Fall 2016

Pat Rossi Name ______________________

1. Solve the following Linear Congruences:

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

   This is of the form $ax \equiv b \pmod{n}$,which has a solution exactly when $d|b$, where $d = \gcd(a, n)$. Furthermore, if $d|b$, then there a d mutually incongruent solutions $\bmod n$.

   $d = \gcd(25, 29) = 1$ which divides 15.
   Hence, there exists $d = \gcd(25, 29) = 1$ solution.

   Our next step is to find a particular solution.

   1. 1. Divide the *entire congruence* through by $\gcd(25, 29) = 1$.
      Done!
      2. Multiply both sides of the congruence by a number that will make the left hand side congruent to $1 \cdot x \pmod{29}$.
      Observe: $7 \cdot 25x \equiv 7 \cdot 15 \pmod{29} \Rightarrow 175x \equiv 105 \pmod{29} \Rightarrow 1x \equiv 18 \pmod{29}$.
      i.e., $x = 18$ is our particular solution.
      Since there is only one solution, we need not look for others.
      $x = 18$.

   (b) $5x \equiv 2 \pmod{26}$
   $d = \gcd(a, b) = \gcd(5, 26) = 1$ which divides b (i.e., divides 2), hence, there exists a solution.
   Our next step is to find a particular solution.

   1. 1. Divide the *entire congruence* through by $\gcd(5, 26) = 1$.
      Done!
      2. Multiply both sides of the congruence by a number that will make the left hand side congruent to $1 \cdot x \pmod{26}$.
      Observe: $5 \cdot 5x \equiv 5 \cdot 2 \pmod{26} \Rightarrow 25x \equiv 10 \pmod{26} \Rightarrow -1x \equiv 10 \pmod{26}$.
      Multiplying both sides by (-1) , we have:
      $1x \equiv -10 \pmod{26} \Rightarrow 1x \equiv 16 \pmod{26}$.
      i.e., $x = 16$ is our particular solution.
      Since there is only one solution, we need not look for others.
      $x = 16$.

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

$\gcd(6, 21) = 3$ which divides 15, hence, there exist $\gcd(6, 21) = 3$ solutions.

Our next step is to find a particular solution.

1. 1. Divide the *entire congruence* through by $\gcd(6, 21) = 3$.
   $\Rightarrow 2x \equiv 5 \pmod 7$
   Note: Since $\gcd(2, 7) = 1$, there is exactly one solution to this new congruence. It will be a particular solution to the original congruence.
   2. Multiply both sides of the new congruence by a number that will make the left hand side congruent to $1 \cdot x \pmod 7$.
   Observe: $4 \cdot 2x \equiv 4 \cdot 5 \pmod 7 \Rightarrow 8x \equiv 20 \pmod 7 \Rightarrow 1x \equiv 6 \pmod 7$.
   i.e., $x = 6$ is our particular solution.
   Recall that given a particular solution of x_0, and $\gcd(a, n) = d$, the other solutions are of the form: $x = x_0 + \left(\frac{n}{d}\right) t \pmod{21}$ for $t = 0, 1, 2, \ldots, d-1$.
   $x = 6 + \left(\frac{21}{3}\right)(0) = 6$
   $x = 6 + \left(\frac{21}{3}\right)(1) = 13$
   $x = 6 + \left(\frac{21}{3}\right)(2) = 20$
   The solutions are 6, 13, 20.

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

$\gcd(36, 102) = 6$ which DOES NOT divide 8, hence, there exist NO solutions.

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

$\gcd(34, 98) = 2$ which divides 60, hence, there exist $\gcd(34, 98) = 2$ solutions.

Our next step is to find a particular solution.

1. 1. Divide the *entire congruence* through by $\gcd(34, 98) = 2$.
   $\Rightarrow 17x \equiv 30 \pmod{49}$
   Note: Since $\gcd(17, 49) = 1$, there is exactly one solution to this new congruence. It will be a particular solution to the original congruence.
   2. Multiply both sides of the new congruence by a number that will make the left hand side congruent to $1 \cdot x \pmod{49}$.
   Observe: $3 \cdot 17x \equiv 3 \cdot 30 \pmod{49} \Rightarrow 51x \equiv 90 \pmod{49}$
   $\Rightarrow 2x \equiv 41 \pmod{49} \Rightarrow 2x \equiv (-8) \pmod{49} \Rightarrow 24 \cdot 2x \equiv 24 \cdot (-8) \pmod{49}$
   $\Rightarrow 48x \equiv -192 \pmod{49} \Rightarrow (-1)\,x \equiv 4 \pmod{49} \Rightarrow 1x \equiv -4 \pmod{49}$
   $\Rightarrow 1x \equiv 45 \pmod{49}$.
   i.e., $x = 45$ is a particular solution.
   Recall that given a particular solution of x_0, and $\gcd(a, n) = d$, the other solutions are of the form: $x = x_0 + \left(\frac{n}{d}\right) t$ for $t = 0, 1, 2, \ldots, d-1$.
   $x = 45 + \left(\frac{98}{2}\right)(0) = 45$
   $x = 45 + \left(\frac{98}{2}\right)(1) = 94$
   The solutions are 45, 94.

(f) $140x \equiv 133 \pmod{301}$ (hint: $\gcd(140, 301) = 7$)

$\gcd(140, 301) = 7$ which divides 133, hence, there exist $\gcd(140, 301) = 7$ solutions.

To make things easier for ourselves, we will apply Thm 4.3, which says: If $ca \equiv cb \pmod{n}$, then $a \equiv b \left(\bmod \frac{n}{d}\right)$, where $d = \gcd(c, n)$.

In order to apply Thm 4.3, we'll have to re-write the congruence such that $\gcd(140, 301)$ appears explicitly as a factor on each side.

Thus, our congruence becomes:

$(7)(20)x \equiv (7)(19) \left(\bmod \frac{301}{7}\right)$

i.e., $(7)(20)x \equiv (7)(19) \pmod{43}$

Applying Thm 4.3, we have:

$20x \equiv 19 \pmod{43}$

At this point, a particular solution is not obvious (at least not to me!). So we'll do some more manipulation.

$20x \equiv 19 \pmod{43} \Rightarrow 20x \equiv -24 \pmod{43} \Rightarrow (4)(5)x \equiv (4)(-6) \pmod{43}$ Since 43 is prime and $43 \nmid 4$, we can cancel 4 on each side. $\Rightarrow 5x \equiv -6 \pmod{43} \Rightarrow$

$5x \equiv 37 \pmod{43} \Rightarrow 5x \equiv 80 \pmod{43} \Rightarrow x = 16$

i.e., $x = 16$ is our particular solution of the linear congruence $20x \equiv 19 \pmod{43}$.

$x = 16$ is also a particular solution of the original linear congruence $140x \equiv 133 \pmod{301}$

All other solutions are of the form: $x = x_0 + \frac{tn}{d}; \qquad t = 0, 1, \ldots, d-1$

All other solutions are of the form: $x = 16 + \frac{301t}{7}; \qquad t = 0, 1, \ldots, 6$

i.e., $x = 16 + 43t; \qquad t = 0, 1, \ldots, 6$

Our solutions are: $x = 16, 59, 102, 145, 188, 231, 274$

3. Find all solutions of the linear congruence $3x - 7y \equiv 11 \pmod{13}$

   We can rewrite this congruence as $3x \equiv (11 + 7y) \pmod{13}$

   Since $\gcd(3, 13) = 1$, there is a unique solution - for each value of $7y \bmod 13$

   (i.e., there is a unique solution for $y = 0, 1, 2, 3, \ldots, 12$)

   For $y = 0$, we have: $3x \equiv 11 \pmod{13} \Rightarrow 3x \equiv 24 \pmod{13} \Rightarrow x = 8$

   i.e., $x_0 = 8$; $y_0 = 0$ is a particular solution.

   How do we get all other solutions?

   Recall that we have a unique solution for $y = 0, 1, 2, 3, \ldots, 12$.

   Observe that if $y_1 = y_0 + 1$, then we have:

   $$3x_1 \equiv (11 + 7y_1) \pmod{13} \Rightarrow 3x_1 \equiv (11 + 7(y_0 + 1)) \pmod{13}$$

   $$\Rightarrow 3x_1 \equiv (11 + 7y_0 + 7) \pmod{13} \Rightarrow 3x_1 - 7 \equiv (11 + 7y_0) \pmod{13}$$

   $$\Rightarrow 3x_1 + 6 \equiv (11 + 7y_0) \pmod{13} \Rightarrow 3\underbrace{(x_1 + 2)}_{x_0} \equiv (11 + 7y_0) \pmod{13}$$

   $$\Rightarrow x_0 = x_1 + 2 \Rightarrow x_1 = x_0 - 2$$

   i.e., $y_1 = y_0 + 1 \Rightarrow x_1 = x_0 - 2$

   Inductively: $y_{i+1} = y_i + 1 \Rightarrow x_{i+1} = x_i - 2$

   Consequently, given the particular solution $x_0 = 8$; $y_0 = 0$, all other solutions are of the form:

   $$x_i = x_0 - 2i; \quad y_i = y_0 + i; \quad \text{for } i = 0, 1, 2, 3, \ldots, 12$$

   i.e., all other solutions are of the form: $x_i = 8 - 2i; \quad y_i = i \quad \text{for } i = 0, 1, 2, 3, \ldots, 12$

4. Solve each of the following sets of simultaneous congruences:

(a) $x \equiv 1 \pmod 3$; $x \equiv 2 \pmod 5$; $x \equiv 3 \pmod 7$

Since $3, 5, 7$ are pair-wise relatively prime, the system of congruences has a unique solution mod$(3 \cdot 5 \cdot 7)$. (i.e., our solution is unique $\bmod (105)$.

To get the solution:

1. Define $n = n_1 n_2 \ldots n_r$

   i.e., $n = 3 \cdot 5 \cdot 7 = 105$

   Define $N_k = \frac{n}{n_k}$ for $k = 1, 2, \ldots, r$.

   $N_1 = \frac{105}{3} = 35$

   $N_2 = \frac{105}{5} = 21$

   $N_3 = \frac{105}{7} = 15$

2. Solve the related congruences:

$$\begin{aligned} N_1 x_1 &\equiv 1 \pmod{n_1} \\ N_2 x_2 &\equiv 1 \pmod{n_2} \\ N_3 x_3 &\equiv 1 \pmod{n_3} \\ \vdots \quad &\vdots \quad \quad \vdots \\ N_r x_r &\equiv 1 \pmod{n_r} \end{aligned}$$

   i.e., solve the congruences:

$$\begin{aligned} 35 x_1 &\equiv 1 \pmod 3 \\ 21 x_2 &\equiv 1 \pmod 5 \\ 15 x_3 &\equiv 1 \pmod 7 \end{aligned}$$

   This yields: $x_1 = 2$; $x_2 = 1$; $x_3 = 1$

3. Our solution is the number $x \equiv (a_1 N_1 x_1 + a_2 N_2 x_2 + \ldots + a_r N_r x_r) \pmod{(n)}$.

   Our solution is the number $x \equiv (1 \cdot 35 \cdot 2 + 2 \cdot 21 \cdot 1 + 3 \cdot 15 \cdot 1) \pmod{(105)}$

   $\equiv 157 \pmod{(105)} \equiv 52 \pmod{(105)}$.

   i.e., $x = 52$

   Check: $\begin{aligned} 52 &\equiv 1 \pmod 3 \quad \text{Check!} \\ 52 &\equiv 2 \pmod 5 \quad \text{Check!} \\ 52 &\equiv 3 \pmod 7 \quad \text{Check!} \end{aligned}$

(b) $x \equiv 5 \pmod{11}$; $x \equiv 14 \pmod{29}$; $x \equiv 15 \pmod{31}$

Since $11, 29, 31$ are pair-wise relatively prime, the system of congruences has a unique solution $\mathrm{mod}(11 \cdot 29 \cdot 31)$. (i.e., our solution is unique $\mathrm{mod}\,(9889)$.

To get the solution:

1. Define $n = n_1 n_2 \ldots n_r$

   i.e., $n = 11 \cdot 29 \cdot 31 = 9889$

   Define $N_k = \frac{n}{n_k}$ for $k = 1, 2, \ldots, r$.

   $N_1 = \frac{9889}{11} = 899$

   $N_2 = \frac{9889}{29} = 341$

   $N_3 = \frac{9889}{31} = 319$

2. Solve the related congruences:

$$\begin{array}{rcl} N_1 x_1 & \equiv & 1 \pmod{n_1} \\ N_2 x_2 & \equiv & 1 \pmod{n_2} \\ N_3 x_3 & \equiv & 1 \pmod{n_3} \\ \vdots & \vdots & \vdots \\ N_r x_r & \equiv & 1 \pmod{n_r} \end{array}$$

   i.e., solve the congruences:

$$\begin{array}{rcl} 899 x_1 & \equiv & 1 \pmod{11} \\ 341 x_2 & \equiv & 1 \pmod{29} \\ 319 x_3 & \equiv & 1 \pmod{31} \end{array}$$

   This yields: $x_1 = 7$; $x_2 = 4$; $x_3 = 7$

3. Our solution is the number $x \equiv (a_1 N_1 x_1 + a_2 N_2 x_2 + \ldots + a_r N_r x_r) \pmod{(n)}$.

   Our solution is the number:

   $x \equiv (5 \cdot 899 \cdot 7 + 14 \cdot 341 \cdot 4 + 15 \cdot 319 \cdot 7) \pmod{(9889)} \equiv$

   $84,056 \pmod{(9889)} \equiv 4944 \pmod{(9889)}$.

   i.e., $x = 4944$

   Check: $4944 \equiv 5 \pmod{11}$ Check!
   $4944 \equiv 14 \pmod{29}$ Check!
   $4944 \equiv 15 \pmod{31}$ Check!

(c) $x \equiv 5 \pmod{6}$; $x \equiv 4 \pmod{11}$; $x \equiv 3 \pmod{17}$

Since $6, 11, 17$ are pair-wise relatively prime, the system of congruences has a unique solution $\text{mod}(6 \cdot 11 \cdot 17)$. (i.e., our solution is unique $\text{mod}\,(1122)$.

To get the solution:

1. Define $n = n_1 n_2 \dots n_r$

   i.e., $n = 6 \cdot 11 \cdot 17 = 1122$

   Define $N_k = \frac{n}{n_k}$ for $k = 1, 2, \dots, r$.

   $N_1 = \frac{1122}{6} = 187$

   $N_2 = \frac{1122}{11} = 102$

   $N_3 = \frac{1122}{17} = 66$

2. Solve the related congruences:

$$\begin{array}{rcl} N_1 x_1 & \equiv & 1 \pmod{n_1} \\ N_2 x_2 & \equiv & 1 \pmod{n_2} \\ N_3 x_3 & \equiv & 1 \pmod{n_3} \\ \vdots & \vdots & \vdots \\ N_r x_r & \equiv & 1 \pmod{n_r} \end{array}$$

   i.e., solve the congruences:

$$\begin{array}{rcl} 187 x_1 & \equiv & 1 \pmod{6} \\ 102 x_2 & \equiv & 1 \pmod{11} \\ 66 x_3 & \equiv & 1 \pmod{17} \end{array}$$

   This yields: $x_1 = 1$; $x_2 = 4$; $x_3 = 8$

3. Our solution is the number $x \equiv (a_1 N_1 x_1 + a_2 N_2 x_2 + \dots + a_r N_r x_r) \pmod{(n)}$.

   Our solution is the number $x \equiv (5 \cdot 187 \cdot 1 + 4 \cdot 102 \cdot 4 + 3 \cdot 66 \cdot 8) \pmod{(1122)} \equiv$

   $4151 \pmod{(1122)} \equiv 785 \pmod{(1122)}$.

   i.e., $x = 785$

   Check:
$$\begin{array}{rcll} 785 & \equiv & 5 \pmod{6} & \text{Check!} \\ 785 & \equiv & 4 \pmod{11} & \text{Check!} \\ 785 & \equiv & 3 \pmod{17} & \text{Check!} \end{array}$$

(d) $2x \equiv 1 \pmod 5$; $3x \equiv 9 \pmod 6$; $4x \equiv 1 \pmod 7$; $5x \equiv 9 \pmod{11}$

Same as: $2x \equiv 1 \pmod 5$; $3x \equiv 3 \pmod 6$; $4x \equiv 1 \pmod 7$; $5x \equiv 9 \pmod{11}$

Since $1, 6, 7, 11$ are pair-wise relatively prime, the system of congruences has a unique solution mod$(5 \cdot 6 \cdot 7 \cdot 11)$. (i.e., our solution is unique $\bmod{(2310)}$.)

However, our Theorem and algorithm requires congruences of the form:

$$x \equiv a_1 \pmod n$$

So let's convert our congruences to that form:

$\boxed{2x \equiv 1 \pmod 5} \Rightarrow 3 \cdot 2x \equiv 3 \cdot 1 \pmod 5 \Rightarrow 6x \equiv 3 \pmod 5 \Rightarrow x \equiv 3 \pmod 5$

i.e., $x \equiv 3 \pmod 5$

$\boxed{3x \equiv 3 \pmod 6}$ Since, $\gcd(3, 6) \neq 1,$ we won't be able to get a congruence of the form $x \equiv a_1 \pmod n$, just by multiplying both sides by "the right number." (Try it and see!)

Note also that since $\gcd(3, 6) = 3$, the congruence $3x \equiv 3 \pmod 6$ has *three* "proper" solutions.

To get a congruence of the form $x \equiv a_1 \pmod n$, we can divide the entire congruence by 3. The unique solution of the new congruence will also be a solution of the original congruence $3x \equiv 3 \pmod 6$.

$\frac{1}{3} \cdot 3x \equiv \frac{1}{3} \cdot 3 \left(\bmod \frac{1}{3} \cdot 6\right) \Rightarrow x \equiv 1 \pmod 2$

i.e., $x \equiv 1 \pmod 2$

$\boxed{4x \equiv 1 \pmod 7} \Rightarrow 2 \cdot 4x \equiv 2 \cdot 1 \pmod 7 \Rightarrow 8x \equiv 2 \pmod 7 \Rightarrow x \equiv 2 \pmod 7$

i.e., $x \equiv 2 \pmod 7$

$\boxed{5x \equiv 9 \pmod{11}} \Rightarrow 9 \cdot 5x \equiv 9 \cdot 9 \pmod{11} \Rightarrow 45x \equiv 81 \pmod{11} \Rightarrow x \equiv 4 \pmod{11}$

i.e., $x \equiv 4 \pmod{11}$

To get the solution:

1. Define $n = n_1 n_2 \dots n_r$

   i.e., $n = 5 \cdot 2 \cdot 7 \cdot 11 = 770$

   Define $N_k = \frac{n}{n_k}$ for $k = 1, 2, \dots, r$.

   $N_1 = \frac{770}{5} = 154$

   $N_2 = \frac{770}{2} = 385$

   $N_3 = \frac{770}{7} = 110$

   $N_4 = \frac{770}{11} = 70$

2. Solve the related congruences:

$$\begin{array}{rcl} N_1 x_1 & \equiv & 1 \,(\mathrm{mod}\, n_1) \\ N_2 x_2 & \equiv & 1 \,(\mathrm{mod}\, n_2) \\ N_3 x_3 & \equiv & 1 \,(\mathrm{mod}\, n_3) \\ \vdots & \vdots & \vdots \\ N_r x_r & \equiv & 1 \,(\mathrm{mod}\, n_r) \end{array}$$

   i.e., solve the congruences:

$$\begin{array}{rcl} 154 x_1 & \equiv & 1 \,(\mathrm{mod}\, 5) \\ 385 x_2 & \equiv & 1 \,(\mathrm{mod}\, 2) \\ 110 x_3 & \equiv & 1 \,(\mathrm{mod}\, 7) \\ 70 x_4 & \equiv & 1 \,(\mathrm{mod}\, 11) \end{array}$$

   This yields: $x_1 = 4$; $x_2 = 1$; $x_3 = 3$; $x_4 = 3$

3. Our solution is the number $x \equiv (a_1 N_1 x_1 + a_2 N_2 x_2 + \ldots + a_r N_r x_r) \,(\mathrm{mod}\,(n))$.

   Our solution is the number

   $x \equiv (3 \cdot 154 \cdot 4 + 1 \cdot 385 \cdot 1 + 2 \cdot 110 \cdot 3 + 4 \cdot 70 \cdot 3) \,(\mathrm{mod}\,(770)) \equiv$

   $3733 \,(\mathrm{mod}\,(770)) \equiv 653 \,(\mathrm{mod}\,(770))$.

   i.e., $x = 653$

   Check (The original system):
$$\begin{array}{rcll} 2\,(653) & \equiv & 1 \,(\mathrm{mod}\, 5) & \text{Check!} \\ 3\,(653) & \equiv & 9 \,(\mathrm{mod}\, 6) & \text{Check!} \\ 4\,(653) & \equiv & 1 \,(\mathrm{mod}\, 7) & \text{Check!} \\ 5\,(653) & \equiv & 9 \,(\mathrm{mod}\, 11) & \text{Check!} \end{array}$$

8. When eggs in a basket are removed 2, 3, 4, 5, 6, at a time, there remain, respectively, 1, 2, 3, 4, 5 eggs. When they are taken out 7 at a time, none are left over. Find the smallest number of eggs that could have been in the basket.

   This situation yields the system of congruences:

$$\begin{aligned} x &\equiv 1 \pmod{2} \\ x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{4} \\ x &\equiv 4 \pmod{5} \\ x &\equiv 5 \pmod{6} \\ x &\equiv 0 \pmod{7} \end{aligned}$$

   To solve this, we will use the Chinese Remainder Theorem. However, there IS a catch. Given a system of congruences of the form $x \equiv a_i \pmod{n_i}$, the Chinese Remainder Theorem only applies when the n_i's are pairwise relatively prime. This is not the case here.

   To remedy this situation, we recognize that if the original system has a solution, then the related system:

$$\begin{aligned} x &\equiv 1 \pmod{2} \\ x &\equiv 2 \pmod{3} \\ x &\equiv 4 \pmod{5} \\ x &\equiv 0 \pmod{7} \end{aligned}$$

   must have the same solution. The "related system" above is such that all of the n_i's are pairwise relatively prime. Thus, the Chinese Remainder Theorem can be used to solve this "related system." If the original system has a solution (at this point, we're not sure that it does), it must be the exact same solution as that of the "related system." To get the solution to the "related system":

   (a) 1. Define $n = n_1 n_2 \ldots n_r$

   i.e., $n = 2 \cdot 3 \cdot 5 \cdot 7 = 210$

   Define $N_k = \frac{n}{n_k}$ for $k = 1, 2, \ldots, 4$.

   $N_1 = \frac{210}{2} = 105$

   $N_2 = \frac{210}{3} = 70$

   $N_4 = \frac{210}{5} = 42$

   $N_6 = \frac{210}{7} = 30$

   2. Solve the related congruences:

$$\begin{aligned} N_1 x_1 &\equiv 1 \pmod{n_1} \\ N_2 x_2 &\equiv 1 \pmod{n_2} \\ N_4 x_4 &\equiv 1 \pmod{n_4} \\ \vdots \quad &\ \vdots \qquad \vdots \\ N_6 x_6 &\equiv 1 \pmod{n_6} \end{aligned}$$

i.e., solve the congruences:

$$\begin{aligned}105x_1 &\equiv 1 \pmod 2\\ 70x_2 &\equiv 1 \pmod 3\\ 42x_3 &\equiv 1 \pmod 5\\ 30x_4 &\equiv 1 \pmod 7\end{aligned}$$

This yields: $x_1 = 1$; $x_2 = 1$; $x_4 = 3$; $x_6 = 4$

3. Our solution is the number $x \equiv (a_1N_1x_1 + a_2N_2x_2 + a_4N_4x_4 + a_6N_6x_6) \pmod{(n)}$.

   Our solution is the number

   $x \equiv (1 \cdot 105 \cdot 1 + 2 \cdot 70 \cdot 1 + 4 \cdot 42 \cdot 3 + 0 \cdot 30 \cdot 4) \pmod{(210)} \equiv$

   $749 \pmod{(210)} \equiv 119 \pmod{(210)}$.

   i.e., $x = 119$

   Check (The original system):

$$\begin{aligned}119 &\equiv 1 \pmod 2 \quad \textbf{Check!}\\ 119 &\equiv 2 \pmod 3 \quad \textbf{Check!}\\ 119 &\equiv 3 \pmod 4 \quad \textbf{Check!}\\ 119 &\equiv 4 \pmod 5 \quad \textbf{Check!}\\ 119 &\equiv 5 \pmod 6 \quad \textbf{Check!}\\ 119 &\equiv 0 \pmod 7 \quad \textbf{Check!}\end{aligned}$$

9. The basket-of-eggs problem is often phrased in the following form: 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 they are removed 7 at a time. Find the smallest number of eggs that could have been in the basket.

   This situation yields the system of congruences:

$$
\begin{aligned}
x &\equiv 1 \pmod{2} \\
x &\equiv 1 \pmod{3} \\
x &\equiv 1 \pmod{4} \\
x &\equiv 1 \pmod{5} \\
x &\equiv 1 \pmod{6} \\
x &\equiv 0 \pmod{7}
\end{aligned}
$$

   To solve this, we will use the Chinese Remainder Theorem. Again, however, there is a catch. Given a system of congruences of the form $x \equiv a_i \pmod{n_i}$, the Chinese Remainder Theorem only applies when the n_i's are pairwise relatively prime. This is not the case here.

   To remedy this situation, we recognize that if the original system has a solution, then the related system:

$$
\begin{aligned}
x &\equiv 1 \pmod{2} \\
x &\equiv 1 \pmod{3} \\
x &\equiv 1 \pmod{5} \\
x &\equiv 0 \pmod{7}
\end{aligned}
$$

   must have the same solution. The "related system" above is such that all of the n_i's are pairwise relatively prime. Thus, the Chinese Remainder Theorem can be used to solve this "related system." If the original system has a solution (at this point, we're not sure that it does), it must be the exact same solution as that of the "related system." To get the solution to the "related system":

   (a) 1. Define $n = n_1 n_2 \dots n_r$

   i.e., $n = 2 \cdot 3 \cdot 5 \cdot 7 = 210$

   Define $N_k = \frac{n}{n_k}$ for $k = 1, 2, \dots, 4$.

   $N_1 = \frac{210}{2} = 105$

   $N_2 = \frac{210}{3} = 70$

   $N_4 = \frac{210}{5} = 42$

   $N_6 = \frac{210}{7} = 30$

2. Solve the related congruences:

$$\begin{array}{rcl} N_1x_1 & \equiv & 1\,(\mathrm{mod}\,n_1) \\ N_2x_2 & \equiv & 1\,(\mathrm{mod}\,n_2) \\ N_4x_4 & \equiv & 1\,(\mathrm{mod}\,n_4) \\ \vdots & \vdots & \vdots \\ N_6x_6 & \equiv & 1\,(\mathrm{mod}\,n_6) \end{array}$$

i.e., solve the congruences:

$$\begin{array}{rcl} 105x_1 & \equiv & 1\,(\mathrm{mod}\,2) \\ 70x_2 & \equiv & 1\,(\mathrm{mod}\,3) \\ 42x_4 & \equiv & 1\,(\mathrm{mod}\,5) \\ 30x_6 & \equiv & 1\,(\mathrm{mod}\,7) \end{array}$$

This yields: $x_1 = 1$; $x_2 = 1$; $x_4 = 3$; $x_6 = 4$

3. Our solution is the number $x \equiv (a_1N_1x_1 + a_2N_2x_2 + a_4N_4x_4 + a_6N_6x_6)\,(\mathrm{mod}\,(n))$.

The solution to the "related system" is the number

$x \equiv (1 \cdot 105 \cdot 1 + 1 \cdot 70 \cdot 1 + 1 \cdot 42 \cdot 3 + 0 \cdot 30 \cdot 4)\,(\mathrm{mod}\,(210)) \equiv (4)\,(6)\,(210)$:

5040
301 (mod (210)) ≡ 91 (mod (210)).

i.e., $x = 91$

Check (The original system):

$$\begin{array}{rcll} 91 & \equiv & 1\,(\mathrm{mod}\,2) & \textbf{Check!} \\ 91 & \equiv & 1\,(\mathrm{mod}\,3) & \textbf{Check!} \\ 91 & \equiv & 1\,(\mathrm{mod}\,4) & \textbf{Doesn't Check} \\ 91 & \equiv & 1\,(\mathrm{mod}\,5) & \textbf{Check!} \\ 91 & \equiv & 1\,(\mathrm{mod}\,6) & \textbf{Check!} \\ 91 & \equiv & 0\,(\mathrm{mod}\,7) & \textbf{Check!} \end{array}$$

Houston - we have a problem!

Here's the problem: Our solution is the solution to the "related system."

$x \equiv (1 \cdot 105 \cdot 1 + 1 \cdot 70 \cdot 1 + 1 \cdot 42 \cdot 3 + 0 \cdot 30 \cdot 4) \,(\mathrm{mod}\,(210))\,,$ where $210 = n_1 n_2 n_4 n_6$

In order to be sure that our solution is the solution to the "original system," we should compute:

$x \equiv (1 \cdot 105 \cdot 1 + 1 \cdot 70 \cdot 1 + 1 \cdot 42 \cdot 3 + 0 \cdot 30 \cdot 4) \,(\mathrm{mod}\,(n))\,,$

where $n = n_1 n_2 n_3 n_4 n_5 n_6 = 5040$

Thus, $x \equiv (1 \cdot 105 \cdot 1 + 1 \cdot 70 \cdot 1 + 1 \cdot 42 \cdot 3 + 0 \cdot 30 \cdot 4) \,(\mathrm{mod}\,(5040))$

$\equiv 301 \,(\mathrm{mod}\,(5040))$

Check (The original system):

$$\begin{array}{rcll} 301 & \equiv & 1 \pmod 2 & \textbf{Check!} \\ 301 & \equiv & 1 \pmod 3 & \textbf{Check!} \\ 301 & \equiv & 1 \pmod 4 & \textbf{Check} \\ 301 & \equiv & 1 \pmod 5 & \textbf{Check!} \\ 301 & \equiv & 1 \pmod 6 & \textbf{Check!} \\ 301 & \equiv & 0 \pmod 7 & \textbf{Check!} \end{array}$$

10. A band of 17 pirates stole a bag 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, another argument developed in which another pirate was killed. But now the total fortune was evenly distributed among the survivors. What is the least number of coins that could have been stolen?

    Let x be the number of coins. Then

$$x \equiv 3 \pmod{17}$$
$$x \equiv 10 \pmod{16}$$
$$x \equiv 0 \pmod{15}$$

    To solve this, we will use the Chinese Remainder Theorem. Here, $n_1 = 17$, $n_2 = 16$, $n_3 = 15$, so the n_i 's are pairwise relatively prime.

    (a) 1. Define $n = n_1 n_2 \ldots n_r$

    i.e., $n = 17 \cdot 16 \cdot 15 = 4080$

    Define $N_k = \frac{n}{n_k}$ for $k = 1, 2, \ldots, 4$.

    $N_1 = \frac{4080}{17} = 240$

    $N_2 = \frac{4080}{16} = 255$

    $N_3 = \frac{4080}{15} = 272$

    2. Solve the related congruences:

$$\begin{aligned} N_1 x_1 &\equiv 1 \pmod{n_1} \\ N_2 x_2 &\equiv 1 \pmod{n_2} \\ N_3 x_3 &\equiv 1 \pmod{n_3} \end{aligned}$$

    i.e., solve the congruences:

$$\begin{aligned} 240 x_1 &\equiv 1 \pmod{17} \\ 255 x_2 &\equiv 1 \pmod{16} \\ 272 x_3 &\equiv 1 \pmod{15} \end{aligned}$$

    This yields: $x_1 = 9$; $x_2 = 15$; $x_3 = 8$;

3. Our solution is the number $x \equiv (a_1N_1x_1 + a_2N_2x_2 + a_3N_3x_3) \pmod{(n)}$.

Our solution is the number

$x \equiv (3 \cdot 240 \cdot 9 + 10 \cdot 255 \cdot 15 + 0 \cdot 272 \cdot 8) \pmod{(4080)} \equiv$

$44,730 \pmod{(4080)} \equiv 3930 \pmod{(4080)}$.

i.e., $x = 3930$

Check (The original system):

$$\begin{aligned} 3930 &\equiv 3 \pmod{17} && \textbf{Check!} \\ 3930 &\equiv 10 \pmod{16} && \textbf{Check!} \\ 3930 &\equiv 0 \pmod{15} && \textbf{Check!} \end{aligned}$$

17. Find the solutions of the system of congruences:

$$\begin{aligned} 3x + 4y &\equiv 5 \pmod{13} \\ 2x + 5y &\equiv 7 \pmod{13} \end{aligned}$$

First, let's see if this system actually HAS a solution.

The system

$$\begin{aligned} ax + by &\equiv r \pmod{n} \\ cx + dy &\equiv s \pmod{n} \end{aligned}$$

has a a unique solution exactly when $\gcd(ad - bc, n) = 1$.

Check: $\gcd((3)(5) - (2)(4), 13) = \gcd(7, 13) = 1$

Hence, the system has a unique solution.

Multiply the first congruence by d and the second congruence by b.

$$\begin{aligned} 3 \cdot 5x + 4 \cdot 5y &\equiv 5 \cdot 5 \pmod{13} \\ 2 \cdot 4x + 5 \cdot 4y &\equiv 7 \cdot 4 \pmod{13} \end{aligned}$$

Subtract the second congruence from the first, to eliminate y.

$$\begin{array}{rllcl} & 15x & + \ 20y & \equiv & 25 \pmod{13} \\ - & 8x & + \ 20y & \equiv & 28 \pmod{13} \\ \hline & 7x & & \equiv & -3 \pmod{13} \end{array}$$

i.e., $7x \equiv 10 \pmod{13}$

Multiply the equation $(ad-bc)\,x \equiv (dr-bs) \pmod{n}$ by an integer such that the left hand side becomes $x \pmod{n}$.

Observe: $2 \cdot 7x = 14x \equiv x \pmod{13}$

Thus, $2 \cdot 7x \equiv 2 \cdot 10 \pmod{13} \Rightarrow x \equiv 20 \pmod{13} \Rightarrow x \equiv 7 \pmod{13}$

Perform the analogous process to solve for y.

Multiply the first congruence by c and the second congruence by a.

$$\begin{aligned} 2 \cdot 3x + 2 \cdot 4y &\equiv 2 \cdot 5 \pmod{13} \\ 3 \cdot 2x + 3 \cdot 5y &\equiv 3 \cdot 7 \pmod{13} \end{aligned}$$

Subtract the second congruence from the first, to eliminate y.

$$\begin{array}{rrcrcl} & 6x & + & 8y & \equiv & 10 \pmod{13} \\ - & 6x & + & 15y & \equiv & 21 \pmod{13} \\ \hline & & - & 7y & \equiv & -11 \pmod{13} \end{array}$$

i.e., $7y \equiv 11 \pmod{13}$

$2 \cdot 7y \equiv 2 \cdot 11 \pmod{13} \Rightarrow 14y \equiv 22 \pmod{13} \Rightarrow y \equiv 9 \pmod{13}$

$\boxed{\text{The unique solution of the system is } (x,y) = (7,9)}$

19. Obtain the eight incongruent solutions of the linear congruence $3x + 4y \equiv 5 \pmod{8}$.

Observe: If we multiply the congruence by 2, we have:

$2 \cdot 3x + 2 \cdot 4y \equiv 2 \cdot 5 \pmod{8} \Rightarrow 6x + 8y \equiv 10 \pmod{8} \Rightarrow 6x + 8y \equiv 2 \pmod{8} \Rightarrow 6x \equiv 2 \pmod{8}$

This is of the form $ax \equiv b \pmod{n}$,which has a solution exactly when $d|b$, where $d = \gcd(a,n)$. Furthermore, if $d|b$, then there a d mutually incongruent solutions $\bmod n$.

Observe: $d = \gcd(6,8) = 2$

Furthermore: $2|10$ (i.e., $d|b$)

Hence, the congruence $6x \equiv 2 \pmod{8}$ has $d = 2$ mutually incongruent solutions mod 8, that are $\frac{n}{d} = 4$ units apart.

To find one of the solutions, observe that $6x \equiv 6x - 8x \pmod 8 \equiv -2x \pmod 8$.

Thus, $6x \equiv 2 \pmod 8$ is the same as $-2x \equiv 2 \pmod 8$, which yields $x = -1 \equiv 7 \pmod 8$ as a solution.

The other solution is $7 + \frac{n}{d} = 7 + 4 = 11 \equiv 3 \pmod 8$

i.e., The solutions are $x = 3$ and $x = 7$

Similarly, the solutions of the congruence $6x + 8y \equiv 2 \pmod 8$ are $x = 3$ and $x = 7$.

But what about y ? Since $8y \equiv 0 \pmod 8$ for *any* value of y, y can be anything (even a ham sandwich)!

But what about the *original* congruence $3x + 4y \equiv 5 \pmod 8$?

It is possible that when we multiplied both sides of the original congruence by 2, *that we introduced false solutions into the original congruence.*

How do we deal with this?

$\boxed{\text{For } x = 3}$

The original congruence becomes:

$3(3) + 4y \equiv 5 \pmod 8$ same as $4y \equiv -4 \pmod 8$ same as $4y \equiv 4 \pmod 8$.

This has $d = 4$ incongruent solutions spaced $\frac{n}{d} = 2$ units apart.

Since $y = 1$ is a solution, the solution set is $y = 1, 3, 5, 7$

$\boxed{\text{For } x = 7}$

The original congruence becomes:

$3(7) + 4y \equiv 5 \pmod 8$ same as $4y \equiv -16 \pmod 8$ same as $4y \equiv 0 \pmod 8$.

This has $d = 0$ incongruent solutions spaced $\frac{n}{4} = 4$ units apart.

Since $y = 0$ is a solution, the solution set is $y = 0, 4$.

The solution set to the congruence $3x + 4y \equiv 5 \pmod 8$ is $(3,1)$; $(3,3)$; $(3,5)$; $(3,7)$; $(7,0)$; $(7,4)$

20 a. Find the Solution for the system of congruences:

$5x + 3y \equiv 1 \pmod{7}$

$3x + 2y \equiv 4 \pmod{7}$

First, let's see if this system actually HAS a solution.

Recall: The system

$$\begin{aligned} ax + by &\equiv r \pmod{n} \\ cx + dy &\equiv s \pmod{n} \end{aligned}$$

has a a unique solution exactly when $\gcd(ad - bc, n) = 1$.

Check: $\gcd((5)(2) - (3)(3), 7) = \gcd(1, 7) = 1$

Hence, the system has a unique solution.

Multiply the first congruence by d and the second congruence by b.

$$\begin{aligned} 2 \cdot 5x + 2 \cdot 3y &\equiv 2 \cdot 1 \pmod{7} \\ 3 \cdot 3x + 3 \cdot 2y &\equiv 3 \cdot 4 \pmod{7} \end{aligned}$$

Subtract the second congruence from the first, to eliminate y.

$$\begin{array}{rrcrcl} & 10x & + & 6y & \equiv & 2 \pmod{7} \\ - & 9x & + & 6y & \equiv & 12 \pmod{7} \\ \hline & x & & & \equiv & -10 \pmod{7} \end{array}$$

i.e., $x \equiv 4 \pmod{7}$

Perform the analogous process to solve for y.

Multiply the first congruence by c and the second congruence by a.

$$\begin{aligned} 3 \cdot 5x + 3 \cdot 3y &\equiv 3 \cdot 1 \pmod{7} \\ 5 \cdot 3x + 5 \cdot 2y &\equiv 5 \cdot 4 \pmod{7} \end{aligned}$$

Subtract the second congruence from the first, to eliminate y.

$$\begin{array}{rrcrcl} & 15x & + & 9y & \equiv & 3 \pmod{7} \\ - & 15x & + & 10y & \equiv & 20 \pmod{7} \\ \hline & & - & y & \equiv & -17 \pmod{7} \end{array}$$

i.e., $y \equiv 17 \pmod{7} \equiv 3 \pmod{7}$

$$\boxed{\text{The unique solution of the system is } (x, y) = (4, 3)}$$

20 b. Find the Solution for the system of congruences:

$7x + 3y \equiv 6 \pmod{11}$

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

First, let's see if this system actually HAS a solution.

The system

$$\begin{aligned} ax + by &\equiv r \pmod{n} \\ cx + dy &\equiv s \pmod{n} \end{aligned}$$

has a a unique solution exactly when $\gcd(ad - bc, n) = 1$.

Check: $\gcd((7)(2) - (3)(4), 11) = \gcd(2, 11) = 1$

Hence, the system has a unique solution.

Multiply the first congruence by d and the second congruence by b.

$$\begin{aligned} 2 \cdot 7x + 2 \cdot 3y &\equiv 2 \cdot 6 \pmod{11} \\ 3 \cdot 4x + 3 \cdot 2y &\equiv 3 \cdot 9 \pmod{11} \end{aligned}$$

Subtract the second congruence from the first, to eliminate y.

$$\begin{array}{rrcrcl} & 14x & + & 6y & \equiv & 12 \pmod{11} \\ - & 12x & + & 6y & \equiv & 27 \pmod{11} \\ \hline & 2x & & & \equiv & -15 \pmod{11} \end{array}$$

i.e., $2x \equiv 7 \pmod{11}$

Multiply the equation $(ad - bc)\, x \equiv (dr - bs) \pmod{n}$ by an integer such that the left hand side becomes $x \pmod{n}$.

Observe: $6 \cdot 2x = 12x \equiv x \pmod{11}$

Thus, $6 \cdot 2x \equiv 6 \cdot 7 \pmod{11} \Rightarrow x \equiv 42 \pmod{11} \Rightarrow x \equiv 9 \pmod{11}$

Perform the analogous process to solve for y.

Multiply the first congruence by c and the second congruence by a.

$$\begin{aligned} 4 \cdot 7x + 4 \cdot 3y &\equiv 4 \cdot 6 \pmod{11} \\ 7 \cdot 4x + 7 \cdot 2y &\equiv 7 \cdot 9 \pmod{11} \end{aligned}$$

Subtract the second congruence from the first, to eliminate y.

$$\begin{array}{rrcrcl} & 28x & + & 12y & \equiv & 24 \pmod{11} \\ - & 28x & + & 14y & \equiv & 63 \pmod{11} \\ \hline & & - & 2y & \equiv & -39 \pmod{11} \end{array}$$

i.e., $9y \equiv 5 \pmod{11}$

Observe: $5 \cdot 9y = 45y \equiv y \pmod{11}$

$\Rightarrow 5 \cdot 9y \equiv 5 \cdot 5 \pmod{11} \Rightarrow y \equiv 25 \pmod{11} \Rightarrow y \equiv 3 \pmod{11}$

$$\boxed{\text{The unique solution of the system is } (x, y) = (9, 3)}$$

20 c. Find the Solution for the system of congruences:

$11x + 5y \equiv 7 \pmod{20}$

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

First, let's see if this system actually HAS a solution.

The system

$$\begin{aligned} ax + by &\equiv r \pmod{n} \\ cx + dy &\equiv s \pmod{n} \end{aligned}$$

has a a unique solution exactly when $\gcd(ad - bc, n) = 1$.

Check: $\gcd((3)(5) - (2)(4), 13) = \gcd(7, 13) = 1$

Hence, the system has a unique solution.

Multiply the first congruence by d and the second congruence by b.

$$\begin{aligned} 3 \cdot 5x + 4 \cdot 5y &\equiv 5 \cdot 5 \pmod{13} \\ 2 \cdot 4x + 5 \cdot 4y &\equiv 7 \cdot 4 \pmod{13} \end{aligned}$$

Subtract the second congruence from the first, to eliminate y.

$$\begin{array}{rlcrcl} & 15x & + & 20y & \equiv & 25 \pmod{13} \\ - & 8x & + & 20y & \equiv & 28 \pmod{13} \\ \hline & 7x & & & \equiv & -3 \pmod{13} \end{array}$$

i.e., $7x \equiv 10 \pmod{13}$

Multiply the equation $(ad - bc)x \equiv (dr - bs) \pmod{n}$ by an integer such that the left hand side becomes $x \pmod{n}$.

Observe: $2 \cdot 7x = 14x \equiv x \pmod{13}$

Thus, $2 \cdot 7x \equiv 2 \cdot 10 \pmod{13} \Rightarrow x \equiv 20 \pmod{13} \Rightarrow x \equiv 7 \pmod{13}$

Perform the analogous process to solve for y.

Multiply the first congruence by c and the second congruence by a.

$$\begin{aligned} 2 \cdot 3x + 2 \cdot 4y &\equiv 2 \cdot 5 \pmod{13} \\ 3 \cdot 2x + 3 \cdot 5y &\equiv 3 \cdot 7 \pmod{13} \end{aligned}$$

Subtract the second congruence from the first, to eliminate y.

$$\begin{array}{rlcrcl} & 6x & + & 8y & \equiv & 10 \pmod{13} \\ - & 6x & + & 15y & \equiv & 21 \pmod{13} \\ \hline & & - & 7y & \equiv & -11 \pmod{13} \end{array}$$

i.e., $7y \equiv 11 \pmod{13}$

$2 \cdot 7y \equiv 2 \cdot 11 \pmod{13} \Rightarrow 14y \equiv 22 \pmod{13} \Rightarrow y \equiv 9 \pmod{13}$

$$\boxed{\text{The unique solution of the system is } (x, y) = (7, 9)}$$