Math 255 - Spring 2018
Homework 9 Solutions

1. (a) i. We have that $(6, 9) = 3$ and 3 divides 3, so this congruence has 3 solutions. Dividing **everything** by 3, we get the equation $2x \equiv 1 \pmod 3$, which has unique solution $x \equiv 2 \pmod 3$. Lifting back up to $\mathbb{Z}/9\mathbb{Z}$, we get the three solutions $x \equiv 2, 5, 8 \pmod 9$.

   ii. We have $(10, 16) = 2$ and 2 divides 8, so this congruence has 2 solutions. Dividing **everything** by 2, we get the equation $5x \equiv 4 \pmod 8$, which has a unique solution. Since $5^{-1} \equiv 5 \pmod 8$, we multiply both sides by 5 and get $x \equiv 20 \equiv 4 \pmod 8$. Lifting to $\mathbb{Z}/16\mathbb{Z}$, we get the two solutions $x \equiv 4, 12 \pmod{16}$.

   (b) The six systems are (each system is on one line):

$$\begin{aligned}
x &\equiv 2 \pmod 9, \quad \text{and} \quad x \equiv 4 \pmod{16} \\
x &\equiv 5 \pmod 9, \quad \text{and} \quad x \equiv 4 \pmod{16} \\
x &\equiv 8 \pmod 9, \quad \text{and} \quad x \equiv 4 \pmod{16} \\
x &\equiv 2 \pmod 9, \quad \text{and} \quad x \equiv 12 \pmod{16} \\
x &\equiv 5 \pmod 9, \quad \text{and} \quad x \equiv 12 \pmod{16} \\
x &\equiv 8 \pmod 9, \quad \text{and} \quad x \equiv 12 \pmod{16}
\end{aligned}$$

For each of the six systems, we will have $M_1 = 16$ and $x_1 \equiv 16^{-1} \pmod 9$. Since $16 \equiv 7 \pmod 9$, we have $x_1 \equiv 7^{-1} \equiv 4 \pmod 9$. We will also have $M_2 = 9$ and $x_2 \equiv 9^{-1} \pmod{16}$. To find this, we can use the Euclidean algorithm (because no quick answer comes to mind):

$$\begin{aligned}
16 &= 9 + 7 \\
9 &= 7 + 2 \\
7 &= 3 \cdot 2 + 1,
\end{aligned}$$

so

$$\begin{aligned}
1 &= 7 - 3 \cdot 2 \\
&= 7 - 3 \cdot (9 - 7) = 4 \cdot 7 - 3 \cdot 9 \\
&= 4 \cdot (16 - 9) - 3 \cdot 9 = 4 \cdot 16 - 7 \cdot 9.
\end{aligned}$$

Therefore we have $9^{-1} \equiv -7 \equiv 9 \pmod{16}$. To keep our computation smaller, we will choose $x_2 \equiv -7 \pmod{16}$.

Now for each of the six cases we apply the CRT formula, noting that $M = m_1m_2 = 9 \cdot 16 = 144$,

$$x \equiv a_1x_1M_1 + a_2x_2M_2 \pmod{144}.$$

We get:

$$\begin{array}{llcll} x & \equiv 2\cdot 4\cdot 16 & + & 4\cdot(-7)\cdot 9 & \equiv 20 \pmod{144} \\ x & \equiv 5\cdot 4\cdot 16 & + & 4\cdot(-7)\cdot 9 & \equiv 68 \pmod{144} \\ x & \equiv 8\cdot 4\cdot 16 & + & 4\cdot(-7)\cdot 9 & \equiv 116 \pmod{144} \\ x & \equiv 2\cdot 4\cdot 16 & + & 12\cdot(-7)\cdot 9 & \equiv 92 \pmod{144} \\ x & \equiv 5\cdot 4\cdot 16 & + & 12\cdot(-7)\cdot 9 & \equiv 140 \pmod{144} \\ x & \equiv 8\cdot 4\cdot 16 & + & 12\cdot(-7)\cdot 9 & \equiv 44 \pmod{144}. \end{array}$$

The six solutions are therefore $x \equiv 20, 44, 68, 92, 112, 140 \pmod{144}$.

(c) The single system of congruences of the form stated in the problem is the system

$$x \equiv 2 \pmod 3, \quad \text{and} \quad x \equiv 4 \pmod 8.$$

For this CRT problem, $M_1 = 8$, $x_1 \equiv 8^{-1} \equiv 2^{-1} \equiv 2 \pmod 3$, $M_2 = 3$, and $x_2 \equiv 3^{-1} \equiv 3 \pmod 8$. The unique solution is therefore

$$x \equiv 2\cdot 2\cdot 8 + 4\cdot 3\cdot 3 \equiv 20 \pmod{24}.$$

Lifting to solution to $\mathbb{Z}/144\mathbb{Z}$, we get the six solutions

$$x \equiv 20, 44, 68, 92, 116, 140 \pmod{144}.$$

We see that these are the same!

2. (a) Here we have that the moduli as written as pairwise relatively prime, so we can just solve each equation separately and apply CRT.

In the first equation, $(4, 8) = 4$ and 4 divides 8, so we divide **everything** by 4 to get the equation $x \equiv 1 \pmod 2$, which is already solved.

In the second equation, we have $(5, 25) = 5$, but 5 does not divide 6. Therefore there is no solution, and the system does not have a solution.

(b) This problem has it all! The equations must each be solved separately, and once we are done with that the moduli might still not be pairwise relatively prime (they could become pairwise relatively prime if they get smaller in just the right way).

The first equation has $(2, 8) = 2$ and 2 divides 6, so we divide **everything** by 2 and get $x \equiv 3 \pmod 4$. The second equation has $(2, 9) = 1$, so there will be a unique solution. Since $2^{-1} \pmod 9$ exists, we can just divide both sides by 2 to get $x \equiv 4 \pmod 9$. Finally, $(3, 18) = 3$ and 3 is divisible by 3, so we divide **everything** by 3 and get $x \equiv 1 \pmod 6$.

Therefore the system we were given is equivalent to the system

$$x \equiv 3 \pmod 4, \quad x \equiv 4 \pmod 9, \quad x \equiv 1 \pmod 6.$$

As we feared, the moduli are not pairwise relatively prime; $(4, 6) = 2$ and $(6, 9) = 3$. So check if the equations are compatible.

We first consider the pair

$$x \equiv 3 \pmod{4}, \quad x \equiv 1 \pmod{6}.$$

Since $3 \equiv 1 \pmod{2}$, the equations are compatible. Therefore we proceed with our technique to get relatively prime moduli. The modulus of the first equation is already a power of a prime, so it cannot be split up further. The second equation splits into the two equations

$$x \equiv 1 \pmod{2}, \quad x \equiv 1 \pmod{3}.$$

Therefore the system $x \equiv 3 \pmod{4}$, $x \equiv 1 \pmod{6}$ is equivalent to the system

$$\begin{aligned} x &\equiv 3 \pmod{4} \\ x &\equiv 1 \pmod{2} \\ x &\equiv 1 \pmod{3}. \end{aligned}$$

Since 4 is a higher power of 2 than 2 is, the equation $x \equiv 1 \pmod{2}$ is implied by the equation $x \equiv 3 \pmod{4}$. So in the end, the equations $x \equiv 3 \pmod{4}$, $x \equiv 1 \pmod{6}$ are equivalent to the equations

$$x \equiv 3 \pmod{4}, \quad x \equiv 1 \pmod{3}.$$

This means that our original system is now equivalent to the system

$$x \equiv 3 \pmod{4}, \quad x \equiv 4 \pmod{9}, \quad x \equiv 1 \pmod{3}.$$

We still have $(3, 9) = 3$, so we now investigate the pair

$$x \equiv 4 \pmod{9}, \quad x \equiv 1 \pmod{3}.$$

Since $4 \equiv 1 \pmod{3}$, the equations are compatible. The two moduli are powers of prime, so we do not need to split them up; it suffices to notice that $x \equiv 1 \pmod{3}$ is implied by $x \equiv 4 \pmod{9}$, so we keep only $x \equiv 4 \pmod{9}$.
Therefore the whole system we were solving is equivalent to

$$x \equiv 3 \pmod{4}, \quad x \equiv 4 \pmod{9}.$$

We can finally do the CRT algorithm!
Here we have $M_1 = 9$, and $x_1 \equiv 9^{-1} \equiv 1^{-1} \equiv 1 \pmod{4}$; and also $M_2 = 4$ and $x_2 \equiv 4^{-1} \equiv -2 \equiv 7 \pmod{9}$. (Here we used as a trick that $4 \cdot 2 = 8 \equiv -1 \pmod{9}$.)
Therefore, finally we have

$$\begin{aligned} x &\equiv a_1 x_1 M_1 + a_2 x_2 M_2 \pmod{36} \\ &\equiv 3 \cdot 1 \cdot 9 + 4 \cdot (-2) \cdot 4 \pmod{36} \\ &\equiv 27 - 32 \pmod{36} \\ &\equiv 31 \pmod{36}. \end{aligned}$$

Therefore this system has the unique solution $x \equiv 31 \pmod{36}$.

3. Let x be one of the integers we are looking for. Then we are looking for x such that

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

The moduli here are not relatively prime, but we can quickly eliminate the superfluous equations. First, 4 is a higher power of 2 than 2 is, so we can eliminate $x \equiv 1 \pmod 2$, because it is implied by $x \equiv 1 \pmod 4$. Therefore we have the system

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

We now consider the pair of equations $x \equiv 1 \pmod 3$, $x \equiv 1 \pmod 6$. The equation $x \equiv 1 \pmod 6$ can be split up into the equations $x \equiv 1 \pmod 2$, $x \equiv 1 \pmod 3$, so one of the two equations $x \equiv 1 \pmod 3$ is superfluous. We are left with

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

We see that $x \equiv 1 \pmod 2$ has shown up again! But it is still superfluous because $x \equiv 1 \pmod 4$ is still there, so we can eliminate it one more time to end up with

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

and now the moduli are relatively prime.

Note that what happened here is a result of our considering the equations two-by-two in perhaps the wrong order. We could have also said that the triple $x \equiv 1 \pmod 2, x \equiv 1$

(mod 3), $x \equiv 1 \pmod 6$ is equivalent to the pair $x \equiv 1 \pmod 2, x \equiv 1 \pmod 3$, and only after that have eliminated $x \equiv 1 \pmod 2$ because $x \equiv 1 \pmod 4$ implies it. That would have stopped $x \equiv 1 \pmod 2$ from "reappearing." I did it in this order to show that it doesn't matter the order in which we eliminate equations, as long as we just keep going.

In any case, we now solve the CRT problem with the following values:

$$\begin{aligned} M_1 &= 60, \quad x_1 \equiv 60^{-1} \equiv 4^{-1} \equiv 2 \pmod 7 \\ M_2 &= 140, \quad x_2 \equiv 140^{-1} \equiv 2^{-1} \equiv 2 \pmod 3 \\ M_3 &= 105, \quad x_3 \equiv 105^{-1} \equiv 1^{-1} \equiv 1 \pmod 4 \\ M_4 &= 84, \quad x_4 \equiv 84^{-1} \equiv 4^{-1} \equiv -1 \pmod 5. \end{aligned}$$

So we get the solution

$$\begin{aligned} x &\equiv 0 + 1 \cdot 2 \cdot 140 + 1 \cdot 1 \cdot 105 + 1 \cdot (-1) \cdot 84 \pmod{420} \\ &\equiv 280 + 105 - 84 \pmod{420} \\ &\equiv 301 \pmod{420}. \end{aligned}$$

(Note that we shouldn't have computed M_1 and x_1, since $a_1 = 0$!)

We conclude that any integer of the form requested in the question is congruent to 301 modulo 420, but the smallest positive integer satisfying those constraints is 301.

4. No matter what m is, we have that $(m, m+1) = 1$. (This is because any common divisor of m and $m+1$ would also divide $(m+1) - m = 1$, and the only integers that divide 1 are 1 and -1.)

   Therefore, by the Chinese Remainder Theorem the system $x \equiv r \pmod m$, $x \equiv s \pmod{m+1}$ has a unique solution modulo $m(m+1)$. As a consequence, it suffices to prove that

$$r(m+1) - sm \equiv r \pmod m$$

   and

$$r(m+1) - sm \equiv s \pmod{m+1}$$

   to prove the assertion. (This is the wonderful property of uniqueness!)

   We thus begin our task:

$$\begin{aligned} r(m+1) - sm &\equiv rm + r - sm \pmod m \\ &\equiv r \pmod m, \end{aligned}$$

   and

$$\begin{aligned} r(m+1) - sm &\equiv -sm \pmod{m+1} \\ &\equiv s(-m) \pmod{m+1} \\ &\equiv s \pmod{m+1}. \end{aligned}$$

Therefore if $x \equiv r \pmod{m}$ and $x \equiv s \pmod{m+1}$, necessarily it must be the case that $x \equiv r(m+1) - sm \pmod{m(m+1)}$, since this class does solve the problem and there is a unique solution to the problem.

5. (a) The three conditions are equivalent to the system

$$n \equiv 0 \pmod{9}, \quad n+1 \equiv 0 \pmod{16}, \quad n+2 \equiv 0 \pmod{25},$$

or perhaps as we usually write,

$$n \equiv 0 \pmod{9}, \quad n \equiv -1 \pmod{16}, \quad n \equiv -2 \pmod{25}.$$

The moduli are relatively prime so this is a straightforward CRT problem. Note that since $a_1 = 0$, we do not need to compute M_1 and x_1. We have

$$\begin{aligned} M_2 &= 225, \quad x_2 \equiv 225^{-1} \equiv 1^{-1} \equiv 1 \pmod{16} \\ M_3 &= 144, \quad x_3 \equiv 144^{-1} \equiv 19^{-1} \equiv 4 \pmod{25}, \end{aligned}$$

where we computed $19^{-1} \pmod{25}$ using the Euclidean algorithm:

$$\begin{aligned} 25 &= 19 + 6 \\ 19 &= 3 \cdot 6 + 1 \end{aligned}$$

so

$$\begin{aligned} 1 &= 19 - 3 \cdot 6 \\ &= 19 - 3 \cdot (25 - 19) \\ &= 4 \cdot 19 - 3 \cdot 25. \end{aligned}$$

We can now apply the CRT algorithm:

$$\begin{aligned} n &\equiv 0 + (-1) \cdot 1 \cdot 225 + (-2) \cdot 4 \cdot 144 \pmod{3600} \\ &\equiv -225 - 1152 \pmod{3600} \\ &\equiv -1377 \equiv 2223 \pmod{3600}. \end{aligned}$$

Therefore all integers n of this type are of the form $2223 + 3600t$, for $t \in \mathbb{Z}$.

(b) This time the conditions are equivalent to

$$n \equiv 0 \pmod{4}, \quad n+1 \equiv 0 \pmod{9}, \quad n+2 \equiv 0 \pmod{16},$$

or

$$n \equiv 0 \pmod{4}, \quad n \equiv -1 \pmod{9}, \quad n \equiv -2 \pmod{16}.$$

However, we notice that the equations $n \equiv 0 \pmod{4}$ and $n \equiv -2 \pmod{16}$ are not compatible, since $(4, 16) = 4$ and $0 \not\equiv -2 \pmod{4}$. Therefore there are no such ns.