Math 255 - Spring 2017
Homework 5 Solutions

1. The five divisibility statements can be translated into the five congruence relations:

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

We could also write $a \equiv -1 \pmod 3$, etc., which are equivalent congruences. Since this is a set of simultaneous linear congruences, we want to use the Chinese Remainder Theorem to find the solution. However, we cannot apply the Chinese Remainder Theorem right now because the n_is are not pairwise relatively prime.

The way to get pairwise relatively prime moduli is to see if any of the equations imply any of the other equations, so that we can get rid of the superfluous equations (those that are implied by other equations). Hopefully in this way we can end up with equations all of whose moduli are pairwise relatively prime.

Consider first the two equations $a \equiv 0 \pmod 2$ and $a+2 \equiv 0 \pmod 4$. The first equation says that there is $k \in \mathbb{Z}$ such that $a = 2k$. The second equation says that there is $\ell \in \mathbb{Z}$ such that $a+2 = 4\ell$ or $a = 4\ell - 2$. If $a = 4\ell - 2$, then $a = 2(2\ell - 1)$. Therefore a is of the form $2k$, with $k = 2\ell - 1$. Therefore the equation $a \equiv 0 \pmod 2$ is implied by the equation $a + 2 \equiv 0 \pmod 4$ and we can omit it from the set of congruences without losing any information.

(Note that the other way doesn't work: We cannot omit $a + 2 \equiv 0 \pmod 4$ and keep $a \equiv 0 \pmod 4$. This is because if $a \equiv 0 \pmod 2$ then either $a \equiv 0 \pmod 2$ or $a \equiv 2 \pmod 4$. We cannot recover the information that actually $a + 2 \equiv 0 \pmod 4$. This should make sense: Knowing the remainder of division by 4 is more information than just knowing the remainder of division by 2.)

Consider now the three equations $a+1 \equiv 0 \pmod 3$, $a+2 \equiv 0 \pmod 4$ and $a+4 \equiv 0 \pmod 6$. We will show that if $a+1 \equiv 0 \pmod 3$ and $a+2 \equiv 0 \pmod 4$, then $a+4 \equiv 0 \pmod 6$. This will make the equation $a + 4 \equiv 0 \pmod 6$ superfluous.

If $a + 1 \equiv 0 \pmod 3$, then $a + 1 = 3k$ for some $k \in \mathbb{Z}$. If $a + 2 \equiv 0 \pmod 4$, then $a + 2 = 4\ell$ for some $\ell \in \mathbb{Z}$. Consider now $a + 4$: We have

$$a + 4 = a + 1 + 3 = 3k + 3 = 3(k + 1)$$

and

$$a + 4 = a + 2 + 2 = 4\ell + 2 = 2(2\ell + 1).$$

Therefore, $a+4$ is divisible by both 2 and 3. Since $\gcd(2,3)=1$, this implies that $2\cdot 3=6$ divides $a+4$ or $a+4\equiv 0 \pmod 6$. Therefore this last equation is superfluous once we have the equations $a+1\equiv 0 \pmod 3$ and $a+2\equiv 0 \pmod 4$.

Getting rid of the extra equations, we now have the set of simultaneous congruences

$$\begin{aligned} a &\equiv -1 \pmod 3 \\ a &\equiv -2 \pmod 4 \\ a &\equiv -3 \pmod 5. \end{aligned}$$

This is exactly in the form required for the Chinese Remainder Theorem, and so we apply it. We have

$$\begin{aligned} a_1 &= -1, \quad n_1 = 3, \quad \text{and} \quad N_1 = 20 \\ a_2 &= -2, \quad n_2 = 4, \quad \text{and} \quad N_2 = 15 \\ a_3 &= -3, \quad n_3 = 5, \quad \text{and} \quad N_3 = 12 \end{aligned}$$

We now find our x_is:

- x_1 is any integer such that $20x_1 \equiv 1 \pmod 3$. Equivalently, this is $2x_1 \equiv 1 \pmod 3$. By guessing and checking, we see that we can use $x_1 = 2$.
- x_2 is any integer such that $15x_2 \equiv 1 \pmod 4$. Equivalently this is $3x_2 \equiv 1 \pmod 4$. By guessing and checking, we see that we can use $x_2 = 3$.
- Finally, x_3 is such that $12x_3 \equiv 1 \pmod 5$. Equivalently this is $2x_3 \equiv 1 \pmod 5$. One last time, we guess and check and find $x_3 = 3$ works.

Putting it all together we have

$$\begin{aligned} x &\equiv -2\cdot 20 - 2\cdot 3\cdot 15 - 3\cdot 3\cdot 12 \pmod{3\cdot 4\cdot 5} \\ &\equiv -40 - 90 - 108 \pmod{60} \\ &\equiv 20 + 30 - 48 \pmod{60} \\ &\equiv 2 \pmod{60}. \end{aligned}$$

Now we need the smallest integer $a > 2$ that is congruent to 2 modulo 60. That number is $a = 62$.

2. Let x be the number of coins that got stolen. From the story, we can extract the following congruences:

$$\begin{aligned} x &\equiv 3 \pmod{17} \\ x &\equiv 10 \pmod{16} \\ x &\equiv 0 \pmod{15} \end{aligned}$$

This is exactly in the form required to apply the Chinese Remainder Theorem, so we go ahead and apply it.

We have

$$\begin{aligned} a_1 = 3, \quad n_1 = 17, \quad \text{and} \quad N_1 = 15 \cdot 16 = 240 \\ a_2 = 10, \quad n_2 = 16, \quad \text{and} \quad N_2 = 15 \cdot 17 = 255 \\ a_3 = 0, \quad n_3 = 15, \quad \text{and} \quad N_3 = ? \end{aligned}$$

We note that since $a_3 = 0$, we do not need to compute N_3 and x_3, since in the formula at the end they will just be multiplied by $a_3 = 0$.

Therefore we only need to find x_1 and x_2:

- x_1 is any integer such that $240x_1 \equiv 1 \pmod{17}$. Equivalently we have $2x_1 \equiv 1 \pmod{17}$, since $240 \equiv 2 \pmod{17}$. It is perhaps easy to guess that $x_1 = 9$ is a valid solution, because $2 \cdot 9 = 18 \equiv 1 \pmod{17}$.
- x_2 is any integer such that $255x_2 \equiv 1 \pmod{16}$. Because 256 is divisible by 16, $255 \equiv -1 \pmod{16}$, so equivalently we are solving $-x_2 \equiv 1 \pmod{16}$. A possible solution is $x_2 = -1$.

Putting it all together we get

$$\begin{aligned} x &\equiv 3 \cdot 240 \cdot 9 - 10 \cdot 255 + 0 \pmod{15 \cdot 16 \cdot 17} \\ &\equiv 6480 - 2550 \pmod{4080} \\ &\equiv 3930 \pmod{4080}. \end{aligned}$$

Because 3930 is between 0 and 4079, the smallest possible number of coins is 3930.

3. Let $a \in \mathbb{Z}$ be such that $\gcd(a, 35) = 1$.

   First, we notice that $\gcd(a, 5) = 1$. This must be the case because for any integer, $\gcd(a, 5)$ is either 1 or 5 (these are the only divisors of 5). If $\gcd(a, 5)$ were 5, then 5 would divide a. Since 5 also divides 35, it would follow that $\gcd(a, 5) \geq 5$. Therefore it must be that $\gcd(a, 5) = 1$. In the same manner, we can say that $\gcd(a, 7) = 1$.

   We can therefore apply Fermat's Little Theorem for $p = 5$ and $p = 7$: It is the case that

   $$a^{5-1} = a^4 \equiv 1 \pmod{5} \tag{1}$$

   and

   $$a^{7-1} = a^6 \equiv 1 \pmod{7}. \tag{2}$$

   By Theorem 4.2, we can raise both sides of equation (1) to the power of 3 and retain the congruence. Therefore,

   $$(a^4)^3 \equiv 1^3 \pmod{5},$$

   or, to put it more simply,

   $$a^{12} \equiv 1 \pmod{5}.$$

   In the same manner we can square both sides of equation (2) and retain a true statement:

   $$(a^6)^2 \equiv 1^2 \pmod{7}$$

   or

   $$a^{12} \equiv 1 \pmod{7}.$$

   Now for a moment let $x = a^12$. Then we have the simultaneous congruences

   $$\begin{aligned} x &\equiv 1 \pmod{5} \\ x &\equiv 1 \pmod{7}. \end{aligned}$$

   A solution to this set of congruences is $x \equiv 1 \pmod{35}$. By the Chinese Remainder Theorem, this is the unique solution. Therefore we are guaranteed that $a^{12} \equiv 1 \pmod{35}$.