Math 255 - Spring 2018
Solving $x^2 \equiv a \pmod{n}$ Solutions

1. (a) We have that $56 = 7 \cdot 8$, so we must solve $x^2 \equiv 1 \pmod 7$ and $x^2 \equiv 1 \pmod 8$. Thankfully, these are both easy equations!

Since $(1, 7) = 1$ and 7 is a power of an odd prime, $x^2 \equiv 1 \pmod 7$ has two solutions. What's more, we know what they are by inspection: They are $x \equiv 1 \pmod 7$ and $x \equiv -1 \equiv 6 \pmod 7$.

The equation $x^2 \equiv 1 \pmod 8$ is one that should be familiar; it is the base case for the problems $x^2 \equiv a \pmod{2^k}$. It has solutions $x \equiv 1, 3, 5, 7 \pmod 8$.

Therefore we focus on the Chinese Remainder Theorem problem. In this case we will have $m_1 = 7$ and $m_2 = 8$. Therefore we have $M_1 = 8$ and $x_1 \equiv 8^{-1} \equiv 1^{-1} \equiv 1 \pmod 7$, and $M_2 = 7$ and $x_2 \equiv 7^{-1} \equiv (-1)^{-1} \equiv -1 \pmod 8$. The general form of the solution to the problem

$$x \equiv a_1 \pmod 7, \quad x \equiv a_2 \pmod 8$$

is therefore

$$x \equiv 8a_1 - 7a_2 \pmod{56}.$$

Forming all pairs $(a_1 \pmod 7, a_2 \pmod 8)$ from the solutions we got, we get that we should solve the Chinese Remainder Theorem for

$$(1 \pmod 7, 1 \pmod 8), (1 \pmod 7, 3 \pmod 8), (1 \pmod 7, 5 \pmod 8),$$
$$(1 \pmod 7, 7 \pmod 8), (6 \pmod 7, 1 \pmod 8), (6 \pmod 7, 3 \pmod 8),$$
$$(6 \pmod 7, 5 \pmod 8), (6 \pmod 7, 7 \pmod 8).$$

Plugging into our formula we get the 8 solutions

$$x \equiv 8 - 7 \equiv 1 \pmod{56}$$
$$x \equiv 8 - 21 \equiv -13 \equiv 43 \pmod{56}$$
$$x \equiv 8 - 35 \equiv -27 \equiv 29 \pmod{56}$$
$$x \equiv 8 - 49 \equiv -41 \equiv 15 \pmod{56}$$
$$x \equiv 48 - 7 \equiv 41 \pmod{56}$$
$$x \equiv 48 - 21 \equiv 27 \pmod{56}$$
$$x \equiv 48 - 35 \equiv 13 \pmod{56}$$
$$x \equiv 48 - 49 \equiv -1 \equiv 55 \pmod{56}.$$

Therefore the solutions to $x^2 \equiv 1 \pmod{56}$ are

$$x \equiv 1, 13, 15, 27, 29, 41, 43, 55 \pmod{56}.$$

We can note that all solutions come in pairs $x, -x \pmod{56}$; we didn't need to do anything about it, it just happened. We also note that all solutions come in quadruplets $x, -x, x+28, -(x+28) \pmod{56}$. We could have figured that out from the beginning to cut down on the Chinese Remainder Theorem step, but I'm not sure that would have been worth it.

(b) We have that $105 = 3 \cdot 5 \cdot 7$, so we must solve

$$\begin{aligned} x^2 &\equiv 70 \equiv 1 \pmod{3}, \\ x^2 &\equiv 70 \equiv 0 \pmod{5}, \\ x^2 &\equiv 70 \equiv 0 \pmod{7}. \end{aligned}$$

Once again, thankfully these are all easy equations! The first one has solutions $x \equiv 1, 2 \pmod{3}$, since $(1, 3) = 1$ and 3 is a power of an odd prime, the second one has unique solution $x \equiv 0 \pmod{5}$, and the last one has unique solution $x \equiv 0 \pmod{7}$.

Therefore the overall problem will have 2 solutions, which are the solutions to the two Chinese Remainder Theorem problems

$$x \equiv 1 \pmod{3}, \quad x \equiv 0 \pmod{5}, \quad x \equiv 0 \pmod{7},$$

and

$$x \equiv 2 \pmod{3}, \quad x \equiv 0 \pmod{5}, \quad x \equiv 0 \pmod{7}.$$

Here we have $m_1 = 3$, $m_2 = 5$ and $m_3 = 7$; and for both solutions we have $a_2 = 0$, and $a_3 = 0$. We also compute

$$M_1 = 35, \quad x_1 \equiv 35^{-1} \equiv 2^{-1} \equiv 2 \pmod{3}, M_2 = 21, \quad x_2 \equiv 21^{-1} \equiv 1^{-1} \equiv 1 \pmod{5}, M_3 = 1$$

(Although we note that since $a_2 = a_3 = 0$ for both solutions, we don't actually need to know M_2, x_2, M_3, and x_3; they are only included here in case someone computed them and wants to check their work.)

Plugging this all in we have as a first solution, when $a_1 = 1$,

$$\begin{aligned} x &\equiv a_1 M_1 x_1 + a_2 M_2 x_2 + a_3 M_3 x_3 \pmod{105} \\ &\equiv 70 + 0 + 0 \equiv 70 \pmod{105}. \end{aligned}$$

And the second solution is

$$\begin{aligned} x &\equiv a_1 M_1 x_1 + a_2 M_2 x_2 + a_3 M_3 x_3 \pmod{105} \\ &\equiv 140 + 0 + 0 \equiv 35 \pmod{105}. \end{aligned}$$

The two solutions are therefore

$$x \equiv 35, 70 \pmod{105}.$$

We note that since we knew there would be two solutions, once we got $x \equiv 70 \pmod{105}$ as a solution we could have immediately concluded that the other solution was $x \equiv -70 \equiv 35 \pmod{105}$. That is acceptable reasoning, but we see that the Chinese Remainder Theorem step is not much longer to do.

(c) We have that $135 = 3^3 \cdot 5$, so we must solve the two equations

$$\begin{aligned} x^2 &\equiv 59 \equiv 5 \pmod{27} \\ x^2 &\equiv 59 \equiv 4 \pmod{5}. \end{aligned}$$

We solve the first equation, $x^2 \equiv 5 \pmod{27}$. The base case is to solve $x^2 \equiv 5 \equiv 2 \pmod{3}$. This does not have a solution, since $1^2 \equiv 2^2 \equiv 1 \pmod{3}$. Therefore the whole problem has no solution.

(d) Once again we have that $135 = 3^3 \cdot 5$, so we must solve the equations

$$\begin{aligned} x^2 &\equiv 34 \equiv 7 \pmod{27} \\ x^2 &\equiv 34 \equiv 4 \pmod{5}. \end{aligned}$$

We solve the first equation, $x^2 \equiv 7 \pmod{27}$. The base case is to solve $x^2 \equiv 7 \equiv 1 \pmod{3}$. This does have a solution, this time! One solution is $x \equiv 1 \pmod{3}$, and this is the one we will lift.

Since 3 is odd, we do the p is odd lifting. This requires solving

$$x_1 = 1 + 3y_0 \quad \text{and} x_1^2 \equiv 7 \pmod{9}.$$

We have

$$\begin{aligned} (1 + 3y_0)^2 &\equiv 7 \pmod{9} \\ 1 + 6y_0 + 9y_0^2 &\equiv 7 \pmod{9} \\ 6y_0 &\equiv 6 \pmod{9} \\ 2y_0 &\equiv 2 \pmod{3} \\ y_0 &\equiv 1 \pmod{3}. \end{aligned}$$

And therefore the lifted solution $x_1 \equiv 1 + 3 \cdot 1 \equiv 4 \pmod{9}$.

We lift again! This time we solve

$$x_1 = 4 + 9y_0 \quad \text{and} x_1^2 \equiv 7 \pmod{27}.$$

We have

$$\begin{aligned} (4 + 9y_0)^2 &\equiv 7 \pmod{27} \\ 16 + 72y_0 + 81y_0^2 &\equiv 7 \pmod{27} \\ 18y_0 &\equiv -9 \pmod{27} \\ 2y_0 &\equiv -1 \pmod{3} \\ y_0 &\equiv -2 \equiv 1 \pmod{3}. \end{aligned}$$

And therefore the lifted solution $x_1 \equiv 4 + 9 \cdot 1 \equiv 13 \pmod{27}$. Since p is odd, there is one other solution and it is $-x_1 \equiv -13 \equiv 14 \pmod{27}$.

We now solve the other equation, which is $x^2 \equiv 4 \pmod{5}$. This has solutions $x \equiv 2, 3 \pmod{5}$.

Since each of the two congruences have two solutions, in total we will get four solutions. They correspond to the following pairs $(a_1 \pmod{27}, a_2 \pmod{5})$:

$$(13 \pmod{27}, 2 \pmod{5}), (13 \pmod{27}, 3 \pmod{5}),$$
$$(14 \pmod{27}, 2 \pmod{5}), (14 \pmod{27}, 3 \pmod{5}).$$

We do the preparation steps of the Chinese Remainder Theorem: Here we will have $m_1 = 27$ and $m_2 = 5$, and we compute

$$M_1 = 5, \quad x_1 \equiv 5^{-1} \equiv -16 \equiv 11 \pmod{27},$$
$$M_2 = 27, \quad x_2 \equiv 27^{-2} \equiv 2^{-1} \equiv -2 \pmod{5}.$$

In general the solution to

$$x \equiv a_1 \pmod{27}, \quad \text{and} \quad x \equiv a_2 \pmod{5}$$

is

$$x \equiv 55a_1 - 54a_2 \pmod{135}.$$

Therefore the four solutions are

$$x \equiv 55 \cdot 13 - 54 \cdot 2 \equiv 607 \equiv 67 \pmod{135},$$
$$x \equiv 55 \cdot 13 - 54 \cdot 3 \equiv 607 \equiv 13 \pmod{135},$$
$$x \equiv 55 \cdot 14 - 54 \cdot 2 \equiv 607 \equiv 122 \pmod{135},$$
$$x \equiv 55 \cdot 14 - 54 \cdot 3 \equiv 607 \equiv 68 \pmod{135}.$$

The four solutions are therefore

$$x \equiv 13, 67, 68, 122 \pmod{135}.$$

(e) We have that $80 = 2^4 \cdot 5$. Therefore we must solve

$$x^2 \equiv 25 \equiv 9 \pmod{16}$$
$$x^2 \equiv 25 \equiv 0 \pmod{5}.$$

We can tell from knowledge of the integers that $x^2 \equiv 9 \pmod{16}$ has solution $x \equiv 3 \pmod{16}$. Since $16 = 2^4$, this congruence has three more solutions: $x \equiv -3 \equiv 13 \pmod{16}$, $x \equiv 3 + 8 \equiv 11 \pmod{16}$ and $x \equiv -11 \equiv 5 \pmod{16}$.

The congruence $x^2 \equiv 0 \pmod{5}$ has unique solution $x \equiv 0 \pmod{5}$.

Therefore, overall the problem will have four solutions. We note that since for each of them $a_2 = 0$, we don't need to compute M_2 and x_2. So we compute $M_1 = 5$ and $x_1 \equiv 5^{-1} \equiv 13 \pmod{16}$. The solution to the Chinese Remainder Theorem problem will be

$$x \equiv 65a_1 + 0 \equiv 65a_1 \pmod{80},$$

for $a_1 = 3, 5, 11$ and 13. The solutions are therefore

$$\begin{aligned} x &\equiv 65 \cdot 3 \equiv 195 \equiv 35 \pmod{80}, \\ x &\equiv 65 \cdot 5 \equiv 325 \equiv 5 \pmod{80}, \\ x &\equiv 65 \cdot 11 \equiv 715 \equiv 75 \pmod{80} \\ x &\equiv 65 \cdot 13 \equiv 845 \equiv 45 \pmod{80}. \end{aligned}$$

Therefore the four solutions of this congruence are

$$x \equiv 5, 35, 45, 75 \pmod{80}.$$