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

1. (a) Note that $125 = 5^3$, and $(71, 125) = 1$. We begin by solving $x^2 \equiv 71 \pmod 5$, which is the same equation as $x^2 \equiv 1 \pmod 5$. This has two solutions, $x \equiv 1 \pmod 5$ and $x \equiv -1 \equiv 4 \pmod 5$, and we can lift either solution. We'll lift $x \equiv 1 \pmod 5$.

   Now we lift from $x_0 \equiv 1 \pmod 5$ to a solution $x_1 \pmod{25}$. This solution will satisfy both the lifting equation:

$$x_1 = 1 + 5y_0$$

   (i.e. it is a lift of $1 \pmod 5$) and the congruence we are trying to solve, which is

$$x_1^2 \equiv 71 \pmod{25}.$$

   Plugging the lifting equation into the congruence and simplifying, we get:

$$\begin{aligned}
(1+5y_0)^2 &\equiv 71 \pmod{25}\\
1 + 10y_0 + 25y_0^2 &\equiv 21 \pmod{25}\\
1 + 10y_0 &\equiv 21 \pmod{25}\\
10y_0 &\equiv 20 \pmod{25}\\
2y_0 &\equiv 4 \pmod 5\\
y_0 &\equiv 2 \pmod 5.
\end{aligned}$$

   Therefore we have that $x_1 \equiv 1 + 5 \cdot 2 \equiv 11 \pmod{25}$ is a solution to $x^2 \equiv 71 \pmod{25}$. (We can check that and it is true!)

   Now we lift from $x_0 \equiv 11 \pmod{25}$ to a solution $x_1 \pmod{125}$. This solution will satisfy both the lifting equation:

$$x_1 = 11 + 25y_0$$

   (i.e. it is a lift of $11 \pmod{25}$) and the congruence we are trying to solve, which is

$$x_1^2 \equiv 71 \pmod{125}.$$

   Plugging the lifting equation into the congruence and simplifying, we get:

$$\begin{aligned}
(11+25y_0)^2 &\equiv 71 \pmod{125}\\
121 + 550y_0 + 25^2y_0^2 &\equiv 71 \pmod{125}\\
121 + 50y_0 &\equiv 71 \pmod{125}\\
50y_0 &\equiv -50 \pmod{125}\\
2y_0 &\equiv -2 \pmod 5\\
y_0 &\equiv -1 \equiv 4 \pmod 5.
\end{aligned}$$

Therefore we have that $x_1 \equiv 11 + 25 \cdot 4 \equiv 111 \pmod{125}$ is a solution to $x^2 \equiv 71 \pmod{125}$. (We can check that and it is true!)

Now to find all solutions, we use the theorem which says that if $(a, 125) = 1$, $x^2 \equiv a \pmod{125}$ has exactly two solutions, given by x_1 and $-x_1$. Therefore this congruence has exactly two solutions, $x \equiv 111 \pmod{125}$ and $x \equiv -111 \equiv 14 \pmod{125}$.

(b) Here we have that $81 = 3^4$ and $(58, 81) = 1$, so we apply our algorithm. We first solve $x^2 \equiv 58 \equiv 1 \pmod 3$, which has solution $x \equiv 1 \pmod 3$.

We now lift to $\mathbb{Z}/9\mathbb{Z}$. The lifted solution x_1 will satisfy the lifting equation

$$x_1 = 1 + 3y_0$$

and the congruence

$$x_1^2 \equiv 58 \pmod 9.$$

Plugging in, we get

$$\begin{aligned} (1 + 3y_0)^2 &\equiv 58 \pmod 9 \\ 1 + 6y_0 + 9y_0^2 &\equiv 58 \pmod 9 \\ 1 + 6y_0 &\equiv 4 \pmod 9 \\ 6y_0 &\equiv 3 \pmod 9 \\ 2y_0 &\equiv 1 \pmod 3 \\ y_0 &\equiv 2 \pmod 3. \end{aligned}$$

So $x_1 \equiv 1 + 3 \cdot 2 \equiv 7 \pmod 9$ is a solution to $x^2 \equiv 58 \pmod 9$.

Next we lift to $\mathbb{Z}/27\mathbb{Z}$. The lifted solution x_1 will satisfy the lifting equation

$$x_1 = 7 + 9y_0$$

and the congruence

$$x_1^2 \equiv 58 \pmod{27}.$$

Plugging in, we get

$$\begin{aligned} (7 + 9y_0)^2 &\equiv 58 \pmod{27} \\ 49 + 126y_0 + 81y_0^2 &\equiv 58 \pmod{27} \\ 22 + 18y_0 &\equiv 4 \pmod{27} \\ 18y_0 &\equiv -18 \pmod{27} \\ 2y_0 &\equiv -2 \pmod 3 \\ y_0 &\equiv -1 \equiv 2 \pmod 3. \end{aligned}$$

So $x_1 \equiv 7 + 9 \cdot 2 \equiv 25 \pmod{27}$ is a solution to $x^2 \equiv 58 \pmod{27}$.

Finally we lift to $\mathbb{Z}/81\mathbb{Z}$. The lifted solution x_1 will satisfy the lifting equation

$$x_1 = 25 + 27y_0$$

and the congruence

$$x_1^2 \equiv 58 \pmod{81}.$$

Plugging in, we get

$$\begin{aligned}(25 + 27y_0)^2 &\equiv 58 \pmod{81}\\ 625 + 1350y_0 + 27^2y_0^2 &\equiv 58 \pmod{81}\\ 58 + 54y_0 &\equiv 58 \pmod{81}\\ 54y_0 &\equiv 0 \pmod{81}\\ 2y_0 &\equiv 0 \pmod{3}\\ y_0 &\equiv 0 \pmod{3}.\end{aligned}$$

So $x_1 \equiv 25 \pmod{81}$ is a solution to $x^2 \equiv 58 \pmod{81}$.

Now that we have one solution we can find all solutions; they are $x \equiv 25 \pmod{81}$ and $x \equiv -25 \equiv 56 \pmod{81}$.

(c) We have that $343 = 7^3$ and $(39, 343) = 1$. So we begin by solving $x^2 \equiv 39 \equiv 4 \pmod{7}$. This has solution $x \equiv 2 \pmod{7}$.

We lift $x_0 \equiv 2 \pmod{7}$ to $\mathbb{Z}/49\mathbb{Z}$ by solving the equations:

$$x_1 = 2 + 7y_0 \quad \text{and} \quad x_1^2 \equiv 39 \pmod{49}.$$

We have

$$\begin{aligned}(2 + 7y_0)^2 &\equiv 39 \pmod{49}\\ 4 + 28y_0 + 49y_0^2 &\equiv 39 \pmod{49}\\ 4 + 28y_0 &\equiv 39 \pmod{49}\\ 28y_0 &\equiv 35 \pmod{49}\\ 4y_0 &\equiv 5 \pmod{7}\\ y_0 &\equiv 10 \equiv 3 \pmod{7}.\end{aligned}$$

And therefore $x_1 \equiv 2 + 7 \cdot 3 \equiv 23 \pmod{49}$ is a solution ot $x^2 \equiv 39 \pmod{49}$.

Then, we lift $x_0 \equiv 23 \pmod{49}$ to $\mathbb{Z}/343\mathbb{Z}$ by solving the equations:

$$x_1 = 23 + 49y_0 \quad \text{and} \quad x_1^2 \equiv 39 \pmod{343}.$$

We have

$$\begin{aligned}(23 + 49y_0)^2 &\equiv 39 \pmod{343}\\ 529 + 2254y_0 + 49^2y_0^2 &\equiv 39 \pmod{343}\\ 186 + 196y_0 &\equiv 39 \pmod{343}\\ 196y_0 &\equiv -147 \pmod{343}\\ 4y_0 &\equiv -3 \equiv 4 \pmod{7}\\ y_0 &\equiv 1 \pmod{7}.\end{aligned}$$

And therefore $x_1 \equiv 23+49\cdot 1 \equiv 72 \pmod{343}$ is a solution ot $x^2 \equiv 39 \pmod{343}$. The other solution is $x \equiv -72 \equiv 271 \pmod{343}$.

(d) We have that $121 = 11^2$ and $(89, 121) = 1$, so we can do our thing. We first solve $x^2 \equiv 89 \equiv 1 \pmod{11}$, which has solution $x \equiv 1 \pmod{11}$.

We lift this solution to $\mathbb{Z}/121\mathbb{Z}$: The lifted solution will satisfy

$$x_1 = 1 + 11y_0 \quad \text{and} \quad x_1^2 \equiv 89 \pmod{121}.$$

Therefore we must solve

$$\begin{aligned}
(1 + 11y_0)^2 &\equiv 89 \pmod{121} \\
1 + 22y_0 + 121y_0^2 &\equiv 89 \pmod{121} \\
1 + 22y_0 &\equiv 89 \pmod{121} \\
22y_0 &\equiv 88 \pmod{121} \\
2y_0 \equiv 8 \pmod{11} \\
y_0 &\equiv 4 \pmod{11}.
\end{aligned}$$

Therefore $x \equiv 1 + 11 \cdot 4 \equiv 45 \pmod{121}$ is one solution and the other is $x \equiv -45 \equiv 76 \pmod{121}$.