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

1. (a) We can see immediately that a solution to this equation is $x \equiv 3 \pmod{16}$, since $3^2 = 9$ in the integers (and therefore $x^2 \equiv 9 \pmod{n}$ always has solution $x \equiv 3 \pmod{n}$, no matter what n is; the question is what the other solutions are!).

   By our theorem, the other solutions are $-x_1 \equiv -3 \equiv 13 \pmod{16}$, $x_1 + 8 \equiv 3 + 8 \equiv 11 \pmod{16}$ and $-(x_1 + 8) \equiv -11 \equiv 5 \pmod{16}$.

   (b) Since $17 \equiv 1 \pmod{8}$, there is a solution to this equation. We choose to obtain it by lifting $x \equiv 1 \pmod{8}$.

   The first step is to lift $x_0 \equiv 1 \pmod{4}$ to a solution modulo 16. The lifting equation is

$$x_1 = 1 + 4y_0$$

   and we wish to solve the quadratic equation

$$x_1^2 \equiv 17 \equiv 1 \pmod{16}.$$

   (Ok, this clearly has solution $x_1 \equiv 1 \pmod{16}$, but let's practice our lifting step.) Plugging one equation into the other, we get

$$\begin{aligned} (1 + 4y_0)^2 &\equiv 1 \pmod{16} \\ 1 + 8y_0 + 16y_0^2 &\equiv 1 \pmod{16} \\ 8y_0 &\equiv 0 \pmod{16} \\ y_0 &\equiv 0 \pmod{2}. \end{aligned}$$

   Therefore we get the solution $x_1 \equiv 1 \pmod{16}$, as we expected.

   Now we lift $x_0 \equiv 1 \pmod{8}$ to a solution $\mathbb{Z}/32\mathbb{Z}$. The lifting equation is

$$x_1 = 1 + 8y_0$$

   and we wish to solve the quadratic equation

$$x_1^2 \equiv 17 \pmod{32}.$$

   Plugging one equation into the other, we get

$$\begin{aligned} (1 + 8y_0)^2 &\equiv 17 \pmod{32} \\ 1 + 16y_0 + 64y_0^2 &\equiv 17 \pmod{32} \\ 16y_0 &\equiv 16 \pmod{32} \\ y_0 &\equiv 1 \pmod{2}. \end{aligned}$$

   Therefore we get the solution $x_1 \equiv 1 + 8 \cdot 1 \equiv 9 \pmod{32}$. The other solutions are $-x_1 \equiv -9 \equiv 23 \pmod{32}$, $x_1 + 16 \equiv 9 + 16 \equiv 25 \pmod{32}$ and $-(x_1 + 16) \equiv -25 \equiv 7 \pmod{32}$.

(c) If we are very clever, we might notice that $33 \equiv 1 \pmod{32}$. Therefore, the equation $x^2 \equiv 33 \equiv 1 \pmod{32}$ has solution $x \equiv 1 \pmod{32}$. Then we only have one lifting step to do.

We lift $x \equiv 1 \pmod{16}$ to a solution $\mathbb{Z}/64\mathbb{Z}$. The lifting equation is

$$x_1 = 1 + 16y_0$$

and we wish to solve

$$x_1^2 \equiv 33 \pmod{64}.$$

Plugging the first equation into the second, we get

$$\begin{aligned}(1+16y_0)^2 &\equiv 33 \pmod{64}\\ 1+32y_0+16^2y_0^2 &\equiv 33 \pmod{64}\\ 32y_0 &\equiv 32 \pmod{64}\\ y_0 &\equiv 1 \pmod{2}.\end{aligned}$$

Therefore we get a solution $x_1 \equiv 1 + 16 \cdot 1 \equiv 17 \pmod{64}$. The other three solutions are $-x_1 \equiv -17 \equiv 47 \pmod{64}$, $x_1 + 32 \equiv 17 + 32 \equiv 49 \pmod{64}$ and $-(x_1 + 32) \equiv -49 \equiv 15 \pmod{64}$.

We can also of course do the whole problem if we don't notice that $33 \equiv 1 \pmod{32}$. In that case, we begin by solving $x^2 \equiv 33 \equiv 1 \pmod{8}$, which has solution $x \equiv 1 \pmod{8}$.

The solution $x \equiv 1 \pmod{4}$ is then lifted to $x \equiv 1 \pmod{16}$:

$$\begin{aligned}(1+4y_0)^2 &\equiv 33 \pmod{16}\\ 1+8y_0+16y_0^2 &\equiv 1 \pmod{16}\\ 8y_0 &\equiv 0 \pmod{16}\\ y_0 &\equiv 0 \pmod{2}.\end{aligned}$$

The solution $x \equiv 1 \pmod{8}$ is lifted to $x \equiv 1 \pmod{32}$:

$$\begin{aligned}(1+8y_0)^2 &\equiv 33 \pmod{32}\\ 1+16y_0+64y_0^2 &\equiv 1 \pmod{32}\\ 16y_0 &\equiv 0 \pmod{32}\\ y_0 &\equiv 0 \pmod{2}.\end{aligned}$$

And we did the last lifting step first so we will not repeat it here.

(d) Here we have that $111 \equiv 7 \not\equiv 1 \pmod{8}$, so this quadratic congruence has no solution.

(e) As in problem c), if we are very clever, we might notice that $57 \equiv 25 \pmod{32}$. Therefore, the equation $x^2 \equiv 57 \equiv 25 \pmod{32}$ has solution $x \equiv 5 \pmod{32}$. Then we only have one lifting step to do.

We lift $x \equiv 5 \pmod{16}$ to a solution $\mathbb{Z}/64\mathbb{Z}$. The lifting equation is

$$x_1 = 5 + 16y_0$$

and we wish to solve

$$x_1^2 \equiv 57 \pmod{64}.$$

Plugging the first equation into the second, we get

$$\begin{aligned}
(5+16y_0)^2 &\equiv 57 \pmod{64}\\
25 + 160y_0 + 16^2y_0^2 &\equiv 57 \pmod{64}\\
32y_0 &\equiv 32 \pmod{64}\\
y_0 &\equiv 1 \pmod{2}.
\end{aligned}$$

Therefore we get a solution $x_1 \equiv 5 + 16 \cdot 1 \equiv 21 \pmod{64}$. The other three solutions are $-x_1 \equiv -21 \equiv 43 \pmod{64}$, $x_1 + 32 \equiv 21 + 32 \equiv 53 \pmod{64}$ and $-(x_1+32) \equiv -53 \equiv 11 \pmod{64}$.

We can also of course do the whole problem if we don't notice that $57 \equiv 25 \pmod{32}$. In that case, we begin by solving $x^2 \equiv 57 \equiv 1 \pmod{8}$, which has solution $x \equiv 1 \pmod{8}$.

The solution $x \equiv 1 \pmod{4}$ is then lifted to $x \equiv 5 \pmod{16}$:

$$\begin{aligned}
(1+4y_0)^2 &\equiv 57 \pmod{16}\\
1 + 8y_0 + 16y_0^2 &\equiv 9 \pmod{16}\\
8y_0 &\equiv 8 \pmod{16}\\
y_0 &\equiv 1 \pmod{2}.
\end{aligned}$$

The solution $x \equiv 5 \pmod{8}$ is lifted to $x \equiv 5 \pmod{32}$:

$$\begin{aligned}
(5+8y_0)^2 &\equiv 57 \pmod{32}\\
25 + 80y_0 + 64y_0^2 &\equiv 25 \pmod{32}\\
16y_0 &\equiv 0 \pmod{32}\\
y_0 &\equiv 0 \pmod{2}.
\end{aligned}$$

And we did the last lifting step first so we will not repeat it here.