MATH 255 QUIZ 25 MAY 2 2018

Name:

Problem 1: *Please give all solutions to the quadratic congruence*

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

Solution: We might notice that $33 \equiv 1 \pmod{32}$, and therefore the equation $x^2 \equiv 33 \equiv 1 \pmod{32}$ has solution $x \equiv 1 \pmod{32}$.
To get the solutions to the equation $x^2 \equiv 33 \pmod{64}$, 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

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

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 $-(x_1 + 32) \equiv -49 \equiv 15 \pmod{64}$.