Name:

Problem 1: *Please solve the following quadratic congruence:*

$$x^2 \equiv 7 \pmod{3^3}$$

Solution: We apply the method from class. First we solve

$$x^2 \equiv 7 \pmod 3.$$

Since $7 \equiv 1 \pmod 3$, really we solve $x^2 \equiv 1 \pmod 3$ which has solution $x \equiv 1 \pmod 3$.

We now do the first lifting step. Our goal is to solve $x_1^2 \equiv 7 \pmod 9$, with the assumption that x_1 is a lift modulo 9 of $x_0 \equiv 1 \pmod 3$. Therefore we have

$$x_1 = 1 + 3y_0,$$

with $y_0 = 0, 1$ or 2. Squaring both sides we get

$$x_1^2 = (1 + 3y_0)^2 = 1 + 6y_0 + 9y_0^2.$$

Therefore we are looking for y_0 such that

$$1 + 6y_0 \equiv 7 \pmod 9,$$

which is the same as

$$6y_0 \equiv 6 \pmod 9.$$

Since 6 is not a unit modulo 9, we must divide through by 3 to solve instead

$$2y_0 \equiv 2 \pmod 3.$$

Now 2 is a unit and we get $y_0 = 1$, so $x_1 = 1 + 3 = 4$. Indeed $4^2 \equiv 7 \pmod 9$.

We now do the second lifting step. Our goal is to solve $x_1^2 \equiv 7 \pmod{27}$, with the assumption that x_1 is a lift modulo 27 of $x_0 \equiv 4 \pmod 9$. Therefore we have

$$x_1 = 4 + 9y_0,$$

with $y_0 = 0, 1$ or 2. Squaring both sides we get

$$x_1^2 = (4 + 9y_0)^2 = 16 + 72y_0 + 81y_0^2.$$

Therefore we are looking for y_0 such that

$$16 + 72y_0 \equiv 7 \pmod{27},$$

which is the same as

$$18y_0 \equiv -9 \pmod{27}.$$

Since 18 is not a unit modulo 27 and $\gcd(18, 27) = 9$, we divide through by 9 to get

$$2y_0 \equiv -1 \pmod 3.$$

Since $-1 \equiv 2 \pmod 3$, this is the same as

$$2y_0 \equiv 2 \pmod 3$$

and since 2 is a unit modulo 3 we can divide both sides by 2 to obtain $y_0 = 1$. Therefore $x_1 = 4 + 9 \cdot 1 = 13$ and $x_1 \equiv 13 \pmod{27}$ is a solution to $x^2 \equiv 7 \pmod{27}$.

Since 27 is a power of an odd prime, there are two solutions to this quadratic congruence and the other solution is $x \equiv -13 \equiv 14 \pmod{27}$.

Therefore the two solutions are $x \equiv 13 \pmod{27}$ and $x \equiv 14 \pmod{27}$.