Problem 1. Suppose $p$ is a prime number and $p \equiv 1 \mod 4$. Then $\mathbb{Z}_p$ contains a square root of $-1$. In fact, $\frac{p-1}{2}$! times itself if $-1 \mod p$.

(Later in the course we will be able to show that if $p \equiv 3 \mod 4$ then $\mathbb{Z}_p$ does not have a square root of $1$.)

Problem 2. There are infinitely many primes $p$ with the property that $p \equiv 2 \mod 3$. (Hint: adapt the proof from class that there are infinitely many primes.)

Problem 3. Use Hensel’s lemma to find all solutions to $2x^2 - 66x - 81 \equiv 0 \mod 125$.

Problem 4. Let $p$ be an odd prime. For every $n \geq 1$, find all solutions to $x^2 \equiv 1 \mod p^n$. (Hint: for every $n$, there are two solutions. It is possible to do this without Hensel’s Lemma, but I want you to use it.)

Problem 5. How many solutions are there to the congruence $x^3 \equiv 5 \mod 65536$? Prove your answer. (Hint: computer scientists will recognize the modulus as a certain power of a prime. Also, you do not need to find all solutions—just say how many there are. State your reasoning clearly.)