Squares and square roots modulo m

In this activity, we'll look at squares and square roots in $\mathbb{Z}/m\mathbb{Z}$. For example, 8 is a square in $\mathbb{Z}/17\mathbb{Z}$ because $8 \equiv 5^2 \pmod{17}$. This suggests several questions that we might want to answer:

- Is every element of $\mathbb{Z}/m\mathbb{Z}$ a square? If not, can we conveniently determine whether a given element of $\mathbb{Z}/m\mathbb{Z}$ is a square?
- If $x \in \mathbb{Z}/m\mathbb{Z}$ is a square, how many square roots does it have?
- If $x \in \mathbb{Z}/m\mathbb{Z}$ is a square, can we conveniently find a square root of x? Can we conveniently find all the square roots of x?

We'll try to partially answer some of these questions today, but some of them will be too difficult for now. In fact, these questions lead to some very interesting math, which you'll probably see if you take a number theory course.

1. Find all solutions to the equation $X^2 = 1$ in $\mathbb{Z}/15\mathbb{Z}$. (Equivalently, find all solutions of the congruence $n^2 \equiv 1 \pmod{15}$.) Note that there are more than two solutions: this shows that an element of $\mathbb{Z}/15\mathbb{Z}$ can have more than two square roots. This differs from the situation in $\mathbb{R}$, where no number has more than two square roots.
2. Prove that 3 has exactly one square root in $\mathbb{Z}/6\mathbb{Z}$.
3. Is 2 a square in $\mathbb{Z}/7\mathbb{Z}$? What about 3? If they are squares, find all of their square roots.
4. Suppose m is odd. Prove that if x is a square in $\mathbb{Z}/m\mathbb{Z}$, then x has at least two square roots in $\mathbb{Z}/m\mathbb{Z}$. Problem 2 shows that this claim may not be true if m is even, so make sure you understand why your proof doesn't work if m is even. (Hint: If a is a square root of x, what is another square root of x?)
5. Prove that if p is an odd prime, then any nonzero element of $\mathbb{Z}/p\mathbb{Z}$ has either zero or two square roots. In other words, if $x \in \mathbb{Z}/p\mathbb{Z}$ is a nonzero square, then x has exactly two square roots in $\mathbb{Z}/p\mathbb{Z}$. (Hint: This statement is also true for $\mathbb{R}$. How do we prove it there? Try to mimic that proof in $\mathbb{Z}/p\mathbb{Z}$. Since we've seen that the claim is false for $\mathbb{Z}/15\mathbb{Z}$, you'll need to use a special property that is shared by $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{R}$, but not $\mathbb{Z}/15\mathbb{Z}$. What properties of $\mathbb{Z}/p\mathbb{Z}$ did we see in lecture?)
6. Let p be an odd prime. How many squares are there in $\mathbb{Z}/p\mathbb{Z}$? Prove your answer.