My office hours: Monday 2:00 pm - 3:00 pm, or by appointment, in JWB 323.

Squares mod p / squares in $\mathbb{F}_p$.

Recall which real numbers are squares?

All non-negative real numbers are squares - e.g., $2 = (\sqrt{2})^2$.

All negative real numbers are not squares (of a real number).
Which integers are squares (of integers) 0, 1, 4, 9, 16, 25, ... 

(Or: in the prime factorization non-negative \( n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \), all exponents \( e_i \) are even)

Which elements of \( \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \) are squares? (which \( 0 \leq x \leq p-1 \) are congruent to the square of any integer mod \( p \)?)
Examples:

$p = 3$

$F_3$

$0, 1, 2$ $0^2 = 0$ $1^2 = 1$ $2^2 = 1$

$0, 1$ are square

$2$ is not a square.

$p = 5$

$F_5$

$0, 1, 2, 3, 4$

$0^2 = 0$ $1^2 = 1$ $2^2 = 4$ $3^2 = 4$ $4^2 = 1$

$0, 1, 4$ are square

$2, 3$ are not.
p = 7 \quad \mathbb{F}_7

0, 1, 2, 4 \quad 7 \quad \frac{5}{6}

-3 \quad -2 \quad -1

0^2 = 0 \quad 1^2 = 1 \quad 2^2 = 4

3^2 = 2 \quad 4^2 = (-2)^2 = 5 \equiv 2

6^2 = (-1)^2 = 1

0, 1, 2, 4 \quad \text{squares mod } 7

3, 5, 6 \quad \text{not squares mod } 7.

In general - to compute square in \( \mathbb{F}_p \), square everythings up to \( \frac{p-1}{2} \). (negative trick)
Compute squares in \( \mathbb{F}_{11} \) for all \( p \leq 3 \)
and \( \mathbb{F}_{m} \)-squares.

Things in \( \mathbb{F}_{11} \) are \( x = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 \).

A square in \( \mathbb{F}_{11} \) is something I can get as \( x^2 \) for \( x \) in \( \mathbb{F}_{11} \).

\[
\begin{array}{cccccccccc}
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\
\hline
x^2 & 0 & 1 & 4 & 9 & 3 & 5 & 3 & 5 & 9 & 4 & 1 \\
\end{array}
\]

These are the squares in \( \mathbb{F}_{11} \).

Squares in \( \mathbb{F}_{11} \): 0, 1, 3, 4, 5, 9 (or squares mod 11)

Non-squares in \( \mathbb{F}_{11} \) (everything else): 2, 6, 7, 8, 10
Odd Primes \leq 31: 3, 5, 7, 11, 13, 17, 19, 23, 29, 31

Q: How many non-zero squares are there in \( \mathbb{F}_p \)? (Give a simple formula in terms of \( p \)). (Then try to justify).

A: \( \frac{p-1}{2} \)

Justification:

At most \( \frac{p-1}{2} \)
because to make the list I only have to square \( x \) up to \( \frac{p-1}{2} \) because \( x^2 = (-x)^2 \).
Tricky part: why do you get $\frac{p-1}{2}$ distinct things?

Hint: for any $k$ in $\mathbb{F}_p$,

\[ x^2 - k \text{ has at most } \leq 2 \text{ roots in } \mathbb{F}_p \]

Root of this is something that squares to $k$.

E.g. in $\mathbb{F}_{17}$: why $3^2 \neq 5^2$ \( (3, 5 \leq \frac{17-1}{2}) \)

$3$ is a root of $x^2 - 3^2$

$-3$ is also a root of $x^2 - 3^2$
So 3 and -3 are the only roots.

So if $s^2 = s^2$ then

$s$ is a root of $x^2 - 3^2$

So $s = 3$ or $s = -3 \mod 17$

Neither is true!

So $3^2 \neq 5^2$.

Doesn't happen because

$3, s \leq \frac{p-1}{2}$

$-3 \leq p-3 > \frac{p-1}{2}$.
Exercise 2: Finding some patterns,

Hint: Consider \( p \mod \text{power of } 2 \) for all prime \( p \).

1. \(-1\) is a square mod \( p \) \( \iff \) \( p \equiv 1 \mod 4 \)
2. Depends on \( p \mod 8 \).
3. Depends on both \( p \) and \( q \) mod 4.