My office hours: Monday 2:00pm - 3:00pm.
or by appointment.
in JWB 323.
Summer's still online.

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

<u>Recall</u> 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)?

$0, 1, 4, 9, 16, 25, \ldots$

(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 $0 \leq k \leq p-1$ are congruent to the square of any integer mod p?)

Examples:

$p=3$ $\quad \mathbb{F}_3$ $\quad 0, 1, 2$ $\quad 0^2=0$ $\quad 1^2=1$ $\quad 2^2=1$

0, 1 are squares

2 is not a square.

$p=5$ $\quad \mathbb{F}_5$ $\quad 0, 1, 2, 3, 4$

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

$3^2=4 \quad 4^2=1$

0, 1, 4 are squares

2, 3 are not.

$p = 7$ $\quad \mathbb{F}_7$ $\quad 0, 1, 2, 3, \underset{-3}{\underset{\shortparallel}{4}}, \underset{-2}{\underset{\shortparallel}{5}}, \underset{-1}{\underset{\shortparallel}{6}}$

$0^2 \equiv 0 \quad 1^2 \equiv 1 \quad 2^2 \equiv 4$

$3^2 \equiv 2 \quad 4^2 \equiv (-3)^2 \equiv 3^2 \equiv 2$

$5^2 \equiv (-2)^2 \equiv 4$

$6^2 \equiv (-1)^2 \equiv 1$

$0, 1, 2, 4$ squares mod 7

$3, 5, 6$ not squares mod 7.

In general — to compute squares in $\mathbb{F}_p$,

square everything up to $\frac{p-1}{2}$. (negative trick)

Compute squares in $\mathbb{F}_p$ for all $p \leq 31$ and non-squares.

$\mathbb{F}_{11}$ 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 $\mathbb{F}_{11}$.

x	0	1	2	3	4	5	6 (-5)	7 (-4)	8 (-3)	9 (-2)	10 (-1)
x^2	0	1	4	9	5	3	3	5	9	4	1

repeat.

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 ≤ 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 $\mathbb{F}_p$, $x^2 - K$ has at most 2 roots in $\mathbb{F}_p$

root of this is something that squares to K.

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

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 $3^2 = 5^2$ then

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

so $5 \equiv 3$ or $5 \equiv -3 \mod 17$

Neither is true!

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

doesn't happen because

$3, 5 \leq \frac{p-1}{2}$

$-3 \equiv p-3 > \frac{p-1}{2}$.

Exercie 2: Finding some patterns.

Hint: Consider p mod powers of 2.

(1) -1 is a square mod p (odd prime) $\iff$ $p \equiv 1 \bmod 4$

(2) Depends on p mod 8.

(3) Depends on both p and q mod 4