Math 4400
Week 9 - Thursday
The Legendre symbol

In class on Tuesday:

What are the squares in $\mathbb{F}_p$?

(= what are the squares mod p).

$0, 1, 4, 9, 16, 25, \ldots$ reduce these mod p

Example: Squares in $\mathbb{F}_{13}$ $\quad 7^2 = (-6)^2 = 6^2$

								-6	-5	-4	-3	-2	-1
x	0	1	2	3	4	5	6	7	8	9	10	11	12
x^2	0	1	4	9	3	12	10	10	12	3	9	4	1

In general can go up to $\frac{p-1}{2}$.

Squares: $0, 1, 3, 4, 9, 10, 12$

Non-squares: $2, 5, 6, 7, 8, 11$

Always $\frac{p-1}{2}$ nonzero squares / non-squares.

Patterns that can be observed:

For p an odd prime:

Ex 2-(1): -1 is a square in $\mathbb{F}_p \iff p \equiv 1 \bmod 4$

Ex 2-(2): 2 is a square in $\mathbb{F}_p \iff p \equiv 1$ or $7 \bmod 8$

Ex 2-(3): p, q odd primes:

If at least one of $p, q \equiv 1 \bmod 4$, p is a square in $\mathbb{F}_q$ $\iff$ q is a square in $\mathbb{F}_p$

e.g. $p=5$ $q=11$

If both $p, q \equiv 3 \bmod 4$, p is a square in $\mathbb{F}_q$ $\iff$ q is not a square in $\mathbb{F}_p$

e.g. $p=3$ $q=7$

$-1 \equiv 4 \equiv 2^2 \bmod 5$ $\quad -1 \equiv 12 \equiv 5^2 \bmod 13$

$5, 13 \equiv 1 \bmod 4$

Example:
- -1 is a square in $\mathbb{F}_5$, $\mathbb{F}_{13}$,
  not a square in $\mathbb{F}_3$, $\mathbb{F}_7$, $\mathbb{F}_{11}$.

$3^2 \equiv 2 \bmod 7$ $\quad 7 \equiv 7 \bmod 8$ $\quad 17 \equiv 1 \bmod 8.$

- 2 is a square in $\mathbb{F}_7$, $\mathbb{F}_{17}$ $\quad 6^2 \equiv 2 \bmod 17$
  not a square in $\mathbb{F}_3$, $\mathbb{F}_5$, $\mathbb{F}_{11}$, $\mathbb{F}_{13}$

$p \equiv 3 \bmod 8$ $\quad p \equiv 5 \bmod 8$.

- 5 is a square mod 11 $\quad 5 \equiv 4^2 \bmod 11$

$p=5,\ q=11$
$p\equiv 1 \bmod 4$

11 <u>is</u> a square mod 5
$11\equiv 1\equiv 1^2 \bmod 5$.

3 <u>is not</u> a square mod 5

$5\equiv 1 \bmod 4$

5 <u>is not</u> a square mod 3
$5\equiv 2 \bmod 3$

$3,7\equiv 3 \bmod 4$

3 <u>is not</u> a square mod 7
$7\equiv 1 \bmod 3$ is a square mod 3.

(quadratic reciprocity).

Definition: For p a prime and n an integer $p\nmid n$

$$\left(\frac{n}{p}\right)=\begin{cases}1 & \text{if } n \text{ is a square mod } p\\ -1 & \text{if } n \text{ is not a square mod } p\end{cases}$$

The Legendre symbol.

Example: $\left(\frac{18}{5}\right)=-1$ because $18\equiv 3 \bmod 5$ is not a square (squares mod 5 are $0,1,4$).

(Properties of the Legendre symbol)
Theorem: Let p be an odd prime

- $\left(\frac{n}{p}\right)=\left(\frac{m}{p}\right)$ if $n\equiv m \bmod p$.

- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ [multiplicativity]
- $\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \bmod 4 \\ -1 & \text{if } p \equiv 3 \bmod 4 \end{cases}$
- $\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 7 \bmod 8 \\ -1 & \text{if } p \equiv 3 \text{ or } 5 \bmod 8 \end{cases}$
- $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$ if q is another odd prime

$\Updownarrow$

$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ if one of p or $q \equiv 1 \bmod 4$

$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ if both $p, q \equiv 3 \bmod 4$

[quadratic reciprocity]

Example: Is 39 a square mod 59?

(39) (3 · 13)

Compute $\left(\frac{\ }{59}\right) = \left(\frac{\ }{59}\right)$

$3, 59 \equiv 3 \bmod 4.$

quadratic recip. $= \left(\frac{3}{59}\right)\left(\frac{13}{59}\right)$

$\left(\frac{3}{59}\right) = -\left(\frac{59}{3}\right)$

$= -\left(\frac{2}{3}\right)$

$= -(-1)$

$= 1$

$= \left(\frac{13}{59}\right)$

$= \left(\frac{59}{13}\right)$ quadratic recip. ($13 \equiv 1 \bmod 4$).

$= \left(\frac{7}{13}\right)$

$= -1$ by looking at table

(could also use qr again
$\left(\frac{13}{7}\right) = \left(\frac{6}{7}\right)$
$= \left(\frac{-1}{7}\right)$
$= -1$.)

39 is not a square mod 59