Math 4400
Week 10 - Thursday
Quadratic Reciprocity.

Extended Example:

Properties of Legendre symbol imply (if we assume they hold!)

$$\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = \begin{cases} 1 \text{ if } p \equiv 1 \bmod 3 \\ 2 \text{ if } p \equiv 2 \bmod 3 \end{cases}$$

How can we justify this directly?

If $p \equiv 1 \bmod 3$, need to show -3 is a square mod p.
If $p \equiv 2 \bmod 3$, need to show -3 is <u>not</u> a square mod p.

First case is easier. Suppose $p \equiv 1 \bmod 3$.

Then by Exercise 2-(5), I can choose

a primitive 3rd root of unity ζ in $\mathbb{F}_p$.

Reason: $\zeta^3 = 1$ $\overset{\text{disc. log}}{\Longrightarrow}$ $3I(\zeta) = 0$

$\zeta \neq 1$ $\qquad$ $I(\zeta) \neq 0$

$I(\zeta)$ in $\mathbb{Z}/(p-1)\mathbb{Z}$; when is there a non-zero solution to $3y = 0$ in $\mathbb{Z}/(p-1)\mathbb{Z}$

Claim: $\zeta - \zeta^2$ is a square root of -3 in $\mathbb{F}_p$,

i.e. $$(\zeta - \zeta^2)^2 = -3 \text{ in } \mathbb{F}_p.$$

$\zeta^3 = 1$

Justification: $$(\zeta - \zeta^2)^2 = \zeta^2 - 2\zeta^3 + \zeta^4$$
$$= \zeta^2 - 2 + \zeta$$
$$= \zeta^2 + \zeta - 2.$$

Need to see that $\zeta^2 + \zeta = -1$.

<u>But</u> ζ is a root of $\frac{x^3 - 1}{x - 1} = x^2 + x + 1$

(because ζ is a <u>primitive</u> 3rd root of unity)

so $\zeta^2 + \zeta + 1 = 0 \Rightarrow \zeta^2 + \zeta = -1$.

So $(\zeta^2 - \zeta)^2 = \zeta^2 + \zeta - 2 = -1 - 2 = -3$.

$\zeta^2 - \zeta \in \mathbb{F}_p$, so -3 is a square mod p. ✓

What if $p \equiv 2 \bmod 3$?

There's no primitive 3rd root in $\mathbb{F}_p$ (same exercise)

$\Rightarrow$ formula doesn't work

... But couldn't there still be a square root of -3?

No, because can reverse formula:

Recall – in $\mathbb{C}$, $e^{2\pi i/3} = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}$

$$= \frac{-1 + i\sqrt{3}}{2}$$

is a primitive 3rd root of unity.

In fact, in any field where we can divide by 2, if $\alpha^2 = -3$, then

$\frac{-1+\alpha}{2}$ is a primitive 3rd root of unity.

(Can check by expanding $\left(\frac{-1+\alpha}{2}\right)^3$).

This example, when combined with $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)$ and computation of $\left(\frac{-1}{p}\right)$, actually gives quadratic reciprocity for $p=3$

$$\left(\frac{3}{q}\right) = (-1)^{\frac{q-1}{2}}\left(\frac{q}{3}\right)$$

It gets harder for $p > 3$. Still have formula for square root in terms of a primitive pth root of unity.

odd prime

Theorem (Gauss): If ζ is a primitive pth root of unity in a field $\mathbb{K}$, then

$$\left(\sum_{i=1}^{p-1}\left(\frac{i}{p}\right)\zeta^i\right)^2 = (-1)^{\frac{p-1}{2}} p.$$

$$= \begin{cases} p & \text{if } p \equiv 1 \bmod 4 \\ -p & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

Example: If ζ is a primitive 5th root of unity,

$$\left(\zeta + \zeta^4 - \zeta^2 - \zeta^3\right)^2 = 5$$

[see homework]

But now all this gives directly is:

If $q \equiv 1 \bmod p$ then there is a primitive pth root of unity in $\mathbb{F}_q$ thus a square root of $(-1)^{\frac{p-1}{2}} p$.

$$\Rightarrow \left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \underbrace{\left(\frac{q}{p}\right)} = (-1)^{\frac{(p-1)(q-1)}{4}}$$

because $q \equiv 1 \bmod p$, $= \left(\frac{1}{p}\right) = 1$.

In particular, can't reverse formula for $p > 3$ to go from square root to primitive pth root of unity.

Main idea: can always work in a bigger field than $\mathbb{F}_q$ to get a primitive pth root of unity, then check when formula lands in $\mathbb{F}_q$.

like going from $\mathbb{R}$ to $\mathbb{C}$

The same ideas show up in justifying

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 7 \bmod 8 \\ -1 & \text{if } p \equiv 3, 5 \bmod 8 \end{cases}$$

but simpler; we will spend rest of lecture explaining this.

Fact 1: If ζ is a primitive 8th root of unity then

$$(\zeta + \zeta^7)^2 = 2$$

see homework

(can justify like formula for $\sqrt{-3}$, but here no way to reverse it)

Fact 2: If p is an odd prime and $\mathbb{F}_{p^2}$ is a field of order p^2, then $\mathbb{F}_{p^2}$ has a primitive 8th root of unity.

Why? $\mathbb{F}_{p^2}^\times \cong \mathbb{Z}/(p^2-1)\mathbb{Z}$. So has
like discrete log.

a primitive 8th root of unity if $8 \mid (p^2-1)$

But in fact this holds for any odd p.

(compute squares in $\mathbb{Z}/8\mathbb{Z}$ to see this).

Fact 3: If p is an odd prime, there exists a field of order p^2.

If $d \in \mathbb{F}_p$ is not a square ($\frac{p-1}{2}$ choices), then $x^2 - d$ is an irreducible polynomial in $\mathbb{F}_p[x]$

$\mathbb{F}_p[x]/(x^2-d)$ is a field.

elements are $a + bx$, $a, b \in \mathbb{F}_p$
so p^2 elements

So let p be an odd prime, let $\mathbb{F}_{p^2}$ be a field of order p^2, and let ζ be a primitive 8th root of unity in $\mathbb{F}_{p^2}$, so that

$$(\zeta+\zeta^7)^2 = 2.$$

The <u>only</u> two square roots of 2 in $\mathbb{F}_{p^2}$ are $(\zeta+\zeta^7)$ and $-(\zeta+\zeta^7) = \zeta^4(\zeta+\zeta^7) = \zeta^5+\zeta^3$.

$\zeta^4=-1$ since $\zeta^4 \neq 1$ and $(\zeta^4)^2=1$.

Fact 4: An element $\alpha \in \mathbb{F}_{p^2}$ is in $\mathbb{F}_p \iff \alpha^p = \alpha$.

Like: $z \in \mathbb{C}$ then $z \in \mathbb{R} \iff z = \bar{z}$

<u>Step 1</u> $\alpha^p = \alpha \iff \alpha^p - \alpha = 0$

$\iff \alpha$ is a root of $x^p - x$

$x(x^{p-1}-1)$

0 is a root

$\mathbb{F}_p = 0 \cup \mathbb{F}_p^\times$

By Lagrange, all elements in $\mathbb{F}_p^\times$ are roots

$x^p - x$ has degree p

$\mathbb{F}_p$ gives p roots, so there aren't any others!

Remains only to check when

$$(\zeta+\zeta^7)^p = \zeta+\zeta^7$$

Fact 5: In $\mathbb{F}_{p^2}$ (or any field containing $\mathbb{F}_p$),

$(a+b)^p = a^p + b^p$

Admitting this, $(\zeta + \zeta^7)^p = \underline{\zeta^p + \zeta^{7p}}$

depends on p mod 8 because $\zeta^8 = 1$.

$p \equiv 1 \bmod 8$ this is $\zeta^1 + \zeta^7$ so $\zeta + \zeta^7 \in \mathbb{F}_p$

$p \equiv 3 \bmod 8$ get $\zeta^3 + \zeta^5 = -(\zeta + \zeta^7)$

so $\zeta + \zeta^7 \notin \mathbb{F}_p$

$p \equiv 5 \bmod 8$ get $\zeta^3 + \zeta^5 = -(\zeta + \zeta^7)$ not in $\mathbb{F}_p$.

$p \equiv 7 \bmod 8$ get $\zeta^7 + \zeta = \zeta + \zeta^7$

so in $\mathbb{F}_p$

$\pm\sqrt{2} = \pm(\zeta + \zeta^7)$ is in $\mathbb{F}_p$ for $p \equiv 1, 7 \bmod 8$

not in $\mathbb{F}_p$ for $p \equiv 3, 5 \bmod 8$.

i.e. $\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 7 \bmod 8 \\ -1 & \text{if } p \equiv 3 \text{ or } 5 \bmod 8 \end{cases}$

Justification of the Fact:

Fact 5: In $\mathbb{F}_{p^2}$ (or any field containing $\mathbb{F}_p$),

$(a+b)^p = a^p + b^p$

Example: $p = 3$ $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$

$= a^3 + b^3$ in $\mathbb{F}_p$

because $3 = 0$ in $\mathbb{F}_p$

In general $\quad (a+b)(a+b)(a+b)\dots(a+b)$

$$(a+b)^n = a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \dots + \binom{n}{n-1}ab^{n-1} + b^n.$$

$\binom{n}{i}$ binomial coefficients / choose function

Saw on an earlier worksheet given by rows in Pascal's triangle

$$\begin{array}{ccccccc} & & & 1 & & & \\ & & 1 & & 1 & & \\ & 1 & & 2 & & 1 & \\ 1 & & 3 & & 3 & & 1 \end{array}$$

Saw in that exercise is that the p+1 st row of Pascal's triangle is zero mod p except 1's on either side.

$$(a+b)^p = a^p + \underline{\binom{p}{1}}a^{p-1}b \,\underline{\ \ }+ \dots \underline{\ \ }+ b^p$$

Coefficients are zero mod p

$(a+b)^p = a^p + b^p$ whenever $p=0$

e.g. in $\mathbb{F}_{p^2}$ or $\mathbb{F}_p$.