Math 4400
Week 10 - Tuesday

A Formula for the Legendre symbol

Recall from last week:

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.

Theorem: For p an odd prime,

$$\left(\frac{n}{p}\right) = n^{\frac{p-1}{2}} \mod p.$$

Example: $p=7$. Non-zero squares: $1, 2, 4$.

$3 = \frac{7-1}{2}$

n	1	2	3	4	5	6
$\left(\frac{n}{7}\right)$	1	1	-1	1	-1	-1
$n^3 \mod 7$	1	1	-1	1	-1	-1

note $(-n)^3 = -(n^3)$.

Assuming this formula, get immediately:

(1) Multiplicativity: $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$

$a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv (ab)^{\frac{p-1}{2}} \mod p$

(2) $\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \mod 4 \\ -1 & \text{if } p \equiv 3 \mod 4. \end{cases}$

If $p \equiv 1 \mod 4$ $\quad p = 4k+1$

$(-1)^{\frac{p-1}{2}} = (-1)^{\frac{4k}{2}} = (-1)^{2k} = 1$ even

If $p \equiv 3 \bmod 4$ $\quad p = 4k+3$ $\quad$ odd

$$(-1)^{\frac{p-1}{2}} = (-1)^{\frac{4k+2}{2}} = (-1)^{2k+1} = -1.$$

Proof of theorem:

$$\left(n^{\frac{p-1}{2}}\right)^2 \equiv n^{p-1} \equiv 1 \bmod p \text{ by Lagrange.}$$

so $n^{\frac{p-1}{2}} = 1$ or -1 in $\mathbb{F}_p$.
(only solution of $x^2=1$ in $\mathbb{F}_p \leftrightarrow$ roots of x^2-1).

Thus, suffices to show:

$$n^{\frac{p-1}{2}} \equiv 1 \bmod p \iff n \text{ is a square mod } p.$$

if not $\quad n^{\frac{p-1}{2}} \equiv -1 \bmod p \iff n$ is not a square mod p.

Choose a primitive root g for $\mathbb{F}_p$, and let $I : \mathbb{F}_p^\times \to \mathbb{Z}/(p-1)\mathbb{Z}$ be the corresponding discrete log

$$I(g^k) = k.$$

see week 7 - Tuesday

Example: $p=7$, $g=3$,

n	1	2	3	4	5	6	(in $\mathbb{F}_7^\times$)
$I(n)$	0	2	1	4	5	3	(in $\mathbb{Z}/6\mathbb{Z}$)

① n is a square mod $p \iff I(n)$ is even

this makes sense because $2 \mid p-1$.

Example:

n	1	2	3	4	5	6	(in $\mathbb{F}_7^\times$)
$I(n)$	0	2	1	4	5	3	(in $\mathbb{Z}/6\mathbb{Z}$)

$n = x^2 \Rightarrow I(n) = I(x^2) = 2I(x)$ even ✓

if $I(n)$ even $\Rightarrow I(n) = 2y \Rightarrow n = g^{2y} = (g^y)^2$

$g^{I(n)}$

so n is square. ✓

② $I(n)$ is even $\iff \frac{p-1}{2} \cdot I(n) = 0$ in $\mathbb{Z}/p-1\mathbb{Z}$

$$\iff I\left(n^{\frac{p-1}{2}}\right) = 0$$

$$\iff n^{\frac{p-1}{2}} = g^0 = 1.$$

Example:

n	1	2	3	4	5	6	(in $\mathbb{F}_7^\times$)
$I(n)$	0	2	1	4	5	3	(in $\mathbb{Z}/6\mathbb{Z}$)
$3I(n)$	0	0	3	0	3	3	(in $\mathbb{Z}/6\mathbb{Z}$)

$\blacksquare$

Proof of theorem is finished.

Have established:

- $\left(\frac{n}{p}\right) = n^{\frac{p-1}{2}} \mod p$

and as a consequence:

- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
- $\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \mod 4 \\ -1 & \text{if } p \equiv 3 \mod 4 \end{cases}$

Remains for the rest of the week:

- Justify the formula for

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

- Justify quadratic reciprocity

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{if } p \text{ or } q \equiv 1 \bmod 4 \\ -\left(\frac{q}{p}\right) & \text{if } p \text{ and } q \equiv 3 \bmod 4. \end{cases}$$

← root of $x^2 - d$

For both: express square roots using roots of unity (roots of $x^n - 1$)

(Worksheet + Thursday video)