Lecture 9.1

Last time:

- a is a **quadratic residue** mod p if any of the following are true:
  - $x^2 \equiv a \pmod{p}$ has a solution
  - $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.
- Otherwise a is a **quadratic non-residue**, which is equivalent to either of:
  - $x^2 \equiv a \pmod{p}$ has no solutions
  - $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.
- The **Legendre symbol** or **quadratic residue symbol** of a mod p is

$$\left(\frac{a}{p}\right) := a^{\frac{p-1}{2}} \pmod{p}$$

By the above,

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & a \text{ is a QR mod } p \\ -1, & a \text{ is a NR mod } p \end{cases}$$

Theorem For any $a, b \in \mathbb{Z}$ not divisible by p, $\left(\frac{\cdot}{p}\right)$ has the following properties:

(a) $\left(\frac{a^2}{p}\right) = 1$

(b) If $a \equiv b \pmod{p}$ then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(c) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Exercise 1: Prove this Theorem.

Exercise 2: Compute each of the following quadratic residue symbols. If $\left(\frac{a}{p}\right) = 1$, find all solutions to $x^2 \equiv a \pmod{p}$.

(a) $\left(\frac{3}{13}\right)$

(b) $\left(\frac{13}{3}\right)$

(c) $\left(\frac{11}{13}\right)$

(d) $\left(\frac{13}{11}\right)$

(e) $\left(\frac{2}{7}\right)$

(f) $\left(\frac{6}{7}\right)$

(g) $\left(\frac{75}{97}\right)$

(h) $\left(\frac{12}{109}\right)$

Ex Let's use $\left(\frac{\cdot}{p}\right)$ to analyze the congruence $x^2 \equiv -1 \pmod{p}$, i.e. answer the question "which primes p divide numbers of the form x^2+1?"

We know $x^2 \equiv -1 \pmod{p}$ has a solution if and only if $\left(\frac{-1}{p}\right) = 1$, but

$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ which is 1 if $\frac{p-1}{2}$ is even and -1 if $\frac{p-1}{2}$ is odd.

These conditions are just:

$$\frac{p-1}{2} = 2k \iff p-1 = 4k \iff p \equiv 1 \pmod{4}$$

$$\frac{p-1}{2} = 2k+1 \iff p-1 = 4k+2 \iff p \equiv 3 \pmod{4}.$$

This proves:

Theorem For $p > 2$ prime, $x^2 \equiv -1 \pmod{p}$ has a solution if and only if $p \equiv 1 \pmod{4}$.

Corollary The prime divisors of any number of the form $x^2 + 1$ are all of the form $p = 4k + 1$.

Theorem There are infinitely many primes $p \equiv 1 \pmod{4}$.

Exercise 3: Prove it!

Next, let's analyze $\left(\frac{2}{p}\right)$ for $p > 2$.

Here's a table of primes p and solutions to $x^2 \equiv 2 \pmod{p}$, if any exist.

p	3	5	7	11	13	17	19	23	29	31
$x^2 \equiv 2$	NR	NR	3, 4	NR	NR	6, 11	NR	5, 18	NR	8, 23

p	37	41	43	47	53	59	61	67	71	73
$x^2 \equiv 2$	NR	17, 24	NR	7, 40	NR	NR	NR	NR	12, 59	32, 41

p	79	83	89	97	101	103	107	109	113	127
$x^2 \equiv 2$	9, 70	NR	25, 64	14, 83	NR	38, 65	NR	NR	51, 62	16, 111

What patterns do you notice?

Guess:

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

It's not enough to just compute $2^{\frac{p-1}{2}}$ unfortunately.

Instead, consider the complete residue system

$$-\frac{p-1}{2}, \ldots, -1, 0, 1, \ldots, \frac{p-1}{2}.$$

We saw last time that the congruence classes $a, 2a, \ldots, \frac{p-1}{2}a$ can be used to compute $\left(\frac{a}{p}\right)$. Write

$$ia \equiv r_i \pmod{p}$$

for r_i in the above residue system.

Then $r_1 r_2 \cdots r_{\frac{p-1}{2}} \equiv a \cdot 2a \cdots \left(\frac{p-1}{2}\right)a$

$$\equiv a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod{p}.$$

On the other hand, if $r_i \equiv r_j$ then

$ia \equiv ja \pmod{p} \Rightarrow i = j$ as

we've seen before, so $r_1, \ldots, r_{\frac{p-1}{2}}$ are

distinct classes in the residue system

$$-\frac{p-1}{2}, \ldots, -1, 0, 1, \ldots, \frac{p-1}{2}.$$

As a result,

$$r_1 \cdots r_{\frac{p-1}{2}} \equiv (\pm 1)(\pm 2) \cdots \left(\pm \frac{p-1}{2}\right)$$

$$\equiv (-1)^g 1 \cdot 2 \cdots \frac{p-1}{2} \pmod{p}$$

for some g.

Lemma Let $p > 2$ be prime, $\gcd(a, p) = 1$ and let g be the number of negative classes of $a, 2a, \ldots, \frac{p-1}{2}a$ in the complete residue system $-\frac{p-1}{2}, \ldots, \frac{p-1}{2}$. Then

$$\left(\frac{a}{p}\right) = (-1)^g.$$

Pf: So far, we have

$$r_1 \cdots r_{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod{p}$$

and we just showed

$$r_1 \cdots r_{\frac{p-1}{2}} \equiv (-1)^g \left(\frac{p-1}{2}\right)! \pmod{p}.$$

Since $1, 2, \ldots, \frac{p-1}{2} < p$, we can cancel

the $\left(\frac{p-1}{2}\right)!$ term to get

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \equiv (-1)^g \pmod{p}. \quad \square$$

Theorem For any prime $p > 2$,

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

Pf: Suppose $p \equiv 1 \pmod 8$, say $p = 1 + 8k$

for $k \in \mathbb{N}$.

Then $\frac{p-1}{2} = 4k$ so we are looking for

which of $2, 4, \ldots, 2 \cdot 4k$ fall in

the congruence classes

$$-4k, \ldots, -1 \mod p.$$

The first half, $2, 4, \ldots, 4k$, are exactly the positive classes in this complete residue system, so the other half,

$$4k+2, \ldots, 8k,$$

fall into negative classes.

There are $g = 2k$ of these, so

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

The other cases are similar. □

Exercise 3: Prove the other cases.

Quadratic Reciprocity

Recall that for any $a, b \in \mathbb{Z}$ which are relatively prime to p,

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

This means that to understand the

This means that to [illegible]

symbol $\left(\frac{\cdot}{p}\right)$, it's enough to know

$\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$ and $\left(\frac{q}{p}\right)$

for all odd primes q.

Here's a table with a bunch of $\left(\frac{q}{p}\right)$

for primes p, q.

$p \backslash q$	3	5	7	11	13	17	19	23	29	31	37
3		−1	1	−1	1	−1	1	−1	−1	1	1
5	−1		−1	1	−1	−1	1	−1	1	1	−1
7	−1	−1		1	−1	−1	−1	1	1	−1	1
11	1	1	−1		−1	−1	−1	1	−1	1	1
13	1	−1	−1	−1		1	−1	1	1	−1	−1
17	−1	−1	−1	−1	1		1	−1	−1	−1	−1
19	−1	1	1	1	−1	1		1	−1	−1	−1
23	1	−1	−1	−1	1	−1	−1		1	1	−1
29	−1	1	1	−1	1	−1	−1	1		−1	−1

31	-1	1	1	-1	-1	-1	1	-1	-1		-1
37	1	-1	1	1	-1	-1	-1	-1	-1	-1	

Do you observe any patterns?

Here's one: reading across the 5 row and down the 5 column, it appears that $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$ for all $p \neq 5$.

Does this hold for any other q?

Looking at the table for a little longer, we might come up with the following

guess:

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \quad \text{if} \quad p \text{ or } q \equiv 1 \pmod 4$$

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right) \quad \text{if} \quad p \equiv q \equiv 3 \pmod 4.$$

This is in fact a famous theorem, which will take us another lecture to prove:

Theorem (Quadratic Reciprocity) Let p and q be distinct odd primes. Then

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

Ex Let's use this to see if there are solutions to $x^2 \equiv 14 \pmod{137}$.

We have

$$\left(\frac{14}{137}\right) = \left(\frac{2}{137}\right)\left(\frac{7}{137}\right).$$

Since $137 \equiv 1 \pmod 8$, $\left(\frac{2}{137}\right) = 1$ by our theorem earlier.

On the other hand, $137 \equiv 1 \pmod 4$

so by Quadratic Reciprocity,

$$\left(\frac{7}{137}\right) \quad \left(\frac{137}{4}\right) \quad \left(\frac{4}{3}\right)^2$$

$$\left(\frac{137}{7}\right) \equiv \left(\frac{4}{7}\right) \equiv \left(\frac{2}{7}\right) = \left(\frac{2}{7}\right) = 1.$$

Therefore $\left(\frac{14}{137}\right) = 1$ so $x^2 \equiv 14 \pmod{137}$

has solutions, namely $x \equiv 39, 98 \pmod{137}$.

Ex How about $x^2 \equiv 55 \pmod{179}$?

This time, $55 = 5 \cdot 11$ and

$5 \equiv 1 \pmod 4$ and $11, 179 \equiv 3 \pmod 4$.

So $$\left(\frac{55}{179}\right) = \left(\frac{5}{179}\right)\left(\frac{11}{179}\right)$$

$$= \left(\frac{179}{5}\right) \cdot -\left(\frac{179}{11}\right)$$

$$= -\left(\frac{4}{5}\right)\left(\frac{3}{11}\right)$$

$$= -\left(\frac{3}{11}\right)$$

since $3, 11 \equiv 3 \pmod 4$

$$= \left(\frac{11}{3}\right)$$

$$= \left(\frac{2}{3}\right) = -1$$ since 2 is not a square mod 3.

Therefore $x^2 \equiv 55 \pmod{179}$ has no solutions.

More generally, we may want to compute $\left(\frac{a}{p}\right)$ without knowing the prime factorization of a.

To do this, we can extend the definition

of $\left(\frac{\cdot}{\cdot}\right)$ to composite moduli by:

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)^{k_1} \cdots \left(\frac{a}{p_r}\right)^{k_r}$$

for any positive, odd b with prime factorization

$$b = p_1^{k_1} \cdots p_r^{k_r}.$$

Combining this with our reciprocity laws for $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$, we get a general reciprocity law for all $a, b \in \mathbb{Z}$.

Theorem Let $a, b \in \mathbb{Z}$ be relatively prime, with b odd and write $a = (-1)^i 2^j a'$

for odd $a' \in \mathbb{N}$. Then

$$\left(\frac{a}{b}\right) = \left(\frac{-1}{b}\right)^i \left(\frac{2}{b}\right)^j \left(\frac{a'}{b}\right)$$

and

(1) $$\left(\frac{-1}{b}\right) = \begin{cases} 1, & b \equiv 1 \pmod 4 \\ -1, & b \equiv 3 \pmod 4 \end{cases}$$

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

(3) $$\left(\frac{a'}{b}\right) = \begin{cases} \left(\frac{b}{a'}\right), & a' \text{ or } b \equiv 1 \pmod 4 \\ -\left(\frac{b}{a'}\right), & a', b \equiv 3 \pmod 4. \end{cases}$$

Next time: a proof of quadratic reciprocity.