LECTURE 16: (QUADRATIC RECIPROCITY: CHAPTER 9 OF STILLWELL'S Elements of Number Theory)

- primes of form x^2+y^2 are those of the linear form $4n+1$. found by Fermat
- what about primes of form x^2+dy^2 for nonsquare d? Are these also found from some linear form? Fermat studied x^2+2y^2, x^2+3y^2. Key to such study, the quadratic character of -2, -3 or -1 for x^2+y^2.

quadratic character of $-d$ is described by exhibiting the primes q such that $-d$ is square, mod q.

- THE LAW OF QUADRATIC RECIPROCITY describes when p is a square mod q for odd primes p & q

(the "law" is extended, or supplemented, with cases $p=-1$, $p=2$ to make the calculational set-up nice & easy)

Proof Sketch

- Euler's criterion: p a square mod q iff $p^{\frac{q-1}{2}} \equiv 1 \pmod q$

this is a major tool in the arguments.

- Chinese Remainder Th^{m} is used (I think the form here looks quite different from our earlier treatment)
- Legendre's Symbol $\left(\frac{p}{q}\right)$ — not a fraction! allows nice calculation from a few basic facts & rules.

(these comments are mysteries we will only understand after this lecture & perhaps 2 more are complete.)

§9.1 Primes x^2+y^2, x^2+2y^2 and x^2+3y^2

x^2+y^2: $p \mid m^2+1 \iff -1 \equiv m^2 \pmod p$

We used Wilson's Thm f-la for -1 to manipulate mod $p = 4n+1$ until it was clear -1 was congruent to a square mod p.

↪ for arbitrary $p, q \in \mathbb{Z}$ is q a square mod p?
Or what is the quadratic character of q, mod p?

x^2+2y^2: $p = x^2+2y^2 \iff p = 8n+1$ or $8n+3$

Proof follows similar path to 2-squares Thm, but with $\mathbb{Z}[\sqrt{-2}]$ eventually leads to problem of showing

$$-2 \equiv m^2 \pmod p$$

precisely when $p = 8n+1$ or $8n+3$.

x^2+3y^2: $p = x^2+3y^2 \iff p = 3n+1$

Again, proof similar, uses $\mathbb{Z}\left[\frac{-1+\sqrt{-3}}{2}\right]$ with step to show

$$-3 \equiv m^2 \pmod p$$

where $p = 3n+1$

(point here, simply that quadratic reciprocity is crucial to understanding our results thus far & how to generalize them)

Preliminary calculations on Quadratic Reciprocity

- Key to x^2+y^2 prime iff $p=4n+1$ based on $\underbrace{p \mid m^2+1}_{-1 \equiv m^2 \bmod p}$
- Key to x^2+2y^2 prime p iff $p=8n+1$ or $8n+3$ based on $\underbrace{p \mid m^2+2}_{-2 \equiv m^2 \bmod p}$
- Key to x^2+3y^2 prime p iff $p=3n+1$ need $\underbrace{p \mid m^2+3}_{-3 \equiv m^2 \bmod p}$

We see the determination of $q = m^2 \bmod p$ for some m is of importance. In other words, when is q a square modulo p?

~1750 EULER REALIZED knowing primes of form x^2+y^2, x^2+2y^2, x^2+3y^2 depends on whether p is a square mod q. In particular

CONJECTURE:

▷ When p and q are both of form $4n+3$ then

p is a square mod q $\iff$ q is not a square mod p

▷ otherwise,

p is a square mod q $\iff$ q is a square mod p.

Notation: Legendre's Symbol: (quadratic character symbol)

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

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$$ ← CONCISE VERSION OF EULER'S CONJECTURE

for odd primes p & q

▶ when p & q are both of form $4n+3$
then p is a square mod q iff q is not a square mod p

$$(-1)^{\left(\frac{4j+3-1}{2}\right)\left(\frac{4k+3-1}{2}\right)} = (-1)^{\frac{(4j+2)(4k+2)}{4}} = (-1)^{(2j+1)(2k+1)} = \underline{-1}.$$

$$\left(\frac{p}{q}\right) = \pm 1 \quad \& \quad \left(\frac{q}{p}\right) = \mp 1$$

$$\therefore \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (\pm 1)(\mp 1) = -1.$$

▶ Otherwise $p = 4j+3$ & ~~$q = 4k+3$~~ ~~or~~ $4k+1$
or $p = 4j+1$ and $q = 4k+1$ or $4k+3$

$$\frac{(p-1)(q-1)}{4} = \frac{1}{4}\begin{cases} \cancel{(4j+2)(4k+2)} = \cancel{4[2j+1](2k+1)} \\ (4j+2)(4k) = 4k(4j+2) \\ (4j)(4k) = 4k(4j) \\ (4j)(4k+2) = 4j(4k+2) \end{cases} \Leftarrow$$

$$= \left\{\begin{array}{l} k(2j+1)(2) \\ 4kj \\ 2j(2k+1) \end{array}\right\} \text{ even.}$$

$$(-1)^{\left(\frac{p-1}{4}\right)\left(\frac{q-1}{4}\right)} = (-1)^{2m} = \left((-1)^2\right)^m = 1.$$

↳ $$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1$$

$(1)(1) = 1$ — [both p and q squares mod q & p respectively]

$(-1)(-1) = 1$ — [p not square mod q; q not square mod p]

§9.5 THE STORY SO FAR:

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

Euler criterion

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

Multiplicative Property

$$\left(\frac{p_1}{q}\right)\left(\frac{p_2}{q}\right) = \left(\frac{p_1 p_2}{q}\right)$$

Supplements

$\left(\frac{-1}{q}\right) = 1 \iff q = 4n+1$ (I)

$\left(\frac{2}{q}\right) = 1 \iff q = 8n \pm 1$ (II)

To evaluate $\left(\frac{p}{q}\right)$ for odd primes need:

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

QUADRATIC RECIPROCITY LAW (see §9.8 for proof)

→ $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ if one of p, q is $4n+1$ format

→ $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ otherwise

- Also useful, $p \equiv p' \bmod q$

then p is square mod q iff p' is square mod q.

Hence $\left(\frac{p}{q}\right) = \left(\frac{p'}{q}\right)$ where p' is remainder of $\frac{p}{q}$.

Ex 1

$$\left(\frac{37}{59}\right) = \left(\frac{59}{37}\right) \quad \text{as } 37 = 36+1 = 4(9)+1$$

$$= \left(\frac{22}{37}\right) \quad \text{as } 59 \equiv 22 \bmod 37.$$

$$= \left(\frac{2}{37}\right)\left(\frac{11}{37}\right) \quad \text{by (II) } 37 \neq 8n \pm 1.$$

$$= -\left(\frac{11}{37}\right)$$

$$= -\left(\frac{37}{11}\right) = -\left(\frac{4}{11}\right) = -\left(\frac{2}{11}\right)^2 = -(-1)^2 = \boxed{-1}$$

$\therefore$ 37 not a square mod 59.

Extended Legendre symbol

$$\left(\frac{P}{q}\right) = \left(\frac{P_1 P_2 \cdots P_n}{q}\right) = \left(\frac{P_1}{q}\right)\left(\frac{P_2}{q}\right)\cdots\left(\frac{P_n}{q}\right)$$

Need to supplement ∞ for 2 and −1 to cover all possible $P \in \mathbb{Z}$, in particular,

(I) $\left(\frac{-1}{q}\right) = 1$ iff $q = 4n+1$ ← §2.3

(II) $\left(\frac{2}{q}\right) = 1$ iff $q = 8n \pm 1$ ← §2.4

[$\left(\frac{-1}{q}\right) = -1$ if $q \neq 4n+1$

$\left(\frac{2}{q}\right) = -1$ if $q \neq 8n \pm 1$.]

Examples:

E1 $\left(\frac{-2}{8n+1}\right) = \left(\frac{-1}{8n+1}\right)\left(\frac{2}{8n+1}\right)$

$= \left(\frac{-1}{4(2n)+1}\right)\left(\frac{2}{8n+1}\right) = 1.$

$\underbrace{\left(\frac{-1}{4(2n)+1}\right)}_{1\ (\text{I})}\underbrace{\left(\frac{2}{8n+1}\right)}_{1\ (\text{II})}$

E2 $\left(\frac{-2}{8n+3}\right) = \left(\frac{-1}{8n+3}\right)\left(\frac{2}{8n+3}\right) = \underbrace{(-1)}_{\text{(I)}}\underbrace{(-1)}_{\text{(II)}} = 1.$

E3 $\left(\frac{-3}{3n+1}\right) = \left(\frac{-1}{3n+1}\right)\left(\frac{3}{3n+1}\right) =$

$$\begin{cases} 1 \times \left(\frac{3}{3n+1}\right) & \text{if } 3n+1 = 4n'+1 \\ -1 \times \left(\frac{3}{3n+1}\right) & \text{if } 3n+1 \neq 4n'+1 \end{cases}$$

$$= \begin{cases} 1 \times \left(\frac{3}{3n+1}\right) & \text{if } 3n+1 = 4n'+1 \\ -1 \times -1 \times \left(\frac{3n+1}{3}\right) & \text{if } 3n+1 \neq 4n'+1 \end{cases}$$

next step ? p. 163

§9.3 Euler's Criterion

Fermat's little theorem says $a \not\equiv 0 \bmod q$ has $a^{\varphi(q)} \equiv 1 \bmod q$.
When q is prime, $\varphi(q) = q-1$ hence $\underline{a^{q-1} \equiv 1 \bmod q}$.

Euler's Criterion: For an odd prime q,

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

And hence,

p is square mod q $\iff$ $p^{\frac{q-1}{2}} \equiv 1 \pmod q$

Proof: by Lagrange's max-# of incongruent polynomial sol^{n} applied twice and the process of elimination. Assume q odd prime.

CASE 1: if $p \equiv a^2 \pmod q$ for some $a \in \mathbb{Z}$ then by def^{n} of Legendre symbol $\left(\frac{p}{q}\right) = 1$. Also,

$$p^{\frac{q-1}{2}} \equiv (a^2)^{\frac{q-1}{2}} \equiv a^{q-1} \equiv 1 \pmod q$$

by Fermat's little theorem. Thus $\left(\frac{p}{q}\right) \equiv p^{\frac{q-1}{2}}$ as claimed.

CASE 2: if $p \not\equiv a^2 \pmod q$ for all $a \in \mathbb{Z}$ then by def^{n} of Legendre symbol $\left(\frac{p}{q}\right) = -1$. Consider $x = p^{\frac{q-1}{2}}$ has $x^2 \equiv p^{q-1} \equiv 1 \pmod q$ by Fermat's little theorem hence only two sol^{n}'s exist; $x \equiv 1$, $x \equiv -1 \bmod q$ by Lagrange's Th^{m} on polynomial congruences.

Observe $p^{\frac{q-1}{2}} \equiv 1 \pmod q$ has at most $\frac{q-1}{2}$ sol^{n}'s.

In particular, note $p = 1^2, 2^2, \ldots, \left(\frac{q-1}{2}\right)^2$ solve $p^{\frac{q-1}{2}} \equiv 1$ and these $\frac{q-1}{2}$ sol^{n}'s are *distinct* (see next page)

Therefore, $p \not\equiv a^2 \bmod q$ cannot produce another sol^{n} of $p^{\frac{q-1}{2}} \equiv 1 \bmod q$ hence it must be $p^{\frac{q-1}{2}} \equiv -1 \bmod q$ which finishes our proof modulo the next ot ↘

It remains to show $P = 1^2, 2^2, \ldots, \left(\frac{q-1}{2}\right)^2$ are distinct modulo q (an odd prime). Suppose $x^2, y^2 \in \{1^2, 2^2, \ldots, \left(\frac{q-1}{2}\right)^2\}$ and $x^2 \equiv y^2 \bmod q$

then $x^2 \equiv y^2 \bmod q \Rightarrow x^2 - y^2 \equiv 0 \bmod q$

$\Rightarrow (x-y)(x+y) \equiv 0 \bmod q$

$\Rightarrow x - y \equiv 0$ or $x + y \equiv 0 \bmod q$

If $x - y \equiv 0$ then $x \equiv y \bmod q$, but $1 \leq x, y \leq \frac{q-1}{2}$ so we have $x = y$ as integers. On the other hand, if $x \neq y$ then $1 < x+y < q \Rightarrow x+y \not\equiv 0 \bmod q$. Hence the only case possible is $x = y$ when $x^2 \equiv y^2 \bmod q$.

Remark: the proof above does require q be prime, but P prime was not req^d. We may consider $P = -1$ and $P = 2$ as we shall shortly.

Th^m (Multiplicative property of $\left(\frac{P}{q}\right)$). For any $P_1, P_2 \not\equiv 0 \pmod q$

$$\left(\frac{P_1}{q}\right)\left(\frac{P_2}{q}\right) = \left(\frac{P_1 P_2}{q}\right)$$

Proof: by algebra of congruences and Euler's Criterion: modulo q,

$$\left(\frac{P_1}{q}\right)\left(\frac{P_2}{q}\right) \equiv P_1^{\frac{q-1}{2}} P_2^{\frac{q-1}{2}} \equiv (P_1 P_2)^{\frac{q-1}{2}} \equiv \left(\frac{P_1 P_2}{q}\right). \;//$$

Remark: this formula is weird. Why should P_1 being a square or not modulo q and the same for P_2 have anything to do with $P_1 P_2$?

Th^{m} / VALUE OF $\left(\frac{-1}{q}\right)$. For an odd prime q,

$$\left(\frac{-1}{q}\right) = \begin{cases} 1 & \text{if } q = 4n+1 \\ -1 & \text{if } q = 4n+3 \end{cases}$$

Proof: By Euler's Criterion $\left(\frac{-1}{q}\right) \equiv (-1)^{\frac{q-1}{2}} \pmod q$.

If $q = 4n+1$ then

$$\left(\frac{-1}{q}\right) \equiv (-1)^{\frac{4n+1-1}{2}} \equiv (-1)^{2n} \equiv 1 \pmod q.$$

If $q = 4n+3$ then

$$\left(\frac{-1}{q}\right) \equiv (-1)^{\frac{4n+3-1}{2}} \equiv (-1)^{2n+1} \equiv -1 \pmod q. \;//$$

§9.4: THE VALUE OF $\left(\frac{2}{q}\right)$

It turns out that $2^{\frac{q-1}{2}} = \begin{cases} (-1)^{\frac{q-1}{4}} \pmod q & \text{if } q = 4n+1 \\ (-1)^{\frac{q+1}{4}} \pmod q & \text{if } q = 4n+3 \end{cases}$

Our proof mirrors the technique we used to prove Lagrange's Lemma about m^2+1 (§6.7). This is ALL mod q,

Suppose $q = 4n+1$:

$$\begin{aligned}
1\cdot 2\cdot 3\cdots 4n &\equiv [1\cdot 3\cdot 5\cdots(4n-1)]\cdot[2\cdot 4\cdots 4n] \\
&\equiv [1\cdot 3\cdot 5\cdots(4n-1)]\cdot[1\cdot 2\cdots 2n]\,2^{2n} \\
&\equiv [1\cdot 3\cdot 5\cdots(2n-1)][(2n+1)(2n+3)\cdots(4n-1)][1\cdot 2\cdots 2n]\,2^{2n} \\
&\equiv [(-1)(-3)(-5)\cdots(1-2n)](-1)^n[(2n+1)(2n+3)\cdots(4n-1)][1\cdot 2\cdots 2n]\,2^{2n} \\
&\equiv [(4n)(4n-2)\cdots(2n+2)](-1)^n[(2n+1)(2n+3)\cdots(4n-1)][1\cdot 2\cdots 2n]\,2^{2n} \\
&\equiv [(2n+1)(2n+2)(2n+3)\cdots(4n)](-1)^n[1\cdot 2\cdots 2n]\,2^{2n} \\
&\equiv (1\cdot 2\cdots 4n)(-1)^n 2^{2n}
\end{aligned}$$

$$\therefore\ 1 \equiv (-1)^n 2^{2n} \equiv (-1)^{\frac{q-1}{4}} 2^{\frac{q-1}{2}} \Rightarrow \boxed{2^{\frac{q-1}{2}} \equiv (-1)^{\frac{q-1}{4}}}$$

($q = 4n+1$ case) (mod q of course)

§ 9.4 continued,

We proved the $q = 4n+1$ case on last page and the $q = 4n+3$ case is similar (relegated to an exercise) in total:

Proposition: $2^{\frac{q-1}{2}} \equiv \begin{cases} (-1)^{\frac{q-1}{4}} \bmod q \text{ for } q = 4n+1 \\ (-1)^{\frac{q+1}{4}} \bmod q \text{ for } q = 4n+3 \end{cases}$

We can derive an elegant summary of this.

① • If $q = 4n+1$ then $\frac{q-1}{4} = n$ thus

$$\left(\frac{2}{q}\right) \equiv (-1)^{\frac{q-1}{4}} \equiv (-1)^n = \begin{cases} 1 & \text{if } n = 2m \\ -1 & \text{if } n = 2m+1 \end{cases}$$

Hence 2 is a square mod q when $q = 4n+1 = 8m+1$ and 2 is not a square when $q = 4n+1 = 4(2m+1)+1 = 8m+5$.

② • If $q = 4n+3$ then $\frac{q+1}{4} = n+1$ thus,

$$\left(\frac{2}{q}\right) \equiv (-1)^{\frac{q+1}{4}} \equiv (-1)^{n+1} \equiv \begin{cases} 1 & \text{if } n = 2m+1 \\ -1 & \text{if } n = 2m \end{cases}$$

thus 2 is square mod q for $q = 4(2m+1)+3 = 8m+7$ and 2 is not a square mod q for $q = 4(2m)+3 = 8m+3$

Drawing together ① and ② we find,

$8(m-1)+1$

Proposition: 2 is a square mod $q \iff q = 8m \pm 1$