MATH 115, SUMMER 2012
LECTURE 16

JAMES MCIVOR

Today we mark the halfway point of the course by proving one of the most famous theorems in number theory:

Theorem 1 (Quadratic Reciprocity Law)**.** *Let p, q be distinct odd primes. Then*

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

Other ways to say it:

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

- or also:
Look at the two congruences:

$$x^2 \equiv p \mod q \quad \text{and} \quad x^2 \equiv q \mod p$$

If either or both of p and q are congruent to 1 mod 4, then either both congruences have a solution, or both don't. If $p, q \equiv 3 \mod 4$, then one has a solution and the other does not.

- loosely, if either prime is 1 mod 4, they behave the same; if both are 3 mod 4, they behave differently

1. How to use it

- tricks we've learned so far don't help us to deal with the Legendre symbol $\left(\frac{a}{p}\right)$ when p is large.
- QRL lets us "flip it".

Examples 1.1. (1)

$$\left(\frac{7}{23}\right) = (-1)^{3\cdot 11}\left(\frac{23}{7}\right) = -\left(\frac{2}{7}\right) = -1$$

(using yesterday's results at the last step)

(2)

$$\left(\frac{19}{101}\right) = (-1)^{9\cdot 50}\left(\frac{101}{19}\right) = \left(\frac{6}{19}\right) = \left(\frac{2}{19}\right)\left(\frac{3}{19}\right) = (-1)(-1)^{1\cdot 9}\left(\frac{19}{3}\right) = \left(\frac{1}{3}\right) = 1$$

(3) Determine whether the congruence $x^2 \equiv 103 \mod 257$ has a solution.
(4) $\left(\frac{54}{17}\right)$
(5) $\left(\frac{-24}{31}\right)$

2. How to prove it

We'll give a mildly geometric/combinatorial proof, using Gauss' Lemma, which differs from the proof in the textbook.

Proof. Set

$$S = \{1, 2, \dots, \frac{p-1}{2}\}, \quad T = \{1, 2, \dots, \frac{q-1}{2}\}$$

- let m = number of $s \in S$ such that $qs \notin S$.
- let n = number of $t \in T$ such that $pt \not{i}nT$.
- by Gauss' Lemma, we have

$$\left(\frac{p}{q}\right) = (-1)^n, \quad \left(\frac{q}{p}\right) = (-1)^m$$

In $\mathbb{R}^2$, look at the subset

$$S \times T = \{(s,t) \,|\, s \in S, t \in T\}$$

We call a point in $\mathbb{R}^2$ whose coordinates are both integers a **lattice point** (LP); sometimes I'll call them dots.

*** The idea of the proof is to count dots in various regions of $S \times T$. Look at the picture to follow the argument.***

- inside $S \times T$, draw the following four parallel lines:

$$pt - qs = \frac{p-1}{2} \tag{1}$$

$$pt - qs = 1 \tag{2}$$

$$pt - qs = -1 \tag{3}$$

$$pt - qs = -\frac{q-1}{2} \tag{4}$$

- let's call the region above all four lines the TOP; below all four lines the BOTTOM; between lines (1) and (2) the UPPER STRIP, and between lines (3) and (4) the LOWER STRIP
- The total number of dots in $S \times T$ is $\frac{p-1}{2}\frac{q-1}{2}$.
- Let the total number of dots in the top region be M; the number of dots in the bottom region be N
- We'll check the following things:

1. There are no dots between lines (2) and (3)
2. There are m dots in the upper strip
3. There are n dots in the lower strip
4. The number of dots in the top (M) and bottom (N) regions are the same, i.e., $M = N$.

Suppose we've proven all these. Then we're basically done:
- since no dots in the middle strip (between (2) and (3)), we have (using $M = N$ in the last equality):

$$\text{total \# of dots} = \frac{p-1}{2}\frac{q-1}{2} = m + n + M + N = m + n + 2M,$$

so

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

which is what we wanted to prove.
- now we check the facts above.
- **no dots in middle strip**: a point (s,t) is in middle strip iff

$$-1 < pt - qs < 1,$$

which means for LPs: $pt - qs = 0$, and this is impossible since p, q prime and $t < q$, $s < p$.

m **dots in the upper strip**:
- first we show that for each $s \in S$ there is at most one $t \in T$ such that $(s,t) \in$ upper strip
- suppose there were two, say t_1, t_2.
- show $|t_1 - t_2| = 0$:

$$p|t_1 - t_2| = |(pt_1 - qs) - (pt_2 - qs)| < \frac{p-1}{2} < p$$

- the inequality comes from looking at $1 \leq pt_i - qs \leq \frac{p-1}{2}$
- only way $p\cdot$(something) $< p$ in integers is if something $=0$
- so number of dots in upper strip = number of s such that there exists $t \in T$ with (s,t) in upper strip
- now we show the number of these is m.
- one direction: say for some $s \in S$, there is a $t \in T$ with (s,t) in upper strip. then $pt - qs \leq \frac{p-1}{2}$ means $pt - qs \in S$, say $pt - qs = \sigma \in S$ then

$$qs = pt - \sigma \equiv -\sigma \mod p$$

which shows $qs \notin S$.
- conclusion 1: for every dot in the strip, we get an $s \in S$ such that $qs \notin S$
- other direction: say we have an $s \in S$ such that $qs \notin S$
- then $-qs \in S \mod p$, so

$$-qs + kp = \alpha,$$

where $1 \leq \alpha \leq \frac{p-1}{2}$.
- since $\alpha > 0$ and $-qs < 0$, must have $k > 0$.

$$0 < kp = qs + \alpha \leq q\frac{p-1}{2} + \frac{p-1}{2} = (q+1)\frac{p-1}{2}$$

therefore

$$0 < k \leq \frac{(q+1)(p-1)}{2p} < \frac{q+1}{2}$$

in integers, this imples

$$1 \leq k \leq \frac{q-1}{2}$$

so $k \in T$, and we have produced a point (s,k) in the upper strip.
- conclusion 2: for every $s \in S$ such that $qs \notin S$, we get a point in the strip.
- so they're in bijection, hence m = number of dots in upper strip.

n **dots in lower strip** - this is similarr to the above argument - we skip it.

proof that $M = N$ Recall that M is the number of dots in the TOP region, N the number of dots in the BOTTOM region.

- we build a bijection between TOP and BOTTOM
- first look at this bijection from $S \times T$ to itself, call it ϕ:

$$\phi\colon (s,t) \mapsto (\frac{p+1}{2} - s, \frac{q+1}{2} - t)$$

- geometrically, ϕ sort of reflects, with a little twist as well.
- check it's a bijection, by calculating that $\phi \circ \phi$ does nothing, so ϕ is its own inverse.
- now we claim that ϕ sends points in TOP into BOTTOM: this means $N \geq M$.

- Say (s,t) is in the top region. Then ϕ sends it to $(\frac{p+1}{2} - s, \frac{q+1}{2} - t)$, and we have to check that this new point satisfies the inequalities defining the bottom region
- a point (x,y) is in the bottom region if $py - qx < -\frac{q-1}{2}$.
- check:

$$\begin{aligned} p(\frac{q+1}{2} - t) - q(\frac{p+1}{2} - s) &= \frac{p}{2} - pt - \frac{q}{2} + qs \\ &= -pt - qs) + \frac{p-1}{2} - \frac{q-1}{2} \\ &< -\frac{q-1}{2} \end{aligned}$$

- also ϕ sends points in BOTTOM into TOP: this means $M \geq N$ (similar to above, and skipped)
- since $M \leq N$ and $N \leq M$, we get $M = N$, and that finishes it!!

□