Announcements

- Course Evals: if 75% completion, then +1% in course
  Due: 6 pm on Monday, March 14

- Grading: soon
  - ↳ ask for more feedback

- Portfolio 2:
  - ↳ Due 12:15 pm on Thursday, March 17
  - ↳ textbooks and course notes only
  - ↳ no calculator: do all calculations by hand

Announcements

- Good news for next term. possible paper marker

- Next week's office hours:
  - M. 3-4 in Fenton (312 / upstairs atrium)
  - W: 11-12 on Zoom

Section 11.2 - Quadratic Reciprocity

Thm: Let p and q be distinct odd primes. Then $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$

$\left(\frac{p}{q}\right) = 1 \iff p$ is a square mod q

$\left(\frac{q}{p}\right) = 1 \iff q$ is a square mod p

Equivalently:

Thm: Suppose p is an odd prime and $a \in \mathbb{Z}$. If q is a prime with $q \equiv p \bmod 4a$, then $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$

Ex: Compute $\left(\frac{3}{101}\right)$ (3 ← a, 101 ← p)

Look at different integers $\equiv 101 \bmod 4\cdot 3$

Fact: $5 \equiv 101 \bmod 12$

By quadratic reciprocity, $\left(\frac{3}{101}\right) = \left(\frac{3}{5}\right) = -1$

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

Q: when is $\frac{p-1}{2}$ $\frac{q-1}{2}$ even? odd?

$2 \mid \frac{p-1}{2}\cdot\frac{q-1}{2}$ iff $2 \mid \frac{p-1}{2}$ or $2 \mid \frac{q-1}{2}$

(since 2 is prime)

iff $p \equiv 1 \bmod 4$ or $q \equiv 1 \bmod 4$

$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\ \frac{q-1}{2}} = -1$ iff $p \equiv q \equiv 3 \bmod 4$

$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)^2 = -\left(\frac{q}{p}\right)$ iff $p \equiv q \equiv 3 \bmod 4$

* $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ iff $p \equiv q \equiv 3 \bmod 4$

So

* $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ when $p \equiv 1 \bmod 4$ or $q \equiv 1 \bmod 4$

Ex: $\left(\frac{13}{17}\right) = \left(\frac{17}{13}\right) = \left(\frac{4}{13}\right) = 1$

Q.R $13 \equiv 1 \bmod 4$

since $17 \equiv 4 \bmod 13$

since $4 = 2^2$

Ex: $\left(\frac{7}{19}\right) = -\left(\frac{19}{7}\right) = -\left(\frac{5}{7}\right) = -\left(\frac{7}{5}\right) = -\left(\frac{2}{5}\right)$

Q.R. $7 \equiv 19 \equiv 3 \bmod 4$

QR $5 \equiv 1 \bmod 4$

$-\left(\frac{2}{5}\right) = -(-1) = 1$

$\left(\frac{2}{p}\right) = 1$ iff $p \equiv \pm 1 \bmod 8$

Ex: $\left(\frac{713}{1009}\right) = \left(\frac{23 \cdot 31}{1009}\right) = \left(\frac{23}{1009}\right)\left(\frac{31}{1009}\right)$

$713 = 23 \cdot 31$

Since $1009 \equiv 1 \bmod 4$,

$$\left(\frac{23}{1009}\right) = \left(\frac{1009}{23}\right) = \left(\frac{20}{23}\right) = \left(\frac{2^2}{23}\right)\left(\frac{5}{23}\right)$$

$$= \left(\frac{23}{5}\right) = \left(\frac{3}{5}\right) = -1$$

$$\left(\frac{31}{1009}\right) = \left(\frac{1009}{31}\right) = \left(\frac{17}{31}\right) = \left(\frac{31}{17}\right) = \left(\frac{14}{17}\right)$$

$$= \left(\frac{2}{17}\right)\left(\frac{7}{17}\right) = 1 \quad \left(\frac{17}{7}\right) = \left(\frac{3}{7}\right)$$

$$= -\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1$$

$$\left(\frac{713}{1009}\right) = \left(\frac{23}{1009}\right)\left(\frac{31}{1009}\right) = (-1)(-1) = 1$$