

# SETS:

- Will be closed on *Sunday (Dec. 4)*
- You can access this survey through the direct link in the email OR through Canvas

• Your feedback is very important to us!

• Detailed comments  
    → very helpful

MATH-110-01 > Syllabus

Recent Announcements

- Wednesday Lecture + The Student Experience of Teaching Surveys + HWs  
Hi everyone! On Lectures: We will use the zoom link bel...  
Posted on: Nov 22, 2022, 10:35 PM
- Today's lecture note, assignments, and next Lecture.  
Hi everyone! On Lectures: Today's lecture notes can be f...  
Posted on: Nov 21, 2022, 9:35 PM
- Reminder on next meeting and the HW 7  
Hi everyone! Next lecture: Next time, we will discuss per...  
Posted on: Nov 20, 2022, 5:45 PM

Introduction to Number Theory

Fall 2022 • MWF 2:40 PM - 3:45 PM at Soc Sci 2071 (in-person)  
Instructor: Xu Gao ([xgao26@ucsc.edu](mailto:xgao26@ucsc.edu)), McHenry Library 1292  
Office Hours: MW 4:30 - 5:30 PM, or by appointment.  
You can find Lecture Notes [here](#).  
TA: Yuk Shing Lam ([ylam14@ucsc.edu](mailto:ylam14@ucsc.edu)), McHenry 1261.  
TA's Office Hours: Tuesday and Friday 11:00 AM - 12:00 PM  
Discussion Sections.

6d You are currently logged into Student View

Reset Student Leave Student View

Back to Quadratic Reciprocity law:

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right) \text{ where } p^* := (-1)^{\frac{p-1}{2}} \cdot p$$
$$= (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \left(\frac{p}{q}\right)$$

Plan: Find permutations  $\alpha, \beta, \gamma$  s.t.

$$\text{Sign}(\alpha) = \left(\frac{q}{p}\right)$$

$$\text{Sign}(\beta) = \left(\frac{p}{q}\right)$$

$$\text{and } \alpha = \gamma \circ \beta$$

$$\text{Sign}(\alpha) = \text{Sign}(\gamma) \cdot \text{Sign}(\beta)$$

$$\text{Sign}(\gamma) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}$$

Let  $S = \{0, 1, \dots, pq-1\}$  the nat. repns of  $\mathbb{Z}_{pq}$

$[a,b] :=$  the unique inter in  $S$  congruent to  $a \pmod p$  and  $b \pmod q$ .

$$\langle a, b \rangle := aq + b, \quad [a, b] \equiv [a, b] \pmod q$$

$$[a, b\rangle := a + bp, \quad [a, b\rangle \equiv [a, b] \pmod p$$

Every element in  $S$  can be uniquely expressed in each notation. (why?)

$\alpha$ : send each  $[a, b]$  to  $\langle a, b \rangle$

$\beta$ : send each  $[a, b]$  to  $[a, b\rangle$

$\gamma$ : send each  $[a, b\rangle$  to  $\langle a, b \rangle$

Permutations of  $S$  satisfying  $\alpha = \gamma \circ \beta$

E.g.  $p=5$ ,  $q=3$

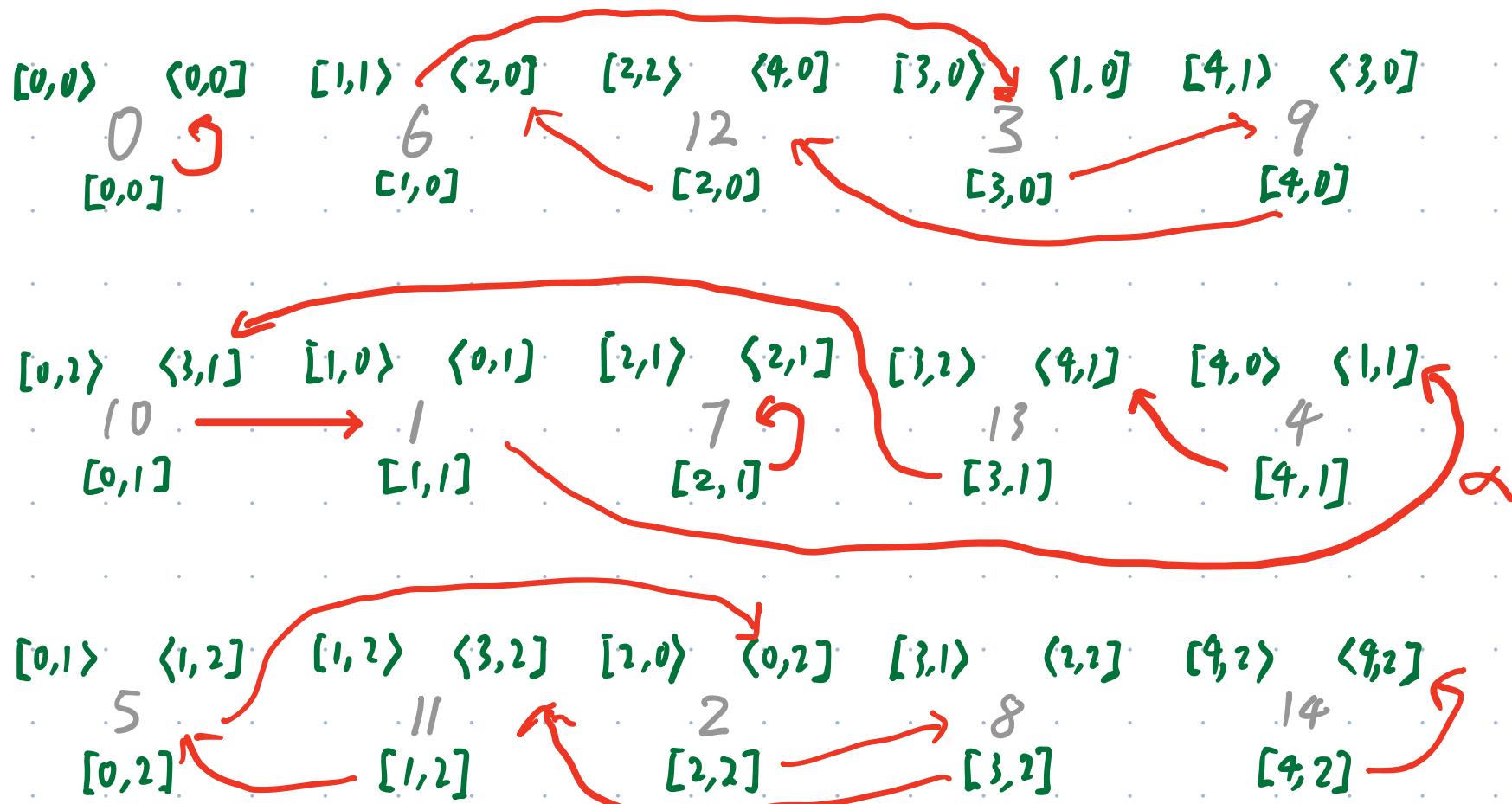
|                          |                          |                          |                         |                          |                                |                          |
|--------------------------|--------------------------|--------------------------|-------------------------|--------------------------|--------------------------------|--------------------------|
| $[0,0]$<br>0<br>$[0,0]$  | $[0,0]$<br>6<br>$[1,0]$  | $[1,1]$<br>12<br>$[2,0]$ | $[2,2]$<br>3<br>$[3,0]$ | $[3,0]$<br>9<br>$[4,0]$  | $[4,1]$<br>$\gamma$<br>$[4,0]$ | $[3,0]$<br>$\beta$       |
| $[0,2]$<br>10<br>$[0,1]$ | $[3,1]$<br>1<br>$[1,1]$  | $[1,0]$<br>0<br>$[0,1]$  | $[0,1]$<br>7<br>$[2,1]$ | $[2,1]$<br>13<br>$[3,1]$ | $[2,1]$<br>$\alpha$<br>$[4,1]$ | $[4,0]$<br>4<br>$[1,1]$  |
| $[0,1]$<br>5<br>$[0,2]$  | $[1,2]$<br>11<br>$[1,2]$ | $[1,2]$<br>2<br>$[2,2]$  | $[2,0]$<br>8<br>$[3,2]$ | $[0,2]$<br>14<br>$[4,2]$ | $[3,1]$<br>9<br>$[2,2]$        | $[2,2]$<br>14<br>$[4,2]$ |

arranged into  $p$  columns and  $q$  rows, as determined by CRT.

Lemma.  $\text{sign}(\alpha) = \left( \frac{q}{p} \right)$      $\text{sign}(\beta) = \left( \frac{p}{q} \right)$

Proof: We will prove the first, the second follows in similar argument.

Rearrange elements of  $S$  into  $p$  columns and  $q$  rows according to  $[r, t]$ .



More precisely, an element  $n \in S$  is

- in the column  $[a, -]$  iff  $n \equiv a \pmod{p}$
- in the row  $[-, b]$  iff  $n \equiv b \pmod{q}$

Note that:  $\langle a, b \rangle \equiv [a, b] \pmod{q}$

Hence,  $\alpha$ , which maps each  $[a, b]$  to  $\langle a, b \rangle$ , maps each element to one in the **SAME** row.

Namely, if we restrict  $\alpha$  to the row  $[-, b]$ , then it is also a permutation of that row. We can identify row  $b$  with  $\mathbb{Z}_p$  by  $[a, b] \mapsto \bar{a}$ .

In the row  $b$ , each column  $a$  is mapped to the column  $aq + b \pmod{p}$ .

Using words from  $\mathbb{Z}_p$ ,  $\alpha$  acts as  $\bar{a} \mapsto \bar{aq} + \bar{b}$ , which can be viewed as the composition of " $\bar{X}^q$ " and " $+\bar{b}$ ".

We have  $\alpha|_{\text{row } b} = "+b \bmod p" \circ "x \not\equiv 1 \bmod p"$

Then  $\text{Sign}(\alpha|_{\text{row } b}) = \text{Sign}(" + b \bmod p") \text{Sign}(" x \not\equiv 1 \bmod p")$

$$\begin{aligned} &= 1 \cdot \left( \frac{q}{p} \right) \text{ by Zolotarev's lemma} \\ &= \left( \frac{q}{p} \right). \end{aligned}$$

Since we have  $q$  rows,

$$\begin{aligned} \text{Sign}(\alpha) &= \text{Sign}(\alpha|_{\text{row } 0}) \cdots \text{Sign}(\alpha|_{\text{row } q-1}) \\ &= \left( \frac{q}{p} \right)^q \\ &= \left( \frac{q}{p} \right). \end{aligned}$$

$\downarrow q$  is odd and  $\left( \frac{q}{p} \right) = \pm 1$



$$\text{Lemma: } \text{Sign}(\gamma) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \quad x < x' \& \gamma(x) > \gamma(x')$$

Proof. We'll use the 3rd characterization of sign.

First, for any  $x, x' \in S$ , write  $x = aq + b$  &  $x' = a'q + b'$ .

Then  $x < x' \iff$  either  $a < a'$   
 or  $a = a'$  but  $b < b'$

Now, we want to compare  $\gamma(x)$  &  $\gamma(x')$ :

$$\gamma(x) = a + bP \quad \text{v.s.} \quad \gamma(x') = a' + b'P$$

Then  $\gamma(x) > \gamma(x') \iff$  either  $b > b'$   
 or  $b = b'$  but  $a > a'$

Combine (\*) & (\*'),  $(x, x')$  is an inversion of  $\gamma \iff a < a' \& b > b'$   
 $x < x' \& \gamma(x) > \gamma(x')$

The # of  $(a, a', b, b')$  s.t.  $0 \leq a < a' \leq p-1$   
and  $0 \leq b' < b \leq q-1$

$$\text{is } \frac{p-1}{2} \cdot \frac{q-1}{2}$$

Hence,  $\text{inv}(\gamma) = \frac{p-1}{2} \cdot \frac{q-1}{2}$ . Then

$$\text{Sign}(\gamma) = (-1)^{\text{inv}(\gamma)} = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}$$

□

### Proof of Quadratic Reciprocity Law:

$$\alpha = \gamma \circ \beta \Rightarrow \text{Sign}(\alpha) = \text{Sign}(\gamma) \text{Sign}(\beta)$$

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

□

# Applications of Quadratic Reciprocity Laws

- Infinitude of primes in arithmetic progressions

General State: Fix  $m$  and  $a \in \mathbb{Z}(m)$ ,

There are infinitely many prime numbers  $P$  s.t.

$$P \equiv a \pmod{m}$$

## Special cases (examples)

- There are infinitely many prime numbers congruent to  $1 \pmod{4}$
- There are infinitely many prime numbers congruent to  $1 \pmod{3}$

How to approach?

Note that : by QRRL,

$$p \equiv 1 \pmod{4} \Leftrightarrow \left(\frac{-1}{p}\right) = 1$$

$$p \equiv 1 \pmod{3} \Leftrightarrow \left(\frac{-1}{p}\right) = 1$$

We want to show:

There are infinitely many prime numbers  $p$  s.t.  $\left(\frac{a}{p}\right) = 1$

Note that :

$$\left(\frac{a}{p}\right) = 1 \Leftrightarrow p \mid n^2 - a \text{ from some } n \\ \text{ & } p \nmid a$$

Lem. Let  $f(T)$  be a nonzero integer polynomial.

Then there are infinitely many prime numbers  $p$  s.t.

$$(*) \quad p \mid f(n) \text{ for some } n.$$

Proof. (prove by contradiction)  $f(T) = a_d T^d + \dots + a_1 T + a_0$

Suppose  $P_1, P_2, \dots, P_N$  are all the prime numbers s.t.  $(*)$

More precisely,  $P_i \mid f(n_i)$ . Then consider

$$P := P_1 P_2 \cdots P_N$$

Let's look at

$$\frac{1}{a_0} f(k a_0 P)$$

$$\begin{aligned}\frac{1}{a_0} f(k a_0 P) &= \frac{1}{a_0} (a_0 + a_1 (k a_0 P) + \cdots + a_d (k a_0 P)^d) \\ &= 1 + \underbrace{a_1 k P + a_2 k^2 a_0 P^2 + \cdots + a_d k^d a_0^{d-1} P^d}_{\text{divided by } P}\end{aligned}$$

Hence, the right hand side is coprime to  $P_1, P_2, \dots, P_N$ .

Also, so  $f$  is a nonconstant polynomial, the right hand side CANNOT be always  $\pm 1$  when you take different  $k$

$\Rightarrow$  at least for some  $k$ , the right hand side is

an integer  $> 1$  and coprime to  $P_1, P_2, \dots, P_N$ .

$\Rightarrow \exists$  prime  $P' \notin \{P_1, P_2, \dots, P_N\}$  s.t.  $P' \mid f(k a_0 P)$

$\Rightarrow \Leftarrow !$

(§)

Apply the lemma to  $T^2 - a$ . We have

There are infinitely many prime numbers  $p$  s.t.  $\left(\frac{a}{p}\right) = 1$

proof:

$$\left(\frac{a}{p}\right) = 1 \iff p \mid n^2 - a \text{ from some } n \\ \text{ & } p \nmid a$$

By the lemma, there are infinitely many prime numbers  $p$  s.t.

$$p \mid n^2 - a \text{ from some } n$$

Among them, there are only finitely many divide  $a$ .

Hence, there are infinitely many prime numbers  $p$  s.t.  $\left(\frac{a}{p}\right) = 1$



Apply Quadratic Reciprocity Laws to previous results, we have:

- There are infinitely many prime numbers congruent to 1 mod 4

$$p \equiv 1 \pmod{4} \Leftrightarrow \left(\frac{-1}{p}\right) = 1$$

- There are infinitely many prime numbers congruent to 1 mod 3

$$p \equiv 1 \pmod{3} \Leftrightarrow \left(\frac{-3}{p}\right) = 1$$

- There are infinitely many prime numbers congruent to  $\pm 1$  mod 8

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