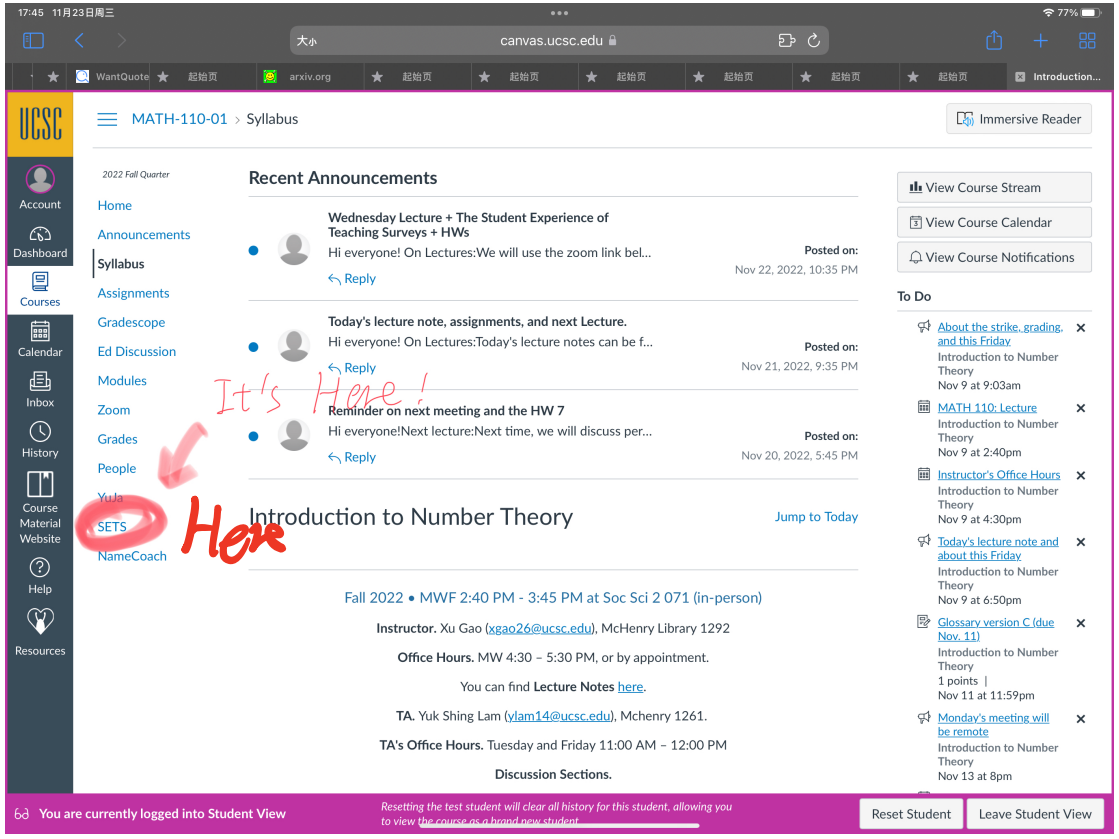
SETS:

- 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



Back to Quadratic Reciprocity law:

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

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

Plan: Find permutations α, β, γ s.t.

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

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

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

and $\alpha = \gamma \circ \beta$

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

Let $S = \{0, 1, \cdots pq-1\}$ the nat. reprs of $\mathbb{Z}/_{pq}$

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

$\langle a,b] := aq + b$. $\quad \langle a,b] \equiv [a,b]$ mod q

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

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

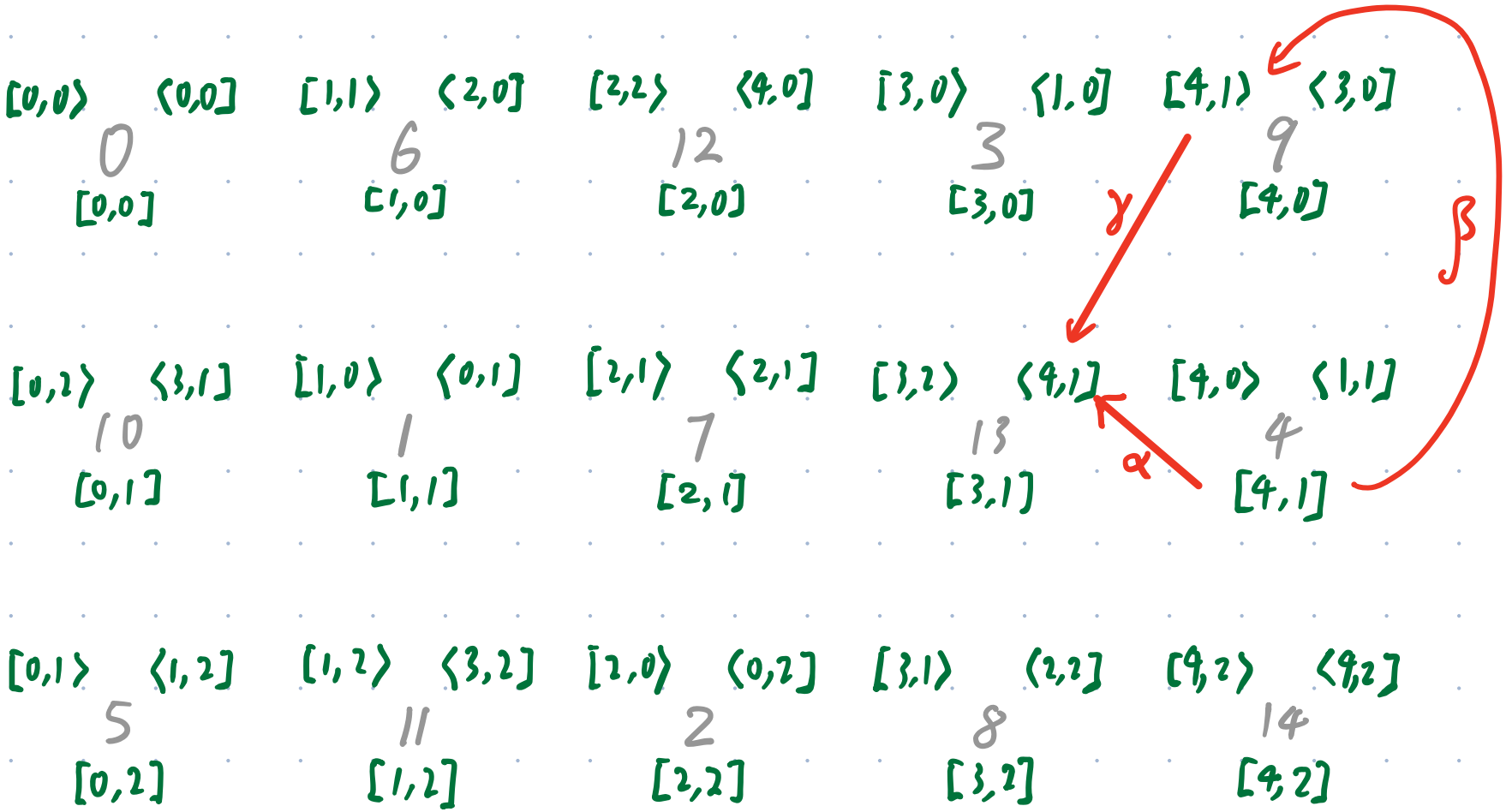
α: send each $[a,b]$ to $\langle a,b]$

β: send each $[a,b]$ to $[a,b\rangle$

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

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

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

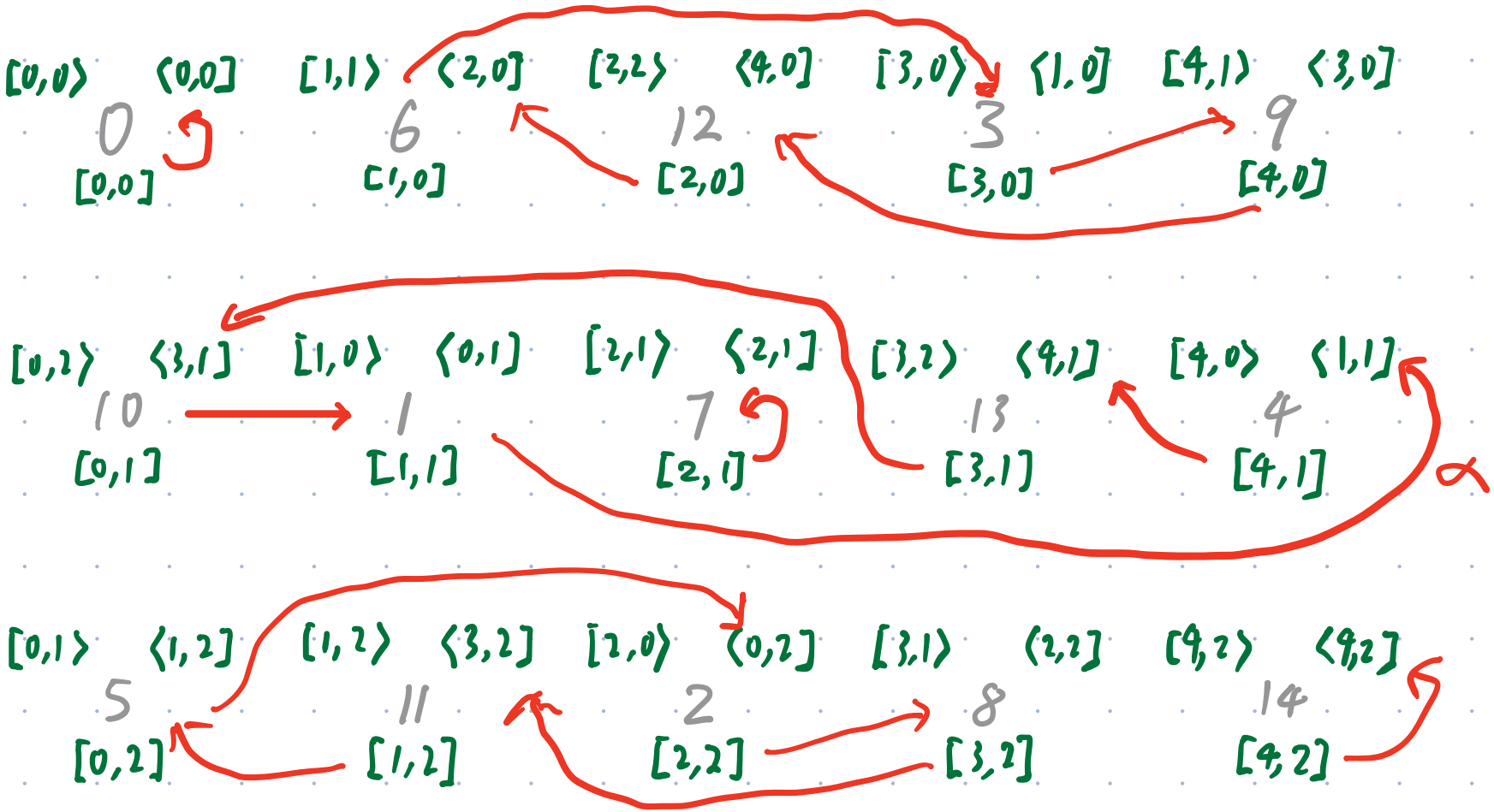


arranged into p columns and q rows, as determined by CRT.

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

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

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



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

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

Note that: $\langle a,b] \equiv [a,b] \bmod q$

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

Namely, if we restrict α 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 maped to the column $aq + b \bmod p$.

Using words from $\mathbb{Z}/p$, α acts as $\bar{a} \longmapsto \overline{aq+b}$, which can be viewed as the composition of "$\overline{\times q}$" and "$\overline{+b}$".

We have $\alpha|_{\text{row } b} = \text{"} + b \bmod p \text{"} \circ \text{"} \times q \bmod p \text{"}$

Then $\operatorname{Sign}(\alpha|_{\text{row } b}) = \operatorname{Sign}(\text{"} + b \bmod p \text{"}) \operatorname{Sign}(\text{"} \times q \bmod p \text{"})$

$= 1 \cdot \left(\frac{q}{p}\right)$ by Zolotarev's lemma

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

Since we have q rows,

$\operatorname{Sign}(\alpha) = \operatorname{Sign}(\alpha|_{\text{row } 0}) \cdots\cdots \operatorname{Sign}(\alpha|_{\text{row } q-1})$

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

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

□

Lemma. $\mathrm{Sign}(\gamma) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ $\qquad x < x'$ & $\gamma(x) > \gamma(x')$

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

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

Then $x < x' \iff$ either $a < a'$

or $a = a'$ but $b < b'$ $\qquad (*)$

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

$\gamma(x) = a + bp$ $\quad <a,b]$ $\qquad$ v.s. $\qquad \gamma(x') = a' + b'p$ $\quad <a',b']$

Then $\gamma(x) > \gamma(x') \iff$ either $b > b'$ $\qquad (*')$

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. $0 \le a < a' \le p-1$

and $0 \le b' < b \le q-1$

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

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

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

□

Proof of Quadratic Reciprocity Law:

$$\alpha = \gamma \circ \beta \Rightarrow Sign(\alpha) = Sign(\gamma)\, Sign(\beta)$$

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

□

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.

$$p \equiv a \mod m$$

Special cases (examples)

- There are infinitely many prime numbers congruent to $1 \mod 4$
- There are infinitely many prime numbers congruent to $1 \mod 3$

How to approach ?

Note that : by QRL,

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

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

We want to show:

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

Note that:

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

$$\& \; p \nmid a$$

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

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

(*) $p \mid f(n)$ for some n.

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

Suppose $p_1, p_2, \cdots, p_N$ 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

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

$$\frac{1}{a_0} f(k a_0 P) = \frac{1}{a_0}\left(a_0 + a_1(k a_0 P) + \cdots + a_d (k a_0 P)^d\right)$$

$$= 1 + \underbrace{a_1 k P + a_2 k^2 a_0 P^2 + \cdots + a_d k^d a_0^{d-1} P^d}_{\text{divided by } P}$$

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

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

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

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

$\Rightarrow \exists$ prime $P' \notin \{P_1, P_2, \cdots, P_N\}$ 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: $\left(\frac{a}{p}\right) = 1 \iff p \mid n^2 - a$ from some n

& $p \nmid a$

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

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

Among them, there are only finitely many divide a.

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

囧

Apply Quadratic Reciprocity Laws to previous results, we have:

- There are infinitely many prime numbers congruent to $1 \bmod 4$

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

- There are infinitely many prime numbers congruent to $1 \bmod 3$

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

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

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

. . . . . .