Welcome to Math 128A

- Use a laptop or desktop with a large screen so you can read these words clearly.
- In general, please turn off your camera and mute yourself.
- Exception: When we do groupwork, please turn both your camera and mic on. (Groupwork will not be recorded.)
- Please always have the chat window open to ask questions.
- Reading for today: Ch. 0. Reading for Mon: Ch. 1.
- PS00 due Mon Aug 24; PS01 outline due Mon Aug 24; PS01 due Wed Aug 26. Part of PS00: Come to my office hours for 5 min
- Also: Print and cut out (or imitate) D_4, D_5, D_6
- Problem session Fri Aug 21, 10:00–noon on Zoom.

Tour of the course website

The course website is:

`http://www.timhsu.net/courses/128a/`

Working in groups

In a minute, I'll send everyone into breakout rooms in groups of 3–4 to answer the following question:

What is one important event in your mathematical life?

In each breakout room:

- Learn **someone else's** name and important event. (I'll visit each room to help you organize cyclically.)
- Be ready to share that person's important event when we get back to the main room. (Take notes!)

Get ready to turn on your cameras and mics. (I'll pause the recording.)

Review: Division algorithm

Theorem

a, d integers, $d > 0$. There exist unique integers q, r such that

$$a = dq + r \qquad \text{with } 0 \leq r < d.$$

I.e., quotient and remainder work just like they did in grade school.

Divisors and GCD

$a, b, d, n \in \mathbf{Z}$.

Definition

To say that d **divides** a means that $a = dq$ for some $q \in \mathbf{Z}$.

Definition

To say that d is a **common divisor** of a and b means that d divides a and d divides b.

Definition

The **greatest common divisor** of $a, b \in \mathbf{Z}$, $a, b \neq 0$, is just what it sounds like. If $\gcd(a, b) = 1$, we say that a and b are **relatively prime**.

GCD is a linear combination

Fact (you don't need to prove this, nor will I):

Theorem
For $a, b \in \mathbf{Z}$, $a, b \neq 0$, there exist $x, y \in \mathbf{Z}$ such that

$$ax + by = \gcd(a, b).$$

This fact will come in handy later!

See also: Die Hard 3, the two bottles/pails puzzle

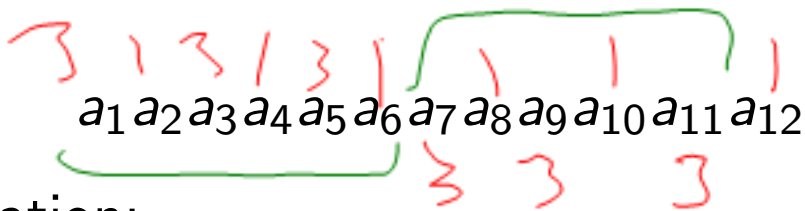
Modular arithmetic

($n > 0$)
When $a = nq + r$, $0 \leq r < n$, we say that r is equal to a reduced "mod n."

By doing ordinary arithmetic and then reducing mod n, we get **arithmetic mod** n, which turns out to have many properties of ordinary arithmetic. (This is best justified in Ch. 14 (!), but we'll go ahead and use it now, because otherwise there will be no examples in the class.)

UPC codes

A **Universal Product Code** has 12 digits that identify the manufacturer and product. A UPC code



satisfies the equation:

$$3a_1 + 1a_2 + 3a_3 + 1a_4 + 3a_5 + 1a_6 + 3a_7 + 1a_8 + 3a_9 + 1a_{10} + 3a_{11} + 1a_{12} = 0 \pmod{10}$$

Groupwork: UPC codes

A pack of organic spaghetti has the UPC code:

0 - 2 1 5 1 1 - 1 3 7 1 5 - ?

What is the last (check) digit of that UPC code?

Equivalence relations

X a set.

Definition

An **equivalence relation on** X is a relation $\sim$ on X that satisfies:

1. (Reflexive) $\forall x \in X,\ x \sim x$
2. (Symmetric) $\forall x, y \in X,\ \text{If } x \sim y \Rightarrow y \sim x$
3. (Transitive) $\forall x, y, z \in X,\ x \sim y,\ y \sim z \Rightarrow x \sim z.$

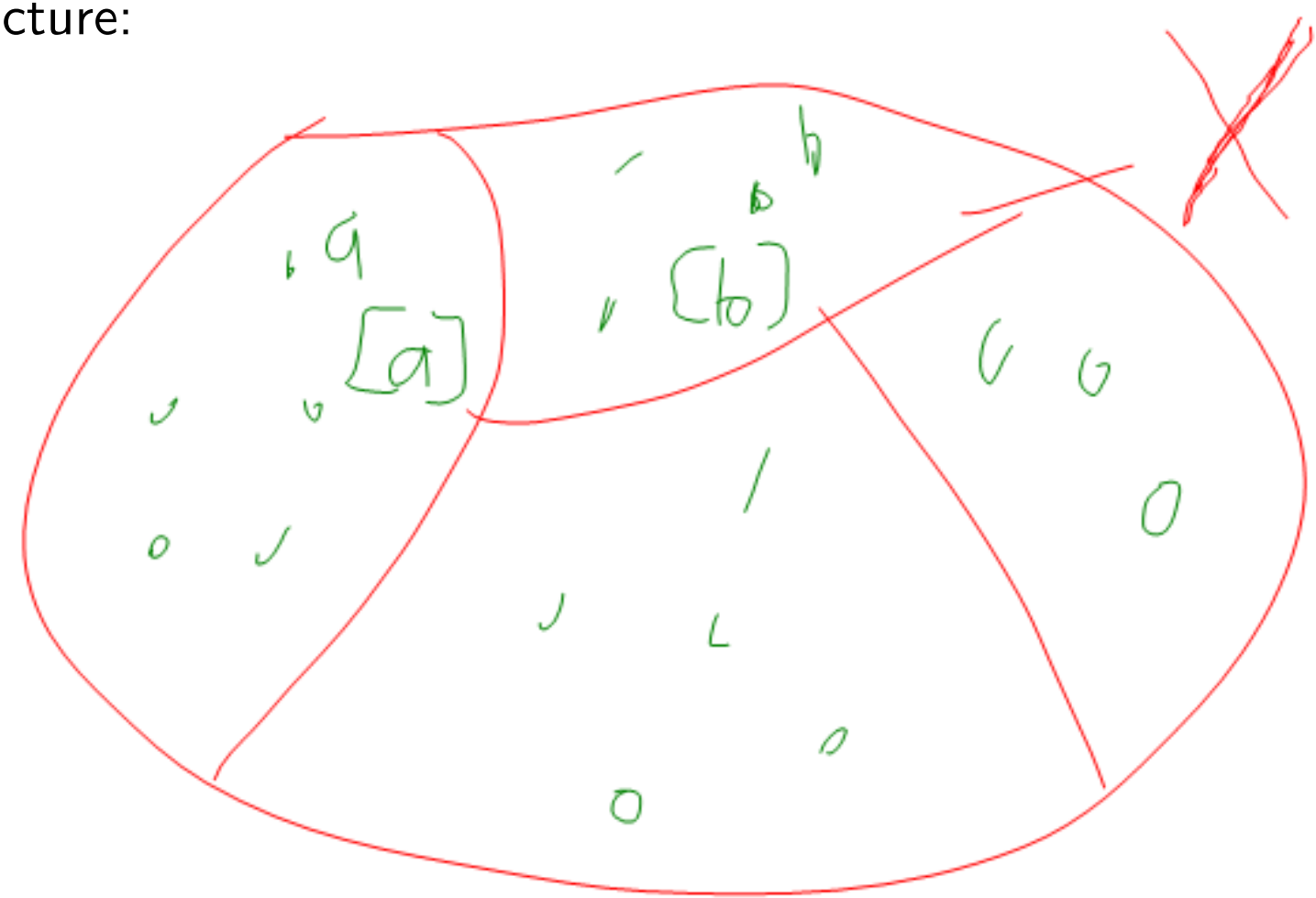
Definition

For $a \in X$, **equivalence class of** a is

$$[a] = \{x \in X \mid a \sim x\}.$$

Equivalence classes partition X

Picture:



I.e., X is equal to the disjoint union of equivalence class.