Welcome to Math 127

- Use a laptop or desktop with a large screen so you can read these words clearly.
- In general, you may 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: 1.1–1.2, 1.3.1–1.3.4, 2.1–2.2.
- Reading for Mon Jan 31: 2.3–2.4.
- COVID Safety HW and PS00 due Mon Jan 31.
- PS01 outline due Wed Feb 02, full version due Mon Feb 07.
- First problem session Fri Feb 04, 10:00–noon on Zoom.

Tour of the course website

The course website is:

`http://www.timhsu.net/courses/127/`

Important: WE ARE COMING BACK

(see today's COVID stats for the Bay Area)

So the important thing to know is:

WE WILL BE BACK HOLDING CLASS IN PERSON ON MON FEB 14

I would bet $50 on it!

Breakout room activity

In breakout rooms, each of you 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.

Why is this course different from other courses?

- The goal of this course is to train you to use algebra to **make money**.
- **Theory** (or rather, understanding theory) is what makes money.
- So much more than before, you need to focus on **language** and **definitions**.
- For a good understanding of algebra, knowing certain **examples** like the back of your hand becomes very important. (In this class: The integers mod m.)
- So you'll need to read the text differently than you've read other texts. Read it like a story that you want to understand and take to heart.
- And when you do problems, instead of just looking for procedures to follow or imitate, you'll often need to understand the **big idea** of a particular topic and apply it.

What are the divisors of 12?

defn?

Let's list them:

$\mathbb{Z}$: $1, 2, 3, 4, 6, 12$ ($\mathbb{Z}, > 0$)

$-1, -2, -3, -4, -6, -12$

$12 = \pi\left(\frac{12}{\pi}\right)$

So π divides?

all $\mathbb{R}$

All nonzero reals

So that was actually a trick question

The meaning of **divisor** depends on the numbers we're allowed to use:

> **Not quite a defn:** *Suppose R is some system of numbers like* $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, *or* $\mathbf{C}$*. To say that we are working in the* **ring** *R means that we are allowed to use numbers in R, and only numbers in R, in our computations, explanations, and so on.*

So now:

working in the ring of integers

Definition

To say that an integer d **divides** an integer n in $\mathbf{Z}$, or alternately, that d is a **divisor** of n, means that $n = qd$ for some $q \in \mathbf{Z}$ (i.e., for some integer q).

So what are the divisors of 12, really?

They are:

$\pm 1, \pm 2, \pm 3, \pm 4,$

$\pm 6, \pm 12$

Definition

To say that integers a and b are **associates** means that $a = \pm b$; equivalently, we say that a and b are the same **up to associates**.

So the divisors of 12 are, up to associates:

$1, 2, 3, 4, 6, 12.$

Another reason definitions are important

Precise definitions make it possible to prove theorems. (See 1.3.1–1.3.4.)

Theorem

Let n be an integer. If 15 divides n, then 5 divides n.

Proof:

Common divisors and greatest common divisor

Definition

For integers d, a, and b, to say that d is a **common divisor** of a and b means that d divides a and d divides b.

Definition

For integers a and b, at least one of which is not 0, the **greatest common divisor**, or **GCD**, of a and b is exactly what it sounds like: the greatest integer d that is a common divisor of a and b. We denote the greatest common divisor of a and b by the symbol $\gcd(a, b)$.

An example

Example: What is $\gcd(8, 12)$? How do you know?

Well, actually: If we use "greatest" to mean biggest in terms of absolute value, then gcd is determined exactly up to associates. So we can say:

Motivating problem for Ch. 2

Motivating Problem

Given nonzero integers a and b, how can we efficiently compute $\gcd(a, b)$?

Here's a **naive** algorithm for finding $\gcd(a, b)$. (Naive doesn't necessarily mean bad!)
Let a and b be positive integers.

1. Make an ordered list of positive divisors of a.
2. Check which of those divisors of a also divides b, starting from the largest divisor and going downwards.

The first common divisor found in step 2 will be $\gcd(a, b)$.

How fast or slow is the naive algorithm?

Suppose $a, b \leq n$. (I.e., we fix a maximum size n of integers that we'll consider.)

1. One way to find all positive divisors of a is to consider all d from 1 to a and divide a by d with remainder. This could take up to n divisions.
2. Then for each d in the list of divisors of a, we divide b by d and see if there's a remainder. There are no more than n divisors of a, so again we have no more than n divisions.

So worst-case scenario is $2n$ steps, where each step is a division with remainder.

Can we beat that speed by an exponential factor?

Motivating Problem

Suppose a, b are positive integers $\leq n$. Can we find an algorithm for computing $\gcd(a, b)$ that is guaranteed to take fewer than $C \log n$ steps, for some constant C?