Math 127, Mon Feb 07

- 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.
- **IN-PERSON CLASSES START MON FEB 14!!!!**
- Reading for today: 3.1.
- Reading for Wed: 3.2–3.3.
- PS01 due today; PS02 outline due Wed, full version due Mon Feb 14.
- Next problem session Fri Feb 11, 10:00–noon on Zoom.
- **Exam 1** in 2 weeks from today.
- Potential new asst prof interviewing today! Algebra talk 3pm today — see email for link.

2.2.2 (c) Naive alg. # divs $\leq 2n$

Want # divs $\leq C\sqrt{n}$ $n = \max$ sized a, b

$= C\sqrt{a} \leq$

↑ in d of a

2.1.1 (a)

Let $k = \cdots$

:

(C) $n = k(b-a)$ for some k

Recap of complexity

The **complexity** of an algorithm is the (estimated) time or space that an algorithm needs to finish, given an input of size n.

This is often expressed in **big O notation**. That is, we say that a given algorithm finishes in $O(f(n))$ time, meaning that there exists some constant C such that the number of steps the algorithm takes is $\leq Cf(n)$ for all $n \in \mathbf{N}$.

The Euclidean Algorithm is exponentially faster

oth rem

Theorem

Let a, b, and n be nonzero integers with $|a| \geq |b|$ and $|b| \leq n$. Using the Signed Euclidean Algorithm to compute $\gcd(a, b)$ finishes in $O(\log n)$ time, or more precisely, requires $O(\log n)$ division-with-remainder steps to finish.

Idea of proof: Look back at the Signed Euclidean Algorithm.

In each step, we have $|r_i| \leq \frac{|r_{i-1}|}{2}$

So, with each step, the size of the remainder reduces by half. 2^k

So k steps allows you to reduce an initial remainder of size <= 2^k to 1.

So # of steps required to finish is k

(starting with remainder of size n) is log_2 (n) = O(log n).

Then: Regular EA takes at most 2 x as many steps as Signed EA, so still O(log n).

gcd(21, 13)

$21 = 1(13) + 8$

$13 = 1(8) + 5$

$8 = 1(5) + 3$

$5 = 1(3) + 2$

$3 = 1(2) + 1$

Take quotients, round DOWN.

Take quotients, round OFF.

$21 = 2(13) - 5$

$13 = 3(5) - 2$

$5 = 2(2) + 1$

$= 3(2) - 1$

need $r \leq \frac{3}{2} = 1$

Another example of a complexity estimate

The traditional Christmas carol "The 12 Days of Christmas" has the following structure: On day 1, the singer gets one gift of type 1 (a partridge in a pear tree) from their true love; on day 2, the singer gets two gifts of type 2 and one gift of type 1 (two turtledoves and a partridge in a pear tree); and so on.
Suppose this song can be extended to any arbitrary number of days. Give a big-O estimate of the *number* of gifts the singer receives on day n.

day 1 : 1
day 2 : 1+2
day 3 : 1+2+3

day n :
$1+2+\cdots+n$
$= \frac{n(n+1)}{2}$
$= \frac{1}{2}n^2 + \cdots$

So # gifts rec'd dayn is $O(n^2)$.

HW: Similar estimates for matrix multiplication and polynomial multiplication.

How do you solve algebraic problems?

Start: Look at small examples, then bigger examples
Find a pattern.

And now for something completely different

Recall that the **ring** in which we work is the set of "numbers" we're allowed to use in computations, proofs, etc.
How do we change the ring we work in? I.e., how do we define a **new** ring? To define a ring R:

- *Choose a set:* First, choose a set R of objects that will be the "numbers" of your ring.
- *Define addition:* Next, define how to add two elements of R.
- *Define multiplication:* Finally, define how to multiply two elements of R.

Reduction mod m

"Z mod m"

We'll be defining a new ring $\mathbf{Z}/(m)$, but first, a pre-definition:

Definition

Let m be a positive integer. For any integer k, k **reduced (mod m)** is the remainder you get when you divide k by m. I.e., if

$$k = qm + r \qquad \text{with } 0 \leq r < m,$$

then k reduced (mod m) is r.

Example: $m = 11$

$21 \pmod{11} = 10$

$73 \pmod{11} = 7$ $\quad (73 = 6(11) + 7)$

$\mathbf{Z}/(m)$, the integers mod m

Let m be a positive integer. We define the ring $\mathbf{Z}/(m)$, or the **integers (mod m)**, as follows.

- The underlying set of $\mathbf{Z}/(m)$ is $\{0, \ldots, m-1\}$.
- For $a, b \in \mathbf{Z}/(m)$, we define $a + b$ to be the ordinary integer sum of a and b, reduced mod m.
- Similarly, for $a, b \in \mathbf{Z}/(m)$, we define the product ab to be the ordinary integer product of a and b, reduced mod m.

When we work in $\mathbf{Z}/(m)$, we refer to m as the **modulus** of our ring.

Example: Addition and multiplication tables in $\mathbf{Z}/(5)$

(Try this in pairs/threes)

$+$	0	1	2	3	4
0					
1					
2					
3					
4					

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

How to be more flexible

For $m = 3$ (as an example), since $-1 = 2 \pmod 3$, it sometimes helps to write the elements of $\mathbf{Z}/(3)$ as $\{-1, 0, 1\}$ instead of $\{0, 1, 2\}$.

More generally:

> **Congruent Substitution Principle:** *If we are working in the ring $\mathbf{Z}/(m)$, we can always replace any integer a with any integer b congruent to $a \pmod m$.*

Even more generally:

> **The $m = 0$ Principle:** *Arithmetic in $\mathbf{Z}/(m)$ is like regular arithmetic, except that we declare that $m = 0$, and accept all of the relations that follow as a consequence (such as the Congruent Substitution Principle).*

Example: Fractions in $\mathbf{Z}/(7)$

In $\mathbf{Z}/(7) = \{0, 1, 2, 3, 4, 5, 6\}$, what is the reciprocal of each element?

Next: We will invert 1,2,3,4,5,6 (mod 7).

Experiment 1: Primitive elements

Defn: To say that $a \in \mathbf{Z}/(m)$ is **primitive** means that every nonzero element of $\mathbf{Z}/(m)$ is a power of 2.

- Is 2 primitive in $\mathbf{Z}/(5)$?
- Is 2 primitive in $\mathbf{Z}/(7)$?
- Is 2 primitive in $\mathbf{Z}/(11)$?

Experiment 2: Quadratic residues

Defn: To say that $a \in \mathbf{Z}/(m)$ is a **quadratic residue** means that $a \neq 0$ and a is a square in $\mathbf{Z}/(m)$, i.e., $x^2 = a$ has a solution in $\mathbf{Z}/(m)$.
Here we use a weird method for solving $x^2 = a$: Because there are only finitely many values of $x \in \mathbf{Z}/(m)$, we can just try all possible x.

- Quadratic residues in $\mathbf{Z}/(5)$:

- Quadratic residues in $\mathbf{Z}/(7)$:

The point of the last few problems in PS02: Experiment!

Try a bunch of examples and see if you find any patterns!

(And yes, the other point is for you to get better at computation in $\mathbf{Z}/(m)$ through practice — but you might as well do something interesting in the process.)