Friday,
April 19

Math is hard. (If it weren't, there would be nothing for Professor Goldmakher to do.) The goal of this class is to make us think like mathematicians.

...however, some of the experiments Professor Goldmakher has tried haven't worked. One is the quizzes. The issue is the problem from the problem sets. People who already get that problem do well, while people who don't don't, effectively hurting the latter group twice.

Solution: From here on out, the only question on the quizzes will be a theorem from class.

The best indicator of grades we have right now is the midterm grade plus 25. A 70-80 is a B. An 80+ is an A.

We don't want to get demoralized regarding grades. As such, Professor Goldmakher will drop the two lowest quiz grades and the two lowest problem set grades (instead of the one lowest for each).

Let's talk about question 2 from quiz 5 for a moment. A lot of answers said that since the power set of S includes the empty set, it includes one more element than S, so it must be larger. This argument works when S is finite. If $S = \mathbb{Z}_{>0}$, $\mathbb{Z}_{\geq 0}$ has one more element than S, but there is a one-to-one correspondence between them, so they have the same cardinality.

In class, we proved that there's no surjection from S to $P(S)$. This is the heart of the argument. Everything else (such as "why") is just a detail. When studying, we should try to synthesize the argument in a sentence.

Let's do some modular arithmetic!

Last time, we defined $a \pmod n$ as the remainder of $a \div n$.

Now let's prove something rather useful.

Proposition: Given $a \in \mathbb{Z}$, $n \in \mathbb{Z}_{>0}$, and $r \in \{0, 1, \ldots, n-1\}$,

$a \pmod n = r$ if and only if n divides $a - r$.

Proof:

($\Rightarrow$) If $a \pmod n = r$, then $a = qn + r$ for some $q \in \mathbb{Z}$ (we proved this the other day). Then $a - r = qn$, which is a multiple of n. //

($\Leftarrow$) If n divides $a - r$, then $a - r = qn$ for some $q \in \mathbb{Z}$. Thus, $a = qn + r \Rightarrow a \pmod n = r$. ∎

It's time for some new notation! We've been using the word "divides" a lot. Well, "$d \mid n$" means "d divides n."

Definition: Given $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}_{>0}$, we'll write $a \equiv b \pmod n$ if and only if $n \mid (a - b)$.

We briefly used this notation on Monday, but let's do some examples:

$23 \pmod 7 = 2$. Thus, $23 \equiv 2 \pmod 7$. Also, $7 \mid (23 - 30)$ and $7 \mid (23 + 5)$, so $23 \equiv 30 \pmod 7$ and $23 \equiv -5 \pmod 7$.

Let's do some arithmetic $\pmod 7$.

$3 - 5 \pmod 7 = -2 \pmod 7 = 5$.

$3 \cdot 5 \pmod 7 = 15 \pmod 7 = 1$.

$3^{-1} \pmod 7 = \frac{1}{3} \pmod 7$. How do we do this?

Well, what is $\frac{1}{3}$? It's the number we have to multiply by 3 to get 1. What number is that? Well, we showed $3 \cdot 5 \pmod 7 = 1$, so it seems like $\frac{1}{3} \pmod 7 = 5$.

This looks a little odd... but it's true! How else can we show it?

$\frac{1}{3} \pmod 7 = 1 \div 3 \pmod 7 \equiv 15 \div 3 \pmod 7 \equiv 5 \pmod 7$. Similarly, $\frac{1}{3} \pmod 7 \equiv \frac{8}{4} \pmod 7 = -2 \pmod 7 \equiv 5 \pmod 7$. This looks good!

Question: What is $\sqrt{2} \pmod 7$? $\sqrt{2}$ is the number we have to square to get $2. \pmod 7$, note that $3^2 \equiv 2 \pmod 7$, so it looks like $\sqrt{2} \equiv 3 \pmod 7$. However, numbers have two square roots, a positive one and a negative one, so $\sqrt{2} \equiv \pm 3 \pmod 7$. Thus, $\sqrt{2} \equiv 3 \pmod 7$ AND $\sqrt{2} \equiv -3 \equiv 4 \pmod 7$. (Cool!)

Finally, let's make a multiplication table $\pmod 7$. (We'll exclude the 0 row and column, since those would just be zeroes.)

x	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

(There are a lot of nifty patterns in this table (some rows are other rows, but backwards; no number appears in a row/column twice; the diagonals are symmetrical; etc.). What can you find? Why do you think these patterns appear?)