Monday

1. Uniqueness in Division Algorithm
2. Recall last time: gcd is linear combo and is 1 when rel. prime
3. Use 1/rel. prime to show Euclid's Lemma
4. Modular Arithmetic
   a. definition
   b. example
   c. theorem: a mod n = b iff n divides a-b
   d. reference exercise: We can "mod first"
5. Complex Numbers: Properties
6. Induction
   a. 1st Principle:
   b. Strong Form:
7. Use induction to prove Fund. Thm of Arithmetic
8. Use Fund. Thm of Arithmetic to prove infinitude of primes

Last time: If a, b are rel. prime then $\underbrace{\exists!}_{\text{there exists a unique}}$ $s, t \in \mathbb{Z}$ such that $as + bt = 1$

Ex:

$13s + 8t = 1$

$13(-3) + 8(5) = 1$

Today: use this idea to prove

Euclid's Lemma: If p is prime & $p \mid ab$, for $a, b \in \mathbb{Z}$ then $p \mid a$ or $p \mid b$

By the way primeness is important! B/c.

$6 \mid 24$ but $24 = 8 \cdot 3$ so $6 \mid 8 \cdot 3$ yet $6 \nmid 8$ & $6 \nmid 3$.

proof: Assume: p prime & $p \mid \overbrace{ab}^{ab = p \cdot q}$, & $p \nmid a$. We show $p \mid b$.

We then have: $ps + at = 1$. (b/c p is prime p is rel. prime to a) & $p \nmid a$.

mult. by b:

$pbs + abt = b$

$pbs + pqt = b$

$p(bs + qt) = b \Rightarrow p \mid b$. $\square$

Modular Arithmetic:

when we say $a = bn + r$ $(w/ \; 0 \le r < n)$ this means

$a \bmod n = r$ $a \% n = r$

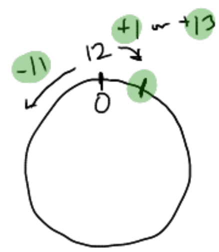
"a mod n is r"

"a modulo n is r"

For clocks (12-hr time)

$13 = 1 \cdot 12 + 1$ means $13 \bmod 12 = 1$

$-11 = (-1)12 + 1$ means $-11 \bmod 12 = 1$



1, 13, -11 all are equivalent modulo 12 ... because they all have remainder 1 in division algorithm.

Thm: You can mod first.

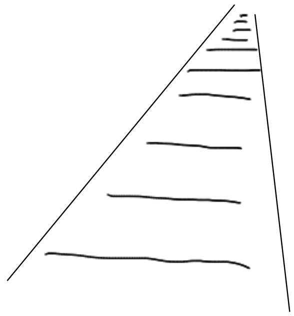
Ex. $17 + 9 \bmod 7 \longrightarrow 17 \bmod 7 + 9 \bmod 7$

or

$$\begin{aligned} &\downarrow & &= 3 + 2 \\ &26 \bmod 7 & &= 5 \\ &= 5 & & \end{aligned}$$

proof: Hint: If $a \bmod n = b$ then $a = nq + b$ $(0 \le b < n)$.

Induction: ∞



To climb ∞'ly high

1. get on ladder
2. know that, from wherever you stand, you can climb to the next rung

<u>theorem</u>: For any $n \in \mathbb{Z}^+$,

$$1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}$$

<u>prove</u>: (1) get on ladder (does it work for)

$$1 = \frac{1(1+1)}{2} \quad \text{(it works)}$$

(2) assume: $1 + 2 + \ldots + k = \frac{k(k+1)}{2}$

prove: we can climb

$$1 + 2 + \ldots + k + (k+1) = \frac{k(k+1)}{2} + \frac{(k+1)2}{2}$$

$$1 + 2 + \ldots + (k+1) = \frac{(k+1)(k+2)}{2}$$ By Induction this is true $\forall n \in \mathbb{Z}$

1. we saw: given $a \in \mathbb{Z}$, $b \in \mathbb{Z}^+$ we can always find $q \in \mathbb{Z}$ & r, s.t. $\underline{0 \le r < b}$ where:

$$a = bq + r$$

$\boxed{\text{Div. Alg.}}$

<u>Fact</u>: q & r are unique! Why?

Suppose $\quad a = \underbrace{bq + r = bq' + r'}_{}$ $\quad 0 \le r' < b$

greater?

$8 = 2 \cdot 4$

$2 | 8$

$$b(q - q') + r = r'$$

$$\boxed{b(q - q') = (r' - r)}$$

$\Rightarrow$ $b | r' - r$ is possible only if $r' - r = 0$ b/c $r' < b$