Friday (start w/ Hi-Lo-Gruffalo)

1. Well-Ordering Principle
2. Division Algorithm
3. Thm: gcd(a,b) is a linear combo of a,b
   a. Proof:
   b. Example
4. Euclid's Lemma
   a. Proof:
   b. Example
5. Fundamental Theorem of Arithmetic
6. Read first 6 pages to catch up - Modular arithmetic for the weekend

Pg: 1 – 6

Well-Ordering Principle: Every finite set of numbers has a minimum (not true for ∞ sets)
eg. In $\mathbb{R}$, $(1,2)$

Division Algorithm: $n=13$, $d=22$

For Any two ints, $n, d \in \mathbb{Z}$ (lives in) $\exists$ (there exists) $q \in \mathbb{Z}^+$ s.t. (or $\ni$ such that) $n = dq + r$ w/ $0 \le r < d$

Ex. $13 = 22 \cdot 0 + 13$

or $22 = 13 \cdot 1 + 9$

Greatest Common Division of $a, b \in \mathbb{Z}$, call it $\gcd(a,b)$. Largest int. dividing both a, b.

Notation: If d divides a, then we write $d \mid a$ meaning:

$a = dq$ (remainder $=0$)

If $\gcd(a,b)=1$ we say a, b are relatively prime.

Thm: $\gcd(a,b)$ is a linear combo of a, b.

proof: $S = \{$all possible non-negative linear combos of $a,b\}$
$= \{a \cdot s + b \cdot t \mid as + bt \ge 0\}$

S has a minimum elt, d. Assume $d = as + bt$.

Show $d \mid a$: By div. alg:

$a = dq + r$ w/ $0 \le r < d$.

$a = (as+bt)q + r$

$= asq + btq + r$

$a(1-sq) + b(-tq) = r$

So $r \in S$, & its smaller than d, the least thing in S, so $r = 0$.

$\Rightarrow a = dq \Rightarrow d \mid a$.

By similar reasoning (changing $a \leftrightarrow b$), we see $d \mid b$. $\Rightarrow$ d is a common divisor.

To see d is the greatest com. div, let d' be any common divisor of a, b: $a = d'q$, $b = d'm$

Recall $d = as + bt = d'qs + d'mt$

$d = d'(qs + mt)$, so $d' \mid d$.

So d is the greatest common divisor.

Any other common divisor divides d.
$\Rightarrow$ If M divides N, then $M \le N$.

Ex. $a=2$, $b=8$
$S = \{2, 8, 6, 4, \ldots\}$

Ex $a=5$, $b=2$
$S = \{5, 2, 7, 9, 3, 1, 4, \ldots\}$

Ex. $a=6$, $b=15$
$S = \{6, 15, 9, 3, \ldots\}$

$S = \{\_\ \_\ \_\ \_\}$

$8 = 2 \cdot 4$
$\Rightarrow 2 \mid 8$

For: $a=3$, $b=16$. (rel. prime) $1 = 3 \cdot (-5) + 1 \cdot 16$

$\gcd(3,16) = 1 \underset{\text{thm}}{=\!=} 3 \cdot (-5) + 16(1)$
(def.)

If a, b are rel prime then you can write
$1 = as + bt$

Relatively Prime: $\gcd(a,b)=1 \overset{\text{thm}}{\Longrightarrow} 1 = as+bt$. So a,b Rel Prime $\Rightarrow \exists\, s,t$ s.t.
If a,b rel prime $\Leftrightarrow$ $as+bt=1$

We'll use this often, for ex:

Euclid's Lemma: If p is prime, $p \mid ab \Rightarrow p \mid a$ or $p \mid b$.

proof: Assume $p \mid ab$ & $p \nmid a$, & show $p \mid b$.
So $ab = pq$ & since p is prime $\exists\, s,t \ni as+pt=1$.
To use assumption, hit eqn w/ b:

$$abs + pbt = b$$
$$pqs + pbt = b$$
$$p(qs+bt) = b$$

so $p \mid b$. Similarly for $p \mid a$.

Ex: $2 \mid 144$ & $144 = 12 \cdot 12$, $2 \mid 12$ ∴ || $144 = 16 \cdot 9$, $2 \mid 16$ ....

Non-Ex: $6 \mid 24$ yet $24 = 8 \cdot 3$ and $6 \nmid 8$ and $6 \nmid 3$

Fundamental thm of Arithmetic: For $n \in \mathbb{Z}^+$ n is prime or product of primes