Well-Ordering Principle: Every finite set has a least element. (Not true of ∞ sets)

Division Algorithm: Given $n, d \in \mathbb{Z}$ $\exists$ $0 \le r < d$ s.t. $n = dq + r$. (subtract d from n q times)

Ex: $21 = 5 \cdot 4 + 1$

Greatest Common Divisor of a, b: Largest divisor of both a, b. $\left(m \mid n \Rightarrow n = mq \right)$

Notation: $\gcd(a,b) = 1$ means a, b are relatively prime

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

Proof: Let S = {set of all possible non-negative linear combos of a, b}

$= \{ as + bt \mid as + bt \ge 0 \text{ w/ } a, s, b, t \in \mathbb{Z} \}$

— To show $\gcd(a,b) \in S$, generalize your Ex.

Ex: $a = 2$, $b = 8$
$S = \{2, 8, 10, 6, 4, \ldots\}$

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

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

see pattern???

S has a minimum, $d = as + bt$ for some s, t. To show it's the gcd, first show it divides a.

Div. Alg $\Rightarrow$ $\exists$ q, $0 \le r < d$ $a = dq + r$

$= (as + bt)q + r$

So, $a = asq + btq + r$ or $a(1 - sq) + b(-tq) = r$

Now r is a linear combo of a, b & thus lives in S.

But since r is less than the minimum elt, $r = 0$. So $a = dq$ or d divides a

Similarly, $d \mid b$ so d is a common divisor

If d' is an arbitrary divisor of a, b then $a = d'q$, $b = d'r$.

So $d = as + bt = d'qs + d'rt = d'(qs + rt)$ so d' divides d.

Example: $\gcd(24, 64) = 8$. $\rightsquigarrow$ $64(2) - 4(24) = 8$

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