Discrete Math

Video 31

The Fundamental Theorem of Arithmetic & Euclid's Lemma

Recall: a "lemma" is a theorem that is used to prove another, bigger theorem

Euclid's Lemma $\forall\, a, b, p \in \mathbb{Z}$

p is prime & $p \mid (ab) \Rightarrow$ $p \mid a$ or $p \mid b$

ex] $p = 5$ $\quad 35 = 5 \cdot 7$

$5 \mid 35$ ✓ $\quad$ EL $\Rightarrow$ $5 \mid 5$ or $5 \mid 7$

✓

ex| $7 \mid 252$

$252 = 14 \cdot 18$

E's L $\Rightarrow$ $7 \mid 14$ or $7 \mid 18$ ✓

non-ex| non prime (composite) $p = 6$

$6 \mid 24$ ✓ $\quad 24 = 3 \cdot 8$

$6 \nmid 3$ and $6 \nmid 8$

in fact, Euclid's Lemma has a true converse

Converse of E's Lemma $\forall\, p \in \mathbb{Z}$

if $\forall\, a, b \in \mathbb{Z}$, $p \mid (ab) \Rightarrow p \mid a \vee p \mid b$

then p is prime.

note one can use Bezout's Identity to write a slick proof of Euclid's Lemma!

(see assigned reading)

The Fundamental Theorem of Arithmetic

Every integer greater than one can be expressed as a (unique*) product of primes.

ex) $24 = 6 \cdot 4 = 2 \cdot 3 \cdot 2 \cdot 2$

$= 2 \cdot 2 \cdot 2 \cdot 3 = 2^3 \cdot 3 =$

* you can re-order the primes

This lets us think of numbers as being "built" by primes

primes $\cong$ elements in periodic table of numbers

catch: finding a big number's prime factor is VERY difficult

light comments on a proof of TFTA

- Euclid's Lemma is useful for showing uniqueness
- another lemma is useful for setting up the existence of such primes

(see assigned reading)