Sec 6.1: FTA

Def 6.1

(a) factor

(b) prime

(c) composite

Prob 6.2: 1 is neither prime nor composite

$\mathbb{N} = \{1\} \cup \{\text{primes}\} \cup \{\text{composites}\}$

↑ all pairwise disjoint

Prob 6.3: 2, 3, 5, 7, 11, 13, 17, 19, 23, 27, ...

Probs 6.4, 6.5: skip

Thm 6.6: If $n \in \mathbb{N}$ w/ $n > 1$, then n can be expressed as a product of primes:

$$n = p_1 \cdots p_k,$$

each p_i is prime (not necessarily distinct).

Pf: See take-home exam

Hint: Let $S = \{n \in \mathbb{N} \mid n > 1$ and n cannot be written as prod of primes$\}$

Goal: Show $S = \phi$.

For sake of a contradiction, assume $S \neq \phi$.

By WOP, S contains a least elmt, say n.

n cannot be prime $\Rightarrow$ n ~~composite~~ has a pair of divisors, say a, b w/ $1 \neq a, b \neq n$.

That is, $n = ab$. By Thm 2.56, $a, b < n$.

Are $a, b \in S$?

Where are we headed?

Goal: Thm 6.17 (FTA): Every nat # greater than 1 can be expressed uniquely (up to the order in which they appear) as the prod of primes

This is Thm 6.6 w/ uniqueness!

To get there, we need

- Thm 6.7 (Division Algorithm) proved for you in book

- Thm 6.13: (special case of Bezout's Lemma)

  If $p, a \in \mathbb{Z}$ s.t. p prime and p and a relatively prime, then $\exists\ s, t \in \mathbb{Z}$ s.t. $ps + at = 1$.

- Thm 6.15 (Euclid's Lemma) Assume p prime.

  If p divs ab w/ $a, b \in \mathbb{N}$, then either p divs a or p divs b.