## Sec G.I: FTA

## Def 6.1

- (a) factor
  - (b) prine
  - (c) composite

Prob6.2: 1 is neither prine noi composite

IN = {13 u { primes } u { composites}?

Tall pairwise disjoint

Pro 66.3: 2,3,5,7,11,13,17,19,23,27,...

Prohs 6.4, 6.5: Skip

Thm 6.6: If nEN w/ mod n > 1, then n can be expressed as a product of prims:

n=p, ... Pk,

rach pi is prime (not necessorily distinct).

Pf: See take-home exam

Hint: Let S = {n E/N | n cannot be written a sprood of prines}

Goal: Show S = d.

For sake of a contradiction, assure 5 + \$.

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

n cannot be prime => n cosupresida has a

pair of divisors, say a,b w 1 1 7 a,b 7 n.

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

Are a, b & S?

Where are we headed?

Goal: Then 6.17 (FTA): Every net # greater than I can be expressed uniquely (up to the order inwhich they appear) as the proof of prines.

This is Then 6.6 w/miqueness!

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 1, a ∈ Z s.t. p prine and 1 and a relatively prine, then ∃ s, t ∈ Z s.t. ps+at=1.
- . Thm 6.15 (Euclid's Lemma) Assure p prine.

  If p divs ab ulabell, then either p divsa

  or p divs b.