

• iPad notes now available on HW page

• Office hours survey - respond today if you want input

• Next presentations - respond ASAP

• Exam 2 graded - 20 point curve

Thm 2.1: McKenzie's proof can be understood as a strong induction:

Assume every k with $1 < k < n$ has a prime divisor.

Case 1: n is prime ✓

Case 2: n is composite $\Rightarrow n = xy$,

where $1 < x, y < n$

By inductive hyp., some $p|x \Rightarrow p|n$.

Thm 2.3: $n > 1$ is prime if and only if every prime $p \leq \sqrt{n}$ does not divide n .

n is prime \Rightarrow every prime $p \leq \sqrt{n}$ doesn't divide n ✓

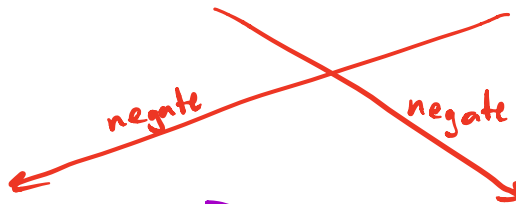
Every prime $p \leq \sqrt{n}$ doesn't divide $n \Rightarrow n$ prime

Equivalently,

n NOT prime

\Rightarrow

some prime $p \leq \sqrt{n}$ does divide n



Ex: 101 is prime $\sqrt{101} \approx \sqrt{100} = 10$

Check 2, 3, 5, 7 don't divide 101

47 $\sqrt{47} < \sqrt{49} = 7$

$2 \nmid 47, 3 \nmid 47, 5 \nmid 47 \Rightarrow 47$ is prime.

Next HW: 2.7 - 2.9

Fundamental Theorem of Arithmetic:

Every natural number $n > 1$ can be written uniquely as a product of primes.

\hookrightarrow up to reordering

$$\underline{\text{Ex:}} \quad 72 = 12 \cdot 6$$

$$= (4 \cdot 3)(2 \cdot 3)$$

$$= (2 \cdot 2 \cdot 3)(2 \cdot 3) = 2^3 \cdot 3^2$$

Existence (2.7) - use 2.1 and strong induction

Uniqueness (2.9) - Let

$$\{p_1, \dots, p_m\}$$

$$\{q_1, \dots, q_s\}$$

be sets of primes with

$$\left(\begin{array}{l} p_i \neq p_j \quad \text{if } i \neq j \\ q_i \neq q_j \end{array} \right)$$

no repeats

If

$$n = p_1^{r_1} \cdots p_m^{r_m}$$

$$= q_1^{t_1} \cdots q_s^{t_s}$$

then these are actually the same factorization

$$\bullet m = s$$

$$\bullet \{p_1, \dots, p_m\} = \{q_1, \dots, q_s\}$$

$$\bullet \text{if } p_i = q_j, \text{ then } r_i = t_j$$

Ex: $72 = \underline{2^3 \cdot 3^2}$

$= \underline{3^2 \cdot 2^3}$

$p_1=2, p_2=3$

$q_1=3, q_2=2$

Idea: Lemma 2.8 + induction

No class Friday