## Organization of materials in Sec 2.5

**(1)** Primes as indivisible units.

Def $\Rightarrow$ Lemma $\Rightarrow$ Prop. 2.53

**(2)** Primes make up all other integers.

Def $\Rightarrow$ Prop. 2.51 $\Rightarrow$ Prop. 2.54 $\Rightarrow$ Prop. 2.56 $\Rightarrow$ Props. 2.57, 2.58 $\Rightarrow$ Prop. 2.59

by2.53 UFT char divisors chars gcd, lcm

**(3)** Fundamental questions

- How many? Prop. 2.51 (by Def)
- How frequent? Prime number theorem
- Primality test: Prop. 2.55 (uses UFT 2.54)

## Summary of materials in Sec 2.5

**(1)** Primes as indivisible units. Let $p$ be prime.

- Def: $p$ has only two positive divisors $1, p$.
- Lemma: $\forall n \in \mathbb{Z}$, $\gcd(p, n) = 1$ if $p \not| n$, $\gcd(p, n) = p$ if $p|n$
- Prop. 2.53: $p|ab \Rightarrow (p|a$ or $p|b)$

**(2)** Primes make up all other integers.

- Prop. 2.51: all $n \geq 2$, $n \in \mathbb{Z}$ are products of primes.
- Prop. 2.54 (UFT): the list of primes unique
- Consequences of 2.54:
  - [UFT++] $n = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}$ for some unique $p_1 < p_2 < \cdots < p_m$, $e_i > 0$
  - [2.56] Char of divisors: $d|n$ iff $d = p_1^{d_1} p_2^{d_2} \cdots p_m^{d_m}$ where $\forall i, 0 \leq d_i \leq e_i$
  - [2.57,2.58] Char of gcd, lcm:

$$\text{If } n = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m},\ k = p_1^{f_1} p_2^{f_2} \cdots p_m^{f_m} \text{ where } e_i, f_i \geq 0,$$
$$\text{then, } \gcd(n,k) = p_1^{\min(e_1,f_1)} p_2^{\min(e_2,f_2)} \cdots p_m^{\min(e_m,f_m)}$$
$$\operatorname{lcm}(n,k) = p_1^{\max(e_1,f_1)} p_2^{\max(e_2,f_2)} \cdots p_m^{\max(e_m,f_m)}$$

**(3)** Fundamental questions

- How many? Prop. 2.51 (infinitely many)
- How frequent? Prime number theorem (# primes $\leq n \approx \frac{n}{\ln n}$, so frequency $\approx \frac{1}{\ln n}$
- Primality test for $n$: Prop. 2.55 (exhaustive search up to $\sqrt{|n|}$)