Last time: If \( N \) is an integer \( > 1 \), then \( N \) has a prime factor.

\[ N = a \cdot b, \ p \text{ divides } a, \ p \text{ also divides } N \]

Thm: \( \exists \) infinitely many prime numbers

Pf: By contradiction. Suppose only finitely many,

- call them \( p_1, p_2, \ldots, p_k \).

Consider \( N = p_1 p_2 \ldots p_k + 1 \).

Know: \( \exists \) \( p \) prime such that \( p \) divides \( N \)

\( \cdot \) \( p = p_1 \) or \( p_2 \) or \( \ldots \) or \( p_k \)

\( \cdot \) But \( \frac{N}{p_1} = p_2 \ldots p_k + \frac{1}{p_1} \) is not an integer

\[ \frac{1}{p_1} \text{ an integer, not an integer} \]

\[ \Rightarrow p_1 \text{ does not divide } N \]

\[ \Rightarrow p_2 \text{ does not divide } N, \]

\[ \vdots \]

\[ \Rightarrow p_k \text{ does not divide } N. \]

This is a contradiction. \( \square \)

Division Algorithm: If \( a, b \) are positive integers then

\( \exists \) unique integers \( q, r \) such that
∃ unique integers \( q, r \) such that
\[
a = b \cdot q + r \quad \text{with} \quad 0 \leq r < b
\]
\( q \): quotient, \( r \): the remainder

E.g. \( a = 21, \ b = 7 \) \( \Rightarrow \) \( 21 = 3 \cdot 7 + 0 \) \( q=3 \)
\( r=0 \)
\( a = 21, \ b = 6 \) \( \Rightarrow \) \( 21 = 3 \cdot 6 + 3 \) \( q=3 \)
\( r=3 \)

**Notation**: If \( a \) and \( b \) are two integers, we write \( a \mid b \) ("\( a \) divides \( b \)"") if \( \exists \) an integer \( c \) such that \( b = ac \).
We write \( a \nmid b \) if \( a \) does not divide \( b \).

E.g. \( 5 \mid 10, \ 3 \nmid 10, \ 6 \mid 0, \ -2 \nmid 4 \)

**Thm**: If \( a, b, d, r, s \) integers, \( d \neq 0 \), \( d \mid a, \ d \mid b \) then
\( d \mid (ra+sb) \) In particular, \( d \mid a+b, \ d \mid a-b, \ d \mid ra. \)

**Pf**: \( d \mid a \) means \( a = de \) \( \forall e \) an integer
\( d \mid b \) means \( b = df \) \( \forall f \) an integer
\[ra+sb = rde + sdf = d(re+sf) \Rightarrow d \mid (ra+sb).\]

**Prop**: If \( a, b, c \) are integers, \( a \neq 0, \ b \neq 0 \) and \( a \mid b, \ b \mid c \)
\( \Rightarrow \) \( a \mid c. \)
\[ \Rightarrow a/c. \]

**Pf:** Clear.

**Pap:** If \( n > 1 \) is an integer, then \( n \) is a finite product of prime numbers.

**Pf:** By induction. True for \( n=2 \) b/c 2 is prime. For general \( n \), if \( n \) is prime then we're done. Otherwise, \( n = a \cdot b \) w/ \( 1 < a < n \), \( 1 < b < n \).

By induction, \( a = p_1 \cdot \ldots \cdot p_k \quad b = p_{k+1} \cdot \ldots \cdot p_r \)

\[ \Rightarrow n = a \cdot b = p_1 \cdot \ldots \cdot p_k \cdot p_{k+1} \cdot \ldots \cdot p_r \] is a finite product of primes. \( \square \)

**Not at all "obvious":** The primes that appear in these factorizations are uniquely determined.

E.g. maybe \( p_1 p_2 p_3 = N = p_4 p_5 \) with the \( p_j \)'s all distinct.

We'll prove: Uniqueness of primes in factorizations.

**Detour C.C.D.'s (greatest common divisors):**

• Suppose \( a, b \) two integers
  • If \( a, b \) are not both 0, \( \exists \) only a finite number of common divisors of \( a \) and \( b \). One such integer is 1.

\[ \Rightarrow \exists \text{ a greatest common divisor, which is } \geq 1. \]

E.g. \( a = 10, \ b = 4 \)
E.g. \( a = 10, \ b = 4 \)

\[
\text{divisors of 10} \quad 1, 2, 5, 10, -1, -2, -5, -10
\]

\[
\text{divisors of 4} \quad 1, 2, 4, -1, -2, -4
\]

\[
\text{common divisors} \quad 2, 1 \quad \text{gcd} : 2
\]

Def \( \text{a, b integers, not both 0. Let } d \text{ be the largest} \)

\( \text{number in the set of common divisors of } \text{a and b. We call} \)

\( \text{the greatest common divisor and write } d = (a, b) \)

E.g. \( (4, 10) = 2, \quad (7, 3) = 1, \quad (4, 0) = 4, \quad (-6, 3) = 3, \quad (n, n) = n \quad \text{if } n > 0. \)

\( \text{(Aside: 10.0 = 0, 11.0 = 0, 12.0 = 0 \Rightarrow 10|0, 11|0, 12|0, \ldots)} \)

Divisors of \( a = \text{Divisors of } -a \)

Divisors of \( b = \text{Divisors of } -b \)

\( \Rightarrow (a, b) = (|a|, |b|) \)

- We'll focus on finding the gcd of positive integers.
- We'll give a fast algorithm.

Suppose \( a = 1234567, \ b = 568234 \)

Example (let check that gcd (1234567, 568234) = 3)

\( 54 = 2 \times 12 + 0 \quad \text{(division algorithm)} \)
Suppose \( d = \gcd(21, 54) \). Then \( d|12 = 54 - 2 \cdot 21 \)
\[ d|21, \ d|12 \quad \Rightarrow \quad d|21 - 1 \cdot 12 = 9. \]
\[ d|12, \ d|19 \quad \Rightarrow \quad \boxed{d|3}. \]

Conversely, \[ 3 = 12 - 1 \cdot 9 \quad \Rightarrow \quad 3|12 = 3 + 1 \cdot 9 \]
\[ 3|12 \quad \Rightarrow \quad 3|21 \]
\[ 3|12 \quad \Rightarrow \quad 3|54. \]

\[ \Rightarrow \quad 3 \text{ is a common divisor of } 21 \text{ and } 54. \]

\[ \Rightarrow \quad \gcd(21, 54) = 3. \]

This is an example of an algorithm that works in general.

We also get: \( 3 = 54 \cdot a + 21 \cdot b \) with integers \( a, b \) as follows
\[ 12 = 54 - 2 \cdot 21 \]
\[ 9 = 21 - 1 \cdot 12 = 21 - 1 \cdot (54 - 2 \cdot 21) = -1 \cdot 54 + 3 \cdot 21 \]
\[ 3 = 12 - 9 = (54 - 2 \cdot 21) - (-1 \cdot 54 + 3 \cdot 21) \]
\[ = 2 \cdot 54 - 5 \cdot 21 \]
Euclidean Algorithm. Given positive integers $d_2, d_1$, the E.A. finds $d = \gcd(d_2, d_1)$ and expresses $d = rd_2 + sd_1$ w/ $r, s$ integers.