Lecture 2

Wednesday, January 5, 2022 12:56 PM

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

$N = a \cdot b$, p divides a, p also divides N

Thm: $\exists$ infinitely many prime numbers

Pf: By contradiction. Suppose only finitely many,

call them $p_1, p_2, \dots, p_k$.

Consider $N = p_1 p_2 \cdots p_k + 1$.

- Know: $\exists$ p prime such that p divides N
- $p = p_1$ or p_2 or $\dots$ or p_k
- But $\frac{N}{p_1} = \underbrace{p_2 \cdots p_k}_{\text{an integer}} + \underbrace{\frac{1}{p_1}}_{\text{not an integer}}$ is not an integer

$\Rightarrow$ p_1 does not divide N

$\Rightarrow$ p_2 does not divide N,

$\vdots$

$\Rightarrow$ p_k " " " N.

This is a contradiction. ▨

Division Algorithm: If a, b are positive integers then

$\exists$ unique integers q, r such that

$\exists$ unique integers q, r such that

$$a = b \cdot q + r \quad \text{with} \quad \boxed{0 \leq r < b}$$

q: quotient, r: the remainde

E.g. · $a = 21,\ b = 7 \Rightarrow 21 = 3 \cdot 7 + 0$ $\quad q = 3,\ r = 0$

· $a = 21,\ b = 6 \Rightarrow 21 = 3 \cdot 6 + 3$ $\quad q = 3,\ r = 3$

Notation: · If a and b are two integers, we write $a|b$ ("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. $5|10,\ 3 \nmid 10,\ 6|0,\ -2|4$

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

Pf: $d|a$ means $a = de$ w/ e an integer

$d|b$ means $b = df$ w/ f an integer

$ra + sb = rde + sdf = d(re + sf) \Rightarrow d|(ra+sb)$. ∎

Prop^n If a, b, c are integers, $a \neq 0$, $b \neq 0$ and $a|b$, $b|c$ $\Rightarrow a|c$.

$\Rightarrow a \mid c$.

Pf: Clear.

Prop: 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, $a = p_1 \cdots p_k$ $b = p_{k+1} \cdots p_r$

$\Rightarrow$ $n = a \cdot b = p_1 \cdots p_k p_{k+1} \cdots p_r$ is a fte product of primes. □

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 GCD'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.
  $\Rightarrow \exists$ a greatest common divisor, which is ≥ 1.

E.g. $a = 10$, $b = 4$

E.g. $a = 10, \quad b = 4$

divisors of 10: $1, 2, 5, 10, -1, -2, -5, -10$

divisors of 4: $1, 2, 4, -1, -2, -4$

common divisors: $1, (2), -1, -2$

gcd: 2

Defn a, b integers, not both 0. Let d be the largest number in the set of common divisors of a and b. We call d the greatest common divisor and write $d = (a, b)$

E.g. $(4, 10) = 2, \quad (7, 3) = 1, \quad (4, 0) = 4, \quad (-6, 3) = 3.$

$(n, n) = n$ if $n > 0$.

(Aside: $10 \cdot 0 = 0, \quad 11 \cdot 0 = 0, \quad 12 \cdot 0 = 0 \Rightarrow 10 | 0, 11 | 0, 12 | 0, \ldots$)

Divisors of a = Divisors of $-a$
Divisors of b = 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 $a = 1,234,567 \quad b = 568234$

Example Let check that $\gcd(21, 54) = 3$.

$54 = 2 \cdot 21 + 12$ (division algorithm)

$54 = 2 \cdot 21 + 12$

$21 = 1 \cdot 12 + 9$

$12 = 1 \cdot 9 + 3$

$9 = 3 \cdot 3 + 0$

(division algorithm)

- Suppose $d = \gcd(21, 54)$. Then $d \mid 12 = 54 - 2 \cdot 21$
- $d \mid 21$, $d \mid 12 \Rightarrow d \mid 21 - 1 \cdot 12 = 9$.
- $d \mid 12$, $d \mid 9 \Rightarrow \boxed{d \mid 3}$

Conversely: • $3 = 12 - 1 \cdot 9 \Rightarrow 3 \mid 12 = 3 + 1 \cdot 9$

• $3 \mid 12$ & $3 \mid 9 \Rightarrow 3 \mid 21$

• $3 \mid 12$ & $3 \mid 21 \Rightarrow 3 \mid 54$.

$\Rightarrow$ **3 is a common divisor of 21 & 54.**

$\Rightarrow \gcd(21, 54) = 3$.

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

We also get: $3 = 54 \cdot a + 21 \cdot b$ w/ a, b integers 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

$$d = r d_{-2} + s d_{-1} \quad \text{w/ } r, s \text{ integers.}$$