MAT 312

08/29/19

Main Thm last time: If $a, b \in \mathbb{Z}^+$ $\exists \alpha, \beta \in \mathbb{Z}$ s.t. $\alpha a + \beta b = \gcd(a,b)$

Cor 1: Let $a, b, c \in \mathbb{Z}^+$ with $\gcd(a,b) = 1$

(i) If $a \mid bc$, then $a \mid c$ (ii) if $a \mid c$ and $b \mid c$, then $ab \mid c$

Well-Ordering Principle $\Rightarrow$ Main Thm $\Rightarrow$ Cor 1

Cor 2: 1.1 6 on HW 1

Lemma 2 here

Lemma 1 (Division w. Remainder) If $a \in \mathbb{Z}^+$, $b \in \mathbb{Z}$, $\exists q, r \in \mathbb{Z}$ s.t. $0 \le r < a$ and $b = qa + r$.

Lemma 2 If $q \in \mathbb{Z}$ and $a, r, aq + r \in \mathbb{Z}^+$, then $\gcd(a,r) = \gcd(a, aq+r)$

proved last time

Euclid's algorithm: Given $a, b \in \mathbb{Z}^+$, $a \le b$, find $\alpha, \beta \in \mathbb{Z}$ s.t. $\alpha a + \beta b = \gcd(a,b)$

Lemma 1 $\Rightarrow \exists q_1, r_1 \in \mathbb{Z}^{\ge 0}$ s.t. $0 \le r_1 < a$, $b = q_1 a + r_1$

if $r_1 = 0$, $a \mid b \Rightarrow a = \gcd(a,b) = 1 \cdot a + 0 \cdot b$

o/w Lemma 2 $\Rightarrow \gcd(a,b) = \gcd(a, r_1)$

Lemma 1 $\Rightarrow \exists q_2, r_2 \in \mathbb{Z}^{\ge 0}$ s.t. $0 \le r_2 < r_1$, $a = q_2 r_1 + r_2$

get $b = q_1 a + r_1$ w. $0 < r_1 < a$, $q_1 \ge 0$

$r_0 = a = q_2 r_1 + r_2$ w. $0 < r_2 < r_1$, $q_2 \ge 0$

$\vdots$

$r_{n-2} = q_n r_{n-1} + r_n$ w. $0 < r_n < r_{n-1}$, $q_n \ge 0$

$r_{n-1} = q_{n+1} r_n + r_{n+1}$ → eventually 0

b/c $0 \le r_{n+1} < r_n < \dots < r_1 < a$

→ Stop $r_n \mid r_{n-1}$

$\Rightarrow r_n = \gcd(r_n, r_{n-1}) = \gcd(q_n r_{n-1} + r_n, r_{n-1})$ (Lemma 2; r_{n-2})

$= \gcd(r_{n-2}, r_{n-3}) = \dots = \gcd(a,b)$

→ Solve backwards for r_n = in terms of a, b

$r_n = r_{n-2} - q_n r_{n-1} = r_{n-2} - q_n (r_{n-3} - q_{n-1} r_{n-2})$

Continue plugging in for r_n ...

Example Find α, β s.t. $24\alpha + 34\beta = \gcd(24,34) = 2$

(1) $34 = 1 \cdot 24 + 10$ ← remainder of division of 34 by 24

(2) $24 = 2 \cdot 10 + 4$ ← " of 24 by 10

(3) $10 = 2 \cdot 4 + 2$ ←

(4) $4 = 2 \cdot 2 + 0 \Rightarrow 2 = \gcd(24,34)$

$2 \overset{(3)}{=} 10 - 2 \cdot 4 \overset{(2)}{=} 10 - 2 \cdot (24 - 2 \cdot 10) = 5 \cdot 10 - 2 \cdot 24$

$\overset{(1)}{=} 5 \cdot (34 - 1 \cdot 24) - 2 \cdot 24 = 5 \cdot 34 - 7 \cdot 24$

(α, β) $= 2$

Today's Main Thm: Unique Factorization for $\mathbb{Z}^+$

$\forall n \in \mathbb{Z}^+$, $n \ge 2$, $\exists!$ primes $p_1 \le p_2 \le \dots \le p_r$ s.t. $n = p_1 p_2 \dots p_r$

($\exists!$ = unique)

$p \in \mathbb{Z}^+$ is prime if it has precisely 2 divisors i.e. 1 and p ($p \ne 1$)

$\Rightarrow$ 1 is not prime; primes: 2, 3, 5, 7, 11, ...

example / thm first; proof (by induction) next

Example $90 = 2 \cdot 3 \cdot 3 \cdot 5 \Rightarrow \exists p_1 \le \dots \le p_r$ ✓ ($p_1 p_2 p_3 p_4$)

Uniqueness: if $90 = 2 \cdot 3 \cdot 3 \cdot 5 = q_1 \cdots q_s$ with $q_1 \le q_2 \le \dots \le q_s$ prime then $s = 4$

$q_1 = 2$ $q_2 = 3$ $q_3 = 3$ $q_4 = 5$

Crl 3 ∃ infinitely many primes

Pf: By contradiction. Suppose $p_1, \dots, p_n$ are all the primes. Let $N = p_1 \cdots p_n + 1$

$N \geq 2 \xrightarrow{\text{Thm}}$ N has a prime divisor p

$p_i \nmid N$ b/c remainder of division of N by p_i is 1

$\Rightarrow p \neq p_1, \dots, p_n$ is another prime; contradiction

---

Pf of Lemma 3: $p, a, b \in \mathbb{Z}^+$, p prime

If $p \nmid a$, then $\gcd(p, a) = 1$ b/c only 1, $p \mid p$ and $p \nmid a$

Lemma last time: Suppose $p, a, b \in \mathbb{Z}^+$ and $\gcd(p, a) = 1$

If $p \mid ab$, then $p \mid b$

∴ If $p, a, b \in \mathbb{Z}^+$, p prime, $p \mid ab$, but $p \nmid a$, then $p \mid b$ ✓

Pf of Main Thm: (i) Existence of decompositions

Given $n \in \mathbb{Z}^+$, $n \geq 2$, $\exists p_1, \dots, p_r$ prime s.t. $n = p_1 \cdots p_r$

Pf by induction on n Base case $n = 2 \cdot 2 = 2$ ✓ ($p_1 = p_r$, p prime)

Suppose true for all $2 \leq n < N$

If N is prime, then $N = N \cdot 1$, p_1 is the decomp.

If N is not prime, then $N = ab$ for some $2 \leq a, b < N$

Pf of uniqueness: Suppose $p_1 \cdots p_r = q_1 \cdots q_s$ and

$p_1 \leq p_2 \leq \cdots \leq p_r$; $q_1 \leq q_2 \leq \cdots \leq q_s$ are primes; $r \leq s$

Then $r = s$ and $p_1 = q_1, \dots, p_r = q_r$.

Proof by induction on r: → can assume $r \leq s$

Base case $r = 1$

$p_1 = q_1 \cdots q_s \xrightarrow{\text{Lemma 4}} p_1 \mid q_i$ for some $i = 1, \dots, s$

q_i prime $\Rightarrow q_i = p_1$; divide by p_1

rest of q_j's multiply to 1 $\Rightarrow$ there were not any of them

$\Rightarrow r = s = 1$, $p_1 = q_1$ ✓

For proof of Today's Main Thm, need

Lemma 3: Suppose $p, a, b \in \mathbb{Z}^+$ and p is prime

If $p \mid ab$, then either $p \mid a$ or $p \mid b$

Lemma 4: Suppose $p, a_1, \dots, a_s \in \mathbb{Z}^+$ and p is prime

If $p \mid a_1 \cdots a_s$, then $p \mid a_i$ for some $i = 1, \dots, s$

Need p prime, e.g. $6 \mid 2 \cdot 3$ but $6 \nmid 2$ and $6 \nmid 3$

Pf of Lemma 4 (induction) ∀ s

Base case ($s = 1$) If $p \mid a_1$, then $p \mid a_1$ ✓

Inductive step: Suppose $p \mid a_1 \cdots a_s \Rightarrow p \mid a_i$ for some i

Suppose $p \mid a_1 \cdots a_s a_{s+1} = (a_1 \cdots a_s) a_{s+1}$

Lemma 3 $\Rightarrow p \mid (a_1 \cdots a_s)$ or $p \mid a_{s+1}$

Inductive assumption $\Rightarrow p \mid a_i$ for some $i = 1, \dots, s$

∴ $p \mid (a_1 \cdots a_{s+1}) \Rightarrow p \mid a_i$ for some $i = 1, \dots, s+1$ ✓

Inductive assumption $\Rightarrow a = p_1 \cdots p_r$, $b = q_1 \cdots q_s$

for some primes $p_1 \cdots p_r, q_1, \dots, q_s$

$\Rightarrow N = p_1 \cdots p_r q_1 \cdots q_s$

$\Rightarrow$ get prime decomposition of N

Inductive step: Suppose the statement is true for r.

and $p_1 \cdots p_{r+1} = q_1 \cdots q_s$, all primes

Lemma 4 $\Rightarrow p_{r+1} \mid q_i$ for some $i = 1, \dots, s$

let's say q_s

q_s prime $\Rightarrow p_{r+1} = q_s$.

Divide both sides by this to get

$p_1 \cdots p_r = q_1 \cdots q_{s-1}$

inductive assumption $\Rightarrow p_1 = q_1$, ... etc.