453 Lecture 7

1. Prime factorization theorem

i) **Def.** A natural number p is a prime if $p \geq 2$ and the only divisors of p are 1 and p.

ii) **Prop.** Let p be a prime, and $a, b \in \mathbb{N}$. If $p \mid ab$ then $p \mid a$ or $p \mid b$.

Proof Suppose $p \mid ab$ and $p \nmid a$.

If $p \nmid a$ and p is a prime, since the only divisors of p are 1 and p

$$\gcd(p, a) = 1.$$

By Bezout identity there exists $x, y \in \mathbb{Z}$ such that

$$1 = px + ay.$$

Multiplying both sides by b,

$$b = bpx + aby$$

Now $p \mid bpx$, and also $p \mid aby$ (because $p \mid ab$).

So $p \mid b$. $\blacksquare$

Scanned by CamScanner

iii) <u>Prop</u> If p is a prime, $a_1, \ldots, a_n \in \mathbb{Z}$ and $p \mid a_1 \cdots a_n$. Then there exists $1 \leq i \leq n$ such that $p \mid a_i$.

<u>Pf</u>: Use induction on n and use the previous proposition. ◻

iv) Thm (Existence and uniqueness of prime factorization). Let $n \in \mathbb{N}$, $n > 0$. Then there n can be expressed as a product $p_1 \cdots p_r$ where each p_i is a prime (not necessarily distinct primes).
Moreover if there is another expression

$n = q_1 \cdots q_s$ with each q_i prime,

then $r = s$ and there exists a bijection $\pi : \{1, \ldots, r\} \to \{1, \ldots, r\}$ such that

$p_i = q_{\pi(i)}$ for $1 \leq i \leq r$.

<u>Pf</u>: To prove existence of the prime decomposition use induction on n.

To prove uniqueness use induction on $\max(r, s)$ and the previous proposition ◻