(Chapter 7)

In this lecture, we study the decomposition of integers, which is known as the fundamental theorem of arithmetic.

Lemma 2 (7.1) Let p be a prime number. Suppose that $p \mid (ab)$. Then either $p \mid a$ or $p \mid b$.

Proof: Assume that $p \mid (ab)$

If $p \mid a$, then the proof is finished.

If $p \nmid a$, then by Lemma 1, $\gcd(p, a) = 1$.

Then by the theorem is last lecture, we can find r, s such that

$$rp + sa = 1. \quad (= \gcd(p, a))$$

Multiply the equation by b,

$$rpb + sab = b.$$

$$p \mid p \qquad p \mid ab \Rightarrow p \mid (rpb + sab) = b$$

Therefore, if $p \nmid a$, then $p \mid b$ □.

Theorem (7.2. Prime Divisibility Property)

Let p be a prime. Suppose that

$$p \mid (a_1 a_2 a_3 \cdots a_r)$$

Then p divides at least one of them.

Proof: We can write

$$a_1 a_2 \cdots a_r = a_1 (a_2 \cdots a_r)$$

$$p \mid (a_1 a_2 \cdots a_r) \overset{\text{Lemma 2}}{\Longrightarrow} p \mid a_1 \text{ or } p \mid (a_2 \cdots a_r)$$

If $p \mid a_1$, ✓

If $p \nmid a_1$, $p \mid a_2 \cdots a_r$.

Again, we write $a_2 \cdots a_r = a_2 (a_3 \cdots a_r)$

We can continue this process and

we can show p divides at least one

of $a_1, \cdots a_r$ □.

Theorem (7.3, the fundamental theorem of arithmetic)

For every integer $n \geq 2$, it can be factored

into a product of primes:

$$n = p_1 p_2 \cdots p_r$$

in exactly one way (up to rearrangement).

Remark: (1) If n is a prime

$$n = n.$$

(2) We don't require that p_i be distinct.

Indeed: $12 = 2 \cdot 2 \cdot 3$

$p_1 \; p_2 \; p_3$

(3) This decomposition/factorization is unique if we don't care about the order.

$$\left.\begin{aligned} 12 &= 2 \cdot 2 \cdot 3 \\ &= 2 \cdot 3 \cdot 2 \\ &= 3 \cdot 2 \cdot 2 \end{aligned}\right\}$$ They are treated as the same.

(4) To prove the theorem, we need to show 2 things:

① Every $n \geq 2$ can be written as the product of primes.

② The factorization is unique.

Proof: We proof by the (complete) induction.

$P(n)$: n can be written as the product of primes

Step I: $P(2)$: This is obvious since

$$2 = 2 \qquad (2 \text{ is prime})$$

Step II: Suppose that this is true for

$$P(2), P(3), \cdots P(n)$$

We look at $P(n+1)$.

We consider two cases.

① If $n+1$ is a prime, then the factorization is:

$$n+1 = n+1.$$

② If $n+1$ is not a prime, then we can write $n+1 = a\,b$.

Notice: $2 \le a \le n \Rightarrow P(a)$ is true

$2 \le b \le b \Rightarrow P(b)$ is true.

Therefore: $a = p_1 \cdots p_r$

$b = q_1 \cdots q_s$

$n+1 = a \cdot b = p_1 \cdots p_r\, q_1 \cdots q_s$

This is a product of primes.

By induction, every integer $n \ge 2$ can be written as the product of primes.

Next, we show there is only one way!

Suppose that: (we can assume $r \le s$)

$n = p_1 p_2 \cdots p_r$

$$= q_1 q_2 \cdots q_s.$$

We need to show: $r = s$

After rearrangement, we can show

$$p_1 = q_1,\ p_2 = q_2,\ p_3 = q_3 \cdots p_r = q_r$$

Indeed: $p_1 \mid n = q_1 \cdots q_s$

Then p_1 divides one of $q_1, \cdots, q_s$

After rearragnets, we assue $p_1 \mid q_1$

p_1, q_1 are both prime $p_1 \mid q_1 \Rightarrow p_1 = q_1$

In this case.

$$n = p_1 p_2 \cdots p_r$$

$$= \underline{q_1} q_2 \cdots q_s = \underline{p_1} q_2 \cdots q_s$$

Then we divide n by p_1

$$\frac{n}{p_1} = p_2 \cdots p_r$$

$$= q_2 \cdots q_s$$

We repeat this process, and we can show $p_2 = q_2$

Then we divide $\frac{n}{p_1}$ by p_2

$$\frac{n}{p_1 p_2} = p_3 \cdots p_r$$

$$= q_3 \cdots q_s$$

We repeat this $\cdots$ and finally we show:

$$\frac{n}{p_1 \cdots p_r} = 1$$

$$= q_{r+1} \cdots q_s \Rightarrow q_{r+1} = \cdots q_s = 1$$

Therefore $r = s$. □

Here is another way to demonstrate the uniqueness: we collect all the same primes together and write it in the power form.

Example: $100 = 2 \cdot 5 \cdot 2 \cdot 5$

$$= 2^2 \cdot 5^2$$

$$162 = 2 \cdot 3 \cdot 3 \cdot 3 \cdot 3$$

$$= 2 \cdot 3^4.$$

Theorem: For any integer $n \geq 2$, n can be factored as:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

with $p_1, \cdots p_r$ being distinct

This factorization is unique.