(Chapter 7).

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

Before the proof, we need several lemmas:

Lemma 1: Let p be a prime and n an arbitrary integer. Then either

$$\gcd(p, n) = 1 \quad \text{or} \quad p \mid n.$$

Proof: We know that

$$\gcd(p, n) \mid p.$$

Since p is a prime, p has only 2 divisors 1 and p.

If $\gcd(p, n) = 1$, this is the first case.

If $\gcd(p, n) = p$, then $p \mid n$. This is the second case. $\square$

Remark: If we futher assume that n is a prime, then either $(p, n) = 1$ or $p = n$.

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

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

Multiply the equation by b,

$$rpb + sab = b.$$

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

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

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

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

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

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: $12 = \underset{p_1}{2} \cdot \underset{p_2}{2} \cdot \underset{p_3}{3}$

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

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

(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

$2 = 2$ (2 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 $n+1 = ab$.

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

$2 \leq b \leq b \Rightarrow P(b)$ 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 $n \geq 2$ can be written as the product of primes.

Next, we show there is only one way!

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

$n = p_1 p_2 \cdots p_r$

$= q_1 q_2 \cdots q_s.$

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 rearrangement, we assume $p_1 \mid q_1$

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 ... 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 $r=s$. $\square$

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.

Some applications

I. The factorization of numbers give another way to find gcd. This may not be efficient but useful.

Example: find gcd (700, 360)

$$700 = 2^2 \cdot 5^2 \cdot 7 = 2^2 \cdot 3^0 \cdot 5^2 \cdot 7^1$$

$$360 = 2^3 \cdot 3^2 \cdot 5 = 2^3 \cdot 3^2 \cdot 5^1 \cdot 7^0$$

Find the smaller power in each prime

$$\gcd(700, 360) = 2^2 \cdot 3^0 \cdot 5^1 \cdot 7^0$$

$= 2^2 \cdot 5^1 = 20.$

Observation: Let m, n be two integers.

$\gcd(m, n) = 1$ is equivalent to

m, n have no common primes.

II. A useful lemma.

Lemma: Let m, n be integers such that $\gcd(m,n)=1$. Then for any integers α, β, $\gcd(m^{\alpha}, n^{\beta}) = 1$.

Proof: $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$

$n = q_1^{\beta_1} \cdots q_s^{\beta_s}$

$\gcd(m,n)=1 \Rightarrow \{p_1, \cdots p_r\} \cap \{q_1, \cdots q_s\} = \phi.$

$m^{\alpha} = p_1^{\alpha_1 \alpha} \cdots p_r^{\alpha \alpha_r}$

$n^{\beta} = q_1^{\beta_1 \beta} \cdots q_s^{\beta_s \beta}$

m^{α}, n^{β} have no common primes.

and hence $\gcd(m^{\alpha}, n^{\beta}) = 1$ $\square$

III. Proposition: Let n be an integer and p a prime. Then we can find an integer $\alpha \geq 0$ and an integer m such that

$$n = p^{\alpha} m$$

and $\gcd(p, m) = 1$.

Proof: When $p \nmid n$, $\alpha = 0$, $m = n$.

When $p \mid n$, by the factorization

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

One of $p_1, \cdots p_r$ must be p; say p_1, then $\alpha = \alpha_1$ $\quad m = p_2^{\alpha_2} \cdots p_r^{\alpha_r}$.

We can show:

$$\gcd(p, m) = \gcd(p, p_2^{\alpha_2} \cdots p_r^{\alpha_r}) = 1. \square$$

Definition: Let n be an integer, and p a prime. Then we can find $\alpha \geq 0$ and m such that $n = p^{\alpha} m$ with $(p, m) = 1$.

We write: $\operatorname{ord}_p(n) = \alpha$.

We also write $p^{\alpha} \| n$

read: p^{α} exactly divides n.

Example: $48 = 2^4 \cdot 3$

$\Rightarrow \operatorname{ord}_2(48) = 4$

$2^4 \| 48$.