3.5 The Fundamental Theorem of Arithmetic

This theorem says that the primes are the multiplicative building blocks of the integers.

ex: $10 = 2 \cdot 5$, $\quad 60 = 2 \cdot 2 \cdot 3 \cdot 5 = 2^2 \cdot 3 \cdot 5$

Lemma 3.4: Let $a, b \in \mathbb{Z}^+$ and $\gcd(a,b) = 1$. Then,

$$a \mid bc \Rightarrow a \mid c.$$

Proof: Since $\gcd(a,b) = 1$, $\exists\ m, n \in \mathbb{Z}$ s.t.

$$ma + nb = 1.$$

$$\therefore mac + nbc = c$$

Now, $a \mid a$ and $a \mid bc$, so

$$a \mid (mac + nbc)$$

$$\therefore a \mid c.$$

Lemma 3.5: Let p be a prime and $a_1, a_2, \cdots, a_n \in \mathbb{Z}^+$. Then,

$$p \mid a_1 a_2 \cdots a_n \Rightarrow p \mid a_i \text{ for some } i.$$

Proof: We use induction on n. When $n = 1$, the result is trivially true.

Assume, $p \mid a_1 a_2 \cdots a_{k-1} \Rightarrow p \mid a_i$ for some i.
Need to show that

$$p \mid a_1 a_2 \cdots a_k \Rightarrow p \mid a_i \text{ for some } i.$$

Suppose $p \mid a_1 a_2 \cdots a_k$ — (1)

We know, $\gcd(p, a_1a_2\cdots a_{k-1}) = 1$ or p
If $\gcd(p, a_1a_2\cdots a_{k-1}) = 1$, then by Lemma 3.4, and (1), $p \mid a_k$.
If $\gcd(p, a_1, a_2, \ldots, a_{k-1}) = p$, then $p \mid a_1a_2\cdots a_{k-1}$ and then by the induction hypothesis, $p \mid a_i$ for some i.
Hence the lemma.

Theorem 3.15 (Fundamental Theorem of Arithmetic):
Let $n \in \mathbb{Z}^+$, $n > 1$. Then, n is a prime or can be written uniquely as a product of primes.

Proof: We use induction on n.
When $n=2$, the theorem is true since 2 is a prime.
Suppose the theorem is true for all integers $2, 3, 4, \ldots, k-1$.

Consider the integer k.
If k is prime, then we're done!

If k is not a prime, then it is composite. Then,

$$k = ab \quad \text{with} \quad 1 < a, b < k.$$

Then, by the induction hypothesis, each of a and b is a prime or a product of primes.

Then, ab is a product of primes.

$\therefore$ k is a product of primes.
Hence, by mathematical induction, ever integer greater than 1 is a prime or a product of primes.
Next, we prove the uniqueness.
We use the method of contradiction.

Suppose the product is not unique.
Then, $\exists$ 2 different representations of n.
Let them be

$$n = p_1 p_2 \cdots p_m \text{ and } n = q_1 q_2 \cdots q_n \quad \text{—— } (1)$$

where p_i's and q_i's are primes with

$$p_1 \leq p_2 \leq \cdots \leq p_m \text{ and } q_1 \leq q_2 \leq \cdots \leq q_n .$$

Suppose we remove all common primes from (1) to get

$$n = p_{i_1} p_{i_2} \cdots p_{i_u} = q_{j_1} q_{j_2} \cdots q_{j_v} \quad \text{—— } (2)$$

Now, each p_{i_r} should be different from all q_{j_s} because we assumed that the two representations are different.

But, (2) implies that $p_{i_1} \mid q_{j_s}$ for some s.

Since p_{i_1} and q_{j_s} are primes, we should have $p_{i_1} = q_{j_s}$, a contradiction.

Hence, the uniqueness and the theorem follows.

<u>ex</u>! $120 = 2^3 \cdot 3 \cdot 5$

All factors of 120 can be found.

1	3	5	$3 \cdot 5 = 15$
2	$2 \cdot 3 = 6$	$2 \cdot 5 = 10$	$2 \cdot 3 \cdot 5 = 30$
$2^2 = 4$	$2^2 \cdot 3 = 12$	$2^2 \cdot 5 = 20$	$2^2 \cdot 3 \cdot 5 = 60$
$2^3 = 8$	$2^3 \cdot 3 = 24$	$2^3 \cdot 5 = 40$	$2^3 \cdot 3 \cdot 5 = 120$

We can use the prime factorization to find the gcd of two positive integers.

<u>ex</u>! $24 = 2^3 \cdot 3$

$60 = 2^2 \cdot 3 \cdot 5$

$\therefore \gcd = 2^2 \cdot 3 = 12$

In general, if $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ and

$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}$

where $\alpha_i, \beta_i \geq 0$, then

$$\gcd(a,b) = p_1^{\min(\alpha_1,\beta_1)} \cdot p_2^{\min(\alpha_2,\beta_2)} \cdots p_n^{\min(\alpha_n,\beta_n)}$$

ex: $24 = 2^3 \cdot 3^1 \cdot 5^0$

$60 = 2^2 \cdot 3^1 \cdot 5^1$

$$\gcd(24,60) = 2^{\min(3,2)} \cdot 3^{\min(1,1)} \cdot 5^{\min(0,1)}$$

$$= 2^2 \cdot 3^1 \cdot 5^0 = 12$$

Definition: The least common multiple of two nonzero integers a and b is the smallest positive integer that is divisible by both a and b. It is denoted by lcm(a,b).

Thus, $c = \mathrm{lcm}(a,b)$ if and only if

$a \mid c$, $b \mid c$ and

$a \mid e$ and $b \mid e \Rightarrow c \leq e$.

ex: $\mathrm{lcm}(4,6) = 12$

$\mathrm{lcm}(7,8) = 56$

$\mathrm{lcm}(a,a) = a$

We can use the fundamental theorem of arithmetic to find lcm as follows.

Let $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ and

$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}$ where $\alpha_i, \beta_i \geq 0$

and p_i's are primes.

Then, $\operatorname{lcm}(a,b) = p_1^{\max(\alpha_1,\beta_1)} p_2^{\max(\alpha_2,\beta_2)} \cdots p_n^{\max(\alpha_n,\beta_n)}$.

ex: $75 = 2^0 \cdot 3^1 \cdot 5^2$
$36 = 2^2 \cdot 3^2 \cdot 5^0$
$\operatorname{lcm}(75,36) = 2^2 \cdot 3^2 \cdot 5^2 = 900$

There is a relationship between gcd and lcm. First we prove a lemma.

Lemma 3.6: For $x, y \in \mathbb{R}$,
$$\max(x,y) + \min(x,y) = x + y.$$

Proof: If $x \geq y$,
$$\max(x,y) + \min(x,y) = x + y$$

If $x < y$,
$$\max(x,y) + \min(x,y) = y + x = x + y.$$

Theorem 3.16: Let $a, b \in \mathbb{Z}^+$. Then,

$$\gcd(a,b) \cdot \operatorname{lcm}(a,b) = ab$$

Proof: Let $a = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ and

$b = p_1^{\beta_1} \cdots p_n^{\beta_n}$.

Then, we saw that

$$\gcd(a,b) = p_1^{\min(\alpha_1,\beta_1)} \cdots p_n^{\min(\alpha_n,\beta_n)}$$

and

$$\operatorname{lcm}(a,b) = p_1^{\max(\alpha_1,\beta_1)} \cdots p_n^{\max(\alpha_n,\beta_n)}$$

Then,

$$\gcd(a,b) \cdot \operatorname{lcm}(a,b) =$$

$$p_1^{\min(\alpha_1,\beta_1)+\max(\alpha_1,\beta_1)} \cdots p_n^{\min(\alpha_n,\beta_n)+\max(\alpha_n,\beta_n)}$$

$$= p_1^{\alpha_1+\beta_1} \cdots p_n^{\alpha_n+\beta_n}$$

$$= (p_1^{\alpha_1} \cdots p_n^{\alpha_n})(p_1^{\beta_1} \cdots p_n^{\beta_n})$$

$$= ab$$

Theorem 3.17: There are infinitely many primes of the form $4n+3$, where $n \in \mathbb{Z}^+$.

Proof: See page 118 of the textbook. Use the following lemma.

Lemma 3.8: The product of two integers of the form $4n+1$ has the same form.

Proof: $a = 4n+1$, $b = 4m+1$

$$\Rightarrow ab = 16mn + 4n + 4m + 1$$
$$= 4(4mn+n+m)+1$$
$$= 4k+1 \text{ where } k = 4mn+n+m \in \mathbb{Z}^+.$$

We know that $\sqrt{2}$ is irrational. So are $\sqrt{3}$, $\sqrt{5}$, $\sqrt[3]{2}$, $\sqrt[5]{10}$ etc. We can prove a general result

Theorem 3.18: Let $\alpha \in \mathbb{R}$ be a root of the polynomial equation

$$x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0 = 0$$

where $c_i \in \mathbb{Z}$ for all i. Then, α is either an integer or an irrational number.

Proof: Suppose α is not an irrational number. We'll show that α is an integer.

Since α is not irrational, it is rational.

Then,

$$\alpha = \frac{a}{b} \text{ for some } a, b \in \mathbb{Z},\ b > 0.$$

Since α is a root of the given equation,

$$\left(\frac{a}{b}\right)^n + c_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + c_1\left(\frac{a}{b}\right) + c_0 = 0.$$

Multiply by b^n to get

$$a^n + c_{n-1}a^{n-1}b + \cdots + c_1 a b^{n-1} + c_0 b^n = 0.$$

Rearrange the terms to get

$$a^n = b\left(-c_{n-1}a^{n-1} + \cdots + c_1 a b^{n-2} + c_0 b^{n-1}\right)$$

$$\therefore\ b \mid a^n$$

Suppose $b \neq 1$. Then, $b > 1$ ($\because b \in \mathbb{Z}^+$)
Then, by the fundamental theorem of arithmetic, b has a prime factor p.

Then, $p \mid a^n$.

Now, by Lemma 3.5 with

$$a_1 = a_2 = \cdots = a_n = a,$$

we get

$$p \mid a.$$

Therefore, p is a prime factor of both a and b.

This is a contradiction because we can always choose a and b without prime factors.
Therefore, $b \neq 1$ is impossible,
Hence, $b = 1$.

$\therefore\ \alpha = \frac{a}{b}$ is an integer.

<u>ex</u>: $\sqrt{2}$ is irrational because it is a root of $x^2 - 2 = 0$ and no integer solutions exist.

Exercise: Why doesn't $x^2 - 2 = 0$ have integer solutions?