Chapter 3

3.1 Primes and Greatest Common Divisors

Definition: A prime is an integer greater than 1 that is divisible by no positive integers other than 1 and itself. An integer greater than 1 that is not a prime is called composite.

ex! 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, . . .

Lemma 3.1: Every integer greater than 1 has a prime divisor.

Proof: We use the method of contradiction. Suppose there is an integer greater than 1 that has no prime divisor. Let n be the smallest such integer. Then, since $n|n$ and n is not prime, n should be composite.

Then, $n = ab$ for some $a, b \in \mathbb{Z}^+$ with $1 < a, b < n$.

Since, for example, $a < n$, a should have a prime divisor ($\because$ n is the least n with no prime divisors).
Let k be a prime divisor of a.

Then, $k \mid a$ and $a \mid n$, so we get $k \mid n$ (Theorem 1.8).

This is a contradiction since we assumed that n has no prime divisors. Hence the result.

Theorem 3.1: There are infinitely many primes.

Proof: The proof is again by the method of contradiction.

Suppose there are finitely many primes.

Let them be $p_1, p_2, \cdots, p_n$.

Let $p = p_1 p_2 \cdots p_n + 1$

By Lemma 3.1, p has a prime divisor, say p_j (it should be one of p_i's).

Then, $p_j \mid p$ and $p_j \mid p_1 p_2 \cdots p_n$.

$\Rightarrow p_j \mid (p - p_1 p_2 \cdots p_n)$

$\Rightarrow p_j \mid 1$, a contradiction.

Hence, there are infinitely many primes.

* Let p_i be the ith prime. Then $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, ...

* $p_1 p_2 \cdots p_n + 1$ is not always a prime (Justify it!)

<u>Theorem 3.2:</u> If n is a composite integer then n has a prime factor less than or equal to $\sqrt{n}$.

Proof: Suppose n is composite.
Then, $n = ab$ for some $1 < a, b < n$.
Without loss of generality, assume $a \leq b$.

Then, $1 < a \leq b < n$.

Note that $a \leq \sqrt{n}$ because, otherwise, $b \geq a > \sqrt{n}$ and hence $ab > n$, a contradiction.

By Lemma 3.1, a has a prime divisor d and then by Theorem 1.8, d is a prime divisor of n, which is clearly less than or equal to $\sqrt{n}$.

Definition: $\pi(x)$ = number of primes less than or equal to x, $x \in \mathbb{R}^+$

ex: $\pi(1)=0$, $\pi(2)=1$, $\pi(3)=2$, $\pi(3.2)=2$

$\pi(5)=3$, $\pi(10)=4$

Theorem 3.3 (Dirichlet's Theorem on Primes in Arithmetic Progressions)

Let $\gcd(a,b)=1$ where $a,b \in \mathbb{Z}^+$.

Then, the arithmetic progression $(an+b)_{n=1}^{\infty}$ has infinitely many primes.

Proof: No simple proof is known. Will look at a proof if time permits.

* Some special cases of Theorem 3.3 can be proved fairly easily. For example, we can prove that there are infinitely many primes of the form $4n+3$.