Chapter 2

\[ \text{§2.1 Euclid's Division Lemma} \]

There exist integers \( m \) and \( r \) such that

\[ n = m \beta + r, \quad 0 \leq r < \beta \]

Proof. Consider multiples of \( \beta \):

\[ 0, \beta, 2\beta, \ldots \]

We can find \( m \) such that

\[ m\beta \leq n < (m+1)\beta. \]

Let \( r = n - m\beta \).

We get the desired conclusion.

We observe that \( r < \beta \).
§ 2.2 Divisibility

Def. If \( a \) and \( b \) (\( b \neq 0 \)) are integers, we say \( b \) divides \( a \) (or \( b \) is a divisor of \( a \) or \( a \) is divisible by \( b \)) if \( \frac{a}{b} \) is an integer.

We will write \( b | a \) to indicate \( b \) divides \( a \).

\[ b + a \quad \text{or} \quad b \text{ does not divide } a \]

Ex. \( 5 | 15 \), \( 6 \nmid 15 \).

Ex. If \( a \) is an integer, then \( 1 | a \) and \( -1 | a \).

Ex. If \( a \neq 0 \) is an integer, then \( a | 0 \).

Ex. If \( a|n \) and \( a|m \), \( c, d \) are integers,
then \( a | cn + dm \).
If \( d \) divides both \( a \) and \( b \), then \( d \) is called a common divisor of \( a \) and \( b \).

Def. \( d \) is called the greatest common divisor of \( a \) and \( b \).

(i) \( d > 0 \).

(ii) \( d \) is a common divisor of \( a \) and \( b \).

(iii) Each common divisor of \( a \) and \( b \) is also a divisor of \( d \).

In this case, we write \( d = \gcd(a, b) \).

**Thm 2.2** If \( a \) and \( b \) are integers, not both zero, then \( \gcd(a, b) \) exists and is unique.

**Ex.** Find \( \gcd(34, 527) \).

(c.m (a, b) = least common multiple of \( a, b \))

**Question:** Prove that \( \gcd(a, b) \cdot \operatorname{c.m}(a, b) = ab \).
The Fundamental Theorem of Arithmetic

Thm 2.3 For each integer \( n > 1 \), there exists a prime \( p_1 < p_2 < \ldots < p_k \) and \( x_1, x_2, \ldots, x_k \), such that

\[
n = p_1^{x_1} p_2^{x_2} \cdots p_k^{x_k},
\]

this factorization is unique.

Thm 2.4 If \( d = \gcd(a, b) \), then there exist integers \( x \) and \( y \) such that

\[
ax + by = d.
\]

Cor 2.5 In order that there exist integers \( x \) and \( y \) satisfying the equation \( ax + by = c \), it is necessary and sufficient that \( d \mid c \), where \( d = \gcd(a, b) \).

Def 2.6 If \( \gcd(a, b) = 1 \), then \( a, b \) are said to be relatively prime.

Thm 2.6 If \( a, b, c \) are integers where \( a \) and \( c \) are coprime, and \( \frac{c}{\gcd(a, b)} = \frac{a}{b} \) then \( \frac{b}{c} \).

Ex. \( \gcd(a, b) = d \) then \( \gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1 \).