Definition 1 (Division Algorithm)**.** Let m be an integer and n a positive integer. Then there exists unique integers q and r which satisfy the following equations:

1. $0 \leq r < n$.
2. $m = qn + r$.

Theorem 1 (Moduluarity and Division)**.**

$$a \equiv b \iff n \mid (b - a).$$

Theorem 2 (Modular Arithmetic)**.** Suppose that a, b, c, d are integers and that all congruences are modulo n. Then

1. $a \equiv b$ and $c \equiv d \implies ac \equiv bd$
2. $a \equiv b$ and $c \equiv d \implies a \pm c \equiv b \pm d$

Theorem 3 (Modular Division)**.**

$$ka \equiv kb \pmod{kn} \implies a \equiv b \pmod{n}.$$

Definition 2 (Injectivity and Surjectivity)**.** Let f be a function such that $f : A \to B$. f is injective if

$$\forall a_1, a_2 \in A, f(a_1) = f(a_2) \implies a_1 = a_2.$$

f is surjective if

$$\forall b \in B, \exists a \in A, f(a) = b.$$