

# Linear Congruence Class Theory

**Definition** (Congruence Classes). A congruence class  $[a]_n$  is the set of all integers that have the same remainder as  $a$  when divided by  $n$ .

**Theorem** (Congruence class alternative). Given a congruence class  $[a]_n$  defined as above,  $[a]_n = \{x : n|x - a\}$ .

**Axiom** (Congruence arithmetic). Equality, addition, subtraction, and multiplication of congruence classes obeys the same arithmetic rules as integer arithmetic.

**Definition.** A pair of congruence classes  $[a]_n$  and  $[b]_n$  are zero-divisor's if and only if  $[a]_n \neq [0]_n$ ,  $[b]_n \neq [0]_n$ , and  $[a]_n[b]_n = [0]_n$ .

**Definition.** A pair of congruence classes  $[a]_n$  and  $[b]_n$  are inverses of each-other if and only if  $[a]_n[b]_n = [1]_n$ . A congruence class with an inverse is called "invertible".

**Theorem.** If a congruence class is invertible, then it has only one inverse, which we represent with  $[a]_n^{-1}$ .

**Theorem.** If a congruence class is invertible, then it is not a zero-divisor.

**Theorem.** Every congruence class  $[a]_n$  is either equal to  $[0]_n$ , invertible, or a zero-divisor.

**Theorem.** If  $n$  is prime and  $n \nmid a$ , then  $[a]_n$  is invertible.

**Theorem.** If  $n$  and  $a$  are not relatively prime, then  $[a]_n$  is a zero-divisor.

**Theorem.** If  $n$  and  $a$  are relatively prime, then  $[a]_n$  is invertible.

**Theorem.** If  $\gcd(n, a) = 1$ ,  $[a]_n^{-1} = [r]_n$ , where  $ar + ns = 1$  for some integer  $s$ .

**Definition.** Two integers are congruent, modulo some positive integer base  $n$  if and only if they have the same remainder when divided by  $n$ . Symbolically,  $x \equiv_n y$  if and only if  $x \% n = y \% n$ .

**Theorem.**  $x \equiv_n y$  if and only if  $n|x - y$ .

**Theorem.** For any positive integer  $k$ ,  $ax \equiv_n b$  if and only if  $(ka)x \equiv_{(kn)} (kb)$ .

**Theorem** (Fundamental theorem of linear congruences). Take a linear congruence  $ax \equiv_n b$ , where all  $a$ ,  $x$ ,  $b$ , and  $n$  are integers and  $n > 1$ . If  $\gcd(n, a) \nmid b$ , then there are no solutions to this equation ( $x \in \emptyset$ ). But if  $\gcd(n, a) | b$ , then  $x \in [a']_n^{-1}[b']_n$ , where  $a' = a/\gcd(a, n)$ , where  $b' = b/\gcd(a, n)$ , and  $n' = n/\gcd(a, n)$ .