MATH 433

Applied Algebra

Lecture 5:
Chinese remainder theorem.
Fermat's little theorem.
Euler's theorem.

Congruence classes

Given an integer a, the **congruence class of** a **modulo** n is the set of all integers congruent to a modulo n: $[a]_n = \{a + nk : k \in \mathbb{Z}\}$.

The set of all congruence classes modulo n is denoted $\mathbb{Z}_n$.

The arithmetic operations on $\mathbb{Z}_n$ are defined as follows. For any integers a and b, we let

$$[a]_n + [b]_n = [a + b]_n,$$
$$[a]_n - [b]_n = [a - b]_n,$$
$$[a]_n \times [b]_n = [ab]_n.$$

Invertible congruence classes

We say that a congruence class $[a]_n$ is **invertible** (or the integer a is **invertible modulo** n) if there exists a congruence class $[b]_n$ such that $[a]_n[b]_n = [1]_n$. If this is the case, then $[b]_n$ is called the **inverse** of $[a]_n$ and denoted $[a]_n^{-1}$.

Theorem A nonzero congruence class $[a]_n$ is invertible if and only if $\gcd(a, n) = 1$.

The set of all invertible congruence classes in $\mathbb{Z}_n$ is denoted G_n or $\mathbb{Z}_n^*$. This set is closed under multiplication.