

Math 310 Chapter 7 Review

Congruences

1. Let $n \in \mathbb{N}$. We say that a is congruence to b modulo n if $n \mid (b - a)$. That is, a and b have the same remainder when divided by n . And we write

$$a \equiv b \pmod{n}.$$

2. We can add, subtract or multiply congruences. That is, if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then

$$a + c \equiv b + d \pmod{n} \quad \text{and} \quad ac \equiv bd \pmod{n}.$$

3. The set of all elements congruent to x modulo n is call the *congruence class containing x* and is denoted \bar{x} . The set of all congruences class modulo n is denoted $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$.
4. Since the set of congruence classes \mathbb{Z}_n is finite, you should know that addition and multiplication can be summarized in tables.
5. The additive identity, additive inverse, and multiplicative identity always exist. In particular, if we want to solve $x + a \equiv b \pmod{n}$, then we are guaranteed that the additive inverse of a , called $-a$ (or $n - a$), exists and we are allowed to write $x \equiv b - a \pmod{n}$.
6. The multiplicative inverse is NOT always guaranteed to exist. We proved the following result:
If $\gcd(a, n) = 1$, then the multiplicative inverse of \bar{a} exists in \mathbb{Z}_n .
That is, if $\gcd(a, n) = 1$, then $ax \equiv 1 \pmod{n}$ has a solution $x \equiv a^{-1} \pmod{n}$. In addition, we can use this to solve, *i.e.* if $\gcd(a, n) = 1$, then $ax \equiv b \pmod{n}$ has a solution $x \equiv a^{-1}b \pmod{n}$.
7. If p is a prime, then every nonzero element in \mathbb{Z}_p has an inverse.