Math 300 Chapter 7 Review

Congruences

1. Please review the solutions to HW 5a. They should really help you understand what is allowed when working with congruences.

2. 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

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

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

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

4. The set of all elements congruent to x modulo n is called the *congruence class containing x* and is denoted $\bar{x}$. The set of all congruences class modulo n is denoted $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$.

5. Since size of the set $\mathbb{Z}_n$ is equal to n and every integer must be in one of the n congruences classes.

6. 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 $x \equiv b - a \pmod{n}$.

7. 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 $x \equiv a^{-1}b \pmod{n}$.

8. If p is a prime, then every nonzero element in $\mathbb{Z}_p$ has an inverse.

9. If p is a prime and a is any integer, then $a^p \equiv a \pmod{p}$. (this is Fermat's Little Theorem, which you proved in HW 6.37). If in addition, $\gcd(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$.