Remember long division and finding remainders? It's going to be important for us...

Definition:

The ____________ of two integers n and m is found by division of n by m and is the number of times m can fully "go into" n. (Division by $m = 0$ is not defined.) The __________________ is an integer value r, where $0 \leq r < |m|$ that is "leftover" when n is divided by m. If the remainder of the division of n by m is 0, then n is __________________ m or m ____________ n. Using the _____________________, we can write n in terms of m, its quotient, and remainder: $n = qm+r$, where $0 \leq r < |m|$.

Note: the "division algorithm" is not an algorithm in the way we will normally talk about algorithms in this class. Rather than giving us a procedure to follow (which is what we normally mean by an algorithm), it gives us an existence proof of the fact that we can always write a number in this format.

Example: Suppose you want to divide n by m. Find the quotient and remainder for the given n and m. Use the division algorithm to write n in terms of m, the quotient, and the remainder.

(a) $n = 15$, $m = 7$

(b) $n = 67$, $m = 5$

(c) $n = 78$, $m = 3$

(d) $n = -72$, $m = 13$

(e) $n = -85$, $m = -9$

In this chapter we will often be just as (if not more) interested in the remainder than the quotient. In particular:

Definition:

Let m be an integer greater than 1. If x and y are integers, we say that x is ____________ to y ____________ m if $x - y$ is divisible by m. If x is congruent to y modulo m, we write ____________; otherwise, we write ____________. We call this relation on the set of integers ___________________.

Example: Find two (or more) integers that are congruent to each other modulo m for each modulus in (a)-(d).

(a) $n = 15$, $m = 7$

(b) $n = 67$, $m = 5$

(c) $n = 78$, $m = 3$

(d) $n = -72$, $m = 13$

Example: We skipped the prior (e) as an example. Why should we have done so?

Example: Determine whether $p \equiv q \pmod{m}$:

(a) $p = 15$, $q = 29$, $m = 7$

(b) $p = 94$, $q = -22$, $m = 5$

(c) $p = -14$, $q = 37$, $m = 3$

Theorem 3.1:

Congruence modulo m is an equivalence relation.

Definition:

The equivalence classes for congruence modulo m are called _________________________ modulo m. The set of all congruence classes modulo m will be denoted $\mathbb{Z}_m$ (or Z_m).

Example: Determine the distinct congruence classes in $\mathbb{Z}_4$.

Example: Determine the distinct congruence classes in $\mathbb{Z}_7$.

Example: Determine which congruence class of $\mathbb{Z}_m$ p and q are in for each example and relate this to congruence (or lack of congruence) mod m.

(a) $p = 15$, $q = 29$, $m = 7$

(b) $p = 94$, $q = -22$, $m = 5$

(c) $p = -14$, $q = 37$, $m = 3$

Theorem 3.2

If $x \equiv x' \pmod{m}$ and $y \equiv y' \pmod{m}$, then

(a) $x + y \equiv x' + y' \pmod{m}$ and

(b) $xy \equiv x'y' \pmod{m}$.

Implication:

Based on Theorem 3.2, we can safely define addition and multiplication in $\mathbb{Z}_m$ as follows:

$[x] + [y] = [x + y]$ and $[x]\,[y] = [xy]$.