Remember long division and finding remainders? It's going to be important for us... $\frac{n}{m}$

Definition:

The quotient 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 remainder is an integer value r, where $\boxed{0 \leq r < |m|}$ that is "leftover" when n is divided by m. If the remainder of the division of n by m is 0, then n is divisible by m or m divides n. Using the division algorithm, we can write n in terms of m, its quotient, and remainder: $\boxed{n = qm+r}$, where $0 \leq r < |m|$. $\frac{n}{m}$

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. $\frac{n}{m}$

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

$15 \div 7 = 2$, $15 - 14 = 1$

$q = 2$ $r = 1$

$\boxed{15 = 7(2) + 1}$

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

$67 \div 5 = 13$, $67 - 65 = 2$

$q = 13$ $r = 2$

$\boxed{67 = 5(13) + 2}$

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

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

~~$-72 \div 13 = -5$, $-72 - (-65) = -7 < 0$~~

$-72 \div 13 = -6$, $-72 - (-78) = 6$

$-72 = \boxed{13(-6) + 6}$

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

$-85 = -9(10) + 5$

~~$-85 \div (-9) = 9$, $-85 - (-81) = -4$~~

$-85 \div (-9) = 10$, $-85 - (-90) = +5$

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

$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$

Definition:

Let m be an integer greater than 1. If x and y are integers, we say that x is congruent to y modulo m if $x - y$ is divisible by m. If x is congruent to y modulo m, we write $x \equiv y \pmod{m}$; otherwise, we write $x \not\equiv y \pmod{m}$. We call this relation on the set of integers congruence modulo m.

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

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

$x = 15 \quad m = 7$

$\boxed{y = 1, 8}$

$\frac{15 - 1}{7} = \frac{14}{7} = 2$

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

$x = 67 \quad m = 5$

$\boxed{y = 2, 52,}$

homework

(c) $n = 78$, $m = 3$ 0

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

$\frac{29 - 15}{7}$ $\quad 29 \equiv 15 \pmod{7}$

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

$94 \not\equiv -22 \pmod{5}$ $\quad \frac{94 - (-22)}{5} = \frac{116}{5}$

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

$\frac{37 - (-14)}{3} = \frac{51}{3} = 17 \quad 37 \equiv -14 \pmod{3}$

Theorem 3.1:

Congruence modulo m is an equivalence relation.

Definition:

The equivalence classes for congruence modulo m are called congruence classes 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 $\mathbb{Z}_4$.

$[0] = [4] = \{\dots, -8, -4, 0, 4, 8, \dots\}$

$[1] = \{\dots, -7, -3, 1, 5, 9, \dots\}$

$[2] = \{\dots, -6, -2, 2, 6, 10, \dots\}$

$[3] = \{\dots, -5, -1, 3, 7, 11, \dots\}$

$\mathbb{Z}_5$

$\mathbb{Z}_{10}$

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

$[0] = \{\dots, -7, 0, 7, 14, \dots\}$

$[1] = \{\dots, -6, 1, 8, 15, \dots\}$

$[2] = \{\dots, -5, 2, 9, 16, \dots\}$

$[3] = \{\dots, -4, 3, 10, 17, \dots\}$

$[4] = \{\dots, -3, 4, 11, 18, \dots\}$

$[5] = \{\dots, -2, 5, 12, 19, \dots\}$

$[6] = \{\dots, -1, 6, 13, 20, \dots\}$

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

$[1]$ $[1]$

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

$[4]$ $[3]$

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

$[1]$ $[1]$

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