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

Definition:

(absolute value of m)

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 $0 \le r < |m|$ 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: $n = qm+r$, where $0 \le r < |m|$.

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

$7 \overline{)15}$ = 2 r. 1; -14; 1

$\boxed{\text{quotient}(q) = 2 \quad \text{remainder}(r) = 1 \quad 15 = 2(7)+1}$

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

$5\overline{)67}$ = 13 r. 2; -5; 17; -15; 2

$\boxed{q = 13,\ r = 2 \quad 67 = 13(5)+2}$

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

$3\overline{)78}$ = 26 r. 0; -6; 18; -18; 0

$\boxed{q = 26,\ r = 0 \quad 78 = 26(3)+0}$

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

$13\overline{)-72}$ = -5 r. -7; $+65$; -7 — neg. remainder – not good

$13\overline{)-72}$ = -6 r. 6; $+78$; 6

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

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

$-9\overline{)-85}$ = 10 r. 5; $+90$; 5

$\boxed{-85 = 10(-9)+5 \quad q = 10,\ r = 5}$

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

Definition: $\{3, 4, \ldots$

> 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) $n = 15$, $m = 7$ $15 \div 7 = 2 \text{ r. } 1$ 15 & 1 are congruent $\Rightarrow 15 \equiv 1 \pmod{7}$

$1 \div 7 = 0 \text{ r. } 1$ $15 - 1 = 14$ $14 \div 7 = 2 \text{ r. } 0$ $22 \equiv 15 \equiv 8 \equiv 1 \pmod{7}$

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

$67 - 2 = 65$ $65 \div 5 = 13 \text{ r. } 0$ so $67 \equiv 2 \pmod{5}$ $5\overline{)2}$ 0 r. 2 $5\overline{)67}$ 13 r. 2

$67 \equiv 12 \pmod{5}$

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

$78 \equiv 0 \pmod{3}$ $78 \div 3 = 26 \text{ r. } 0$

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

$-72 \equiv 6 \pmod{13}$ $-72 - 6 = -78$ $-78 \div 13 = -6 \text{ r. } 0$

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

$-9 < 1$ – we don't use negative moduli

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

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

$29 - 15 = 14$ 14 is divisible by 7 $\Rightarrow 29 \equiv 15 \pmod{7}$

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

$94 + 22 = 116$ does not end in 0 or 5 so not divisible by 5 so $94 \not\equiv -22 \pmod{5}$

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

$37 + 14 = 51$ $3\overline{)51}$ 17 r. 0 divisible $\Rightarrow -14 \equiv 37 \pmod{3}$

Theorem 3.1:

> Congruence modulo m is an equivalence relation.

Definition: conveys a type of sameness (here, same remainder under division by m)

> 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 $\mathbb{Z}_4$.

$[0] = [4] = \{\ldots, -8, -4, 0, 4, 8, \ldots\}$ each class is a set

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

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

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

We usually use remainders as the representative to characterize the set, but we could choose others.

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

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

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

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

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

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

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

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

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

$[1]$ $[1]$

$[1] = [1] \Rightarrow$ same congruence class so congruent

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

$[4]$ $[3]$

$[4] \neq [3] \Rightarrow$ not congruent

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

$[1]$ $[1]$

$\Rightarrow$ congruent

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

Example: For each of the following, use a representative r such that $0 \le r < m$ to characterize the result in $\mathbb{Z}_m$.

0 & 11 inclusive   1 r. 4 $12\overline{)16}$

(a) Find $[9] + [7]$ in $\mathbb{Z}_{12}$.

$[9]+[7] = [9+7] = [16] = [4]$

(b) Find $[13] + [8]$ in $\mathbb{Z}_8$. ~ goal between 0 & 7 inclusive

$[13]=[5]$ $[8]=[0]$ $[13]+[8] \equiv [5]+[0] = [5]$

(c) Find $[111] + [57]$ in $\mathbb{Z}_{112}$.

$[111] \equiv [-1]$ $[111]+[57] = [-1]+[57] = [56]$

OR $[111]+[57] = [168] = [56]$ number between 0 & 111 inclusive

$168 - 112 = 56$

(d) Find $[999] + [402]$ in $\mathbb{Z}_{60}$.

$[999]=[39]$ $[402]=[42]$ $[39]+[42]=[81]=[21]$ between 0 & 59

(e) Find $[9]\,[7]$ in $\mathbb{Z}_{12}$.

$[9][7] = [63] \equiv 3 \bmod 12$ $= \boxed{[3] \text{ in } \mathbb{Z}_{12}}$ 5 r. 3 $12\overline{)63}$, -60, 3

(f) Find $[13]\,[8]$ in $\mathbb{Z}_8$.

$= [5][0] = \boxed{[0] \text{ in } \mathbb{Z}_8}$ $[13]=[5]$ $[8]=[0]$

(g) Find $[111]\,[57]$ in $\mathbb{Z}_{112}$.

$= [-1][57] = [-57] = \boxed{[55] \text{ in } \mathbb{Z}_{112}}$ $112 - 57 = 55$ $-57+112=$

(h) Find $[999]\,[402]$ in $\mathbb{Z}_{60}$.

$= [39][42] = [1638] = [138] = \boxed{[18] \text{ in } \mathbb{Z}_{60}}$ $(1500 \div 60 = 25)$

OR $1638 \div 60 = 27.3$ $60(27) = 1620$ $1620 + 18 = 1638$

(i) Find $[5]^{20}$ in $\mathbb{Z}_4$.

$[1]^{20} = [1]$ $5 \equiv 1 \pmod 4$ aka $[1] = \{\ldots, -3, 1, 5, 9, \ldots\}$

(j) Find $[12]^5$ in $\mathbb{Z}_{13}$. $12-13=-1$

$[-1]^5 = [-1]$ $[12] = \{\ldots, -14, -1, 12, 25, 38, \ldots\}$

(k) Find $[26]^{59}$ in $\mathbb{Z}_{13}$.

$26-13=13$ $13-13=0$ so $[26]=[0]$ & $[26]^{59} = [0]^{59} = \boxed{[0] \text{ in } \mathbb{Z}_{13}}$

(l) Find $[23]^{18}$ in $\mathbb{Z}_{25}$.

$[23]=[-2]$ so $[23]^{18} = [-2]^{18} = [262144] = [19]$

$262144/25 = 10485.76$ so $25(10485) = 262125$ $262144 - 262125 = 19$

Example: Let A denote the equivalence class containing 5 in $\mathbb{Z}_8$ and B denote the congruence class (equivalence class) containing 5 in $\mathbb{Z}_{12}$. Is $A = B$? Why or why not?

$[5]$ in $\mathbb{Z}_8$ is $\{\ldots, -3, 5, 13, \ldots\}$ No - different sets

$[5]$ in $\mathbb{Z}_{12}$ is $\{\ldots, -7, 5, 17, \ldots\}$