Lecture 2 Note Thursday, 02/03/2022

## Announcement

- For students who haven't attend the first two classes, make sure you attend at least one of the first five in-person classes to avoid the WN grade and being withdrawn by the registrar.
- The Lecture Recordings will be available on the following YouTube Playlists Link: https://youtube.com/playlist?list=PLZaTmV9UMKliRBuEs0-dL968iQgE0qwpc

## The Division Algorithm

- Let $a$ be an integer and d a positive integer. Then there are unique integers $q$ and $r$, with $0 \leq r < d$, such that $a = dq + r$.

## Examples of Division Algorithm

- Let $a = 23$ and $d = 7$. Find $q$ and $r$.
  $23 = 7(3) + (2)$, $0 \leq 2 < 7$. So $q = 3$ and $r = 2$.
- Let $a = -23$ and $d = 7$. Find $q$ and $r$.
  We want $-23 = 7q + r$. If we just negate the $q$ and $r$ from the previous question, we get $-23 = 7(-3) + (-2)$. The equation will hold but $0 \nleq -2$.
  We want to make the $r$ bigger so it's not negative and less than $7$.
  To do so, we need to make the $q$ smaller, which $-23 = 7(-4) + (5)$.
  Now we have $0 \leq 5 < 7$, then $q = -4$ and $r = 5$.

## The Division Algorithm

- In the equality given in the division algorithm, $d$ is called the *divisor*, $a$ is called the *dividend*, $q$ is called the *quotient*, and $r$ is called the *remainder*. This notation is used to express the quotient and remainder:
  $q = a \,\mathbf{div}\, d$, $r = a \,\mathbf{mod}\, d$.

## Examples of Division Algorithm

- Find $-220 \,\mathbf{div}\, 100$ and $-220 \,\mathbf{mod}\, 100$.
  $-220 \,\mathbf{div}\, 100$ represent the quotient ($q$) of $-220$ divided by $100$, and
  $-220 \,\mathbf{mod}\, 100$ represent the remainder ($r$) of $-220$ divided by $100$.
  We can put them in the division algorithm form, which we want
  $-220 = 100q + r$. $-220 = 100(-3) + (80)$, so $-220 \,\mathbf{div}\, 100 = -3$ and $-220 \,\mathbf{mod}\, 100 = 80$.
  $-220 \,\mathbf{div}\, 100$ cannot be $-2$, if it does, then we will have $-220 = 100(-2) + (-20)$.
  But $r$, $-220 \,\mathbf{mod}\, 100$, cannot be negative.

## Definition of Congruence and Modulus

- If $a$ and $b$ are integers and $m$ is a positive integer, then $a$ is congruent to $b$ modulo $m$ if $m$ divides $a - b$. We use the notation $a \equiv b (mod\, m)$ to indicate that $a$ is congruent to $b$ modulo $m$. We say that $a \equiv b \,(mod\, m)$ is a **congruence** and that $m$ is its **modulus** (plural **moduli**). If $a$ and $b$ are not congruent modulo $m$, we write $a \not\equiv b \,(mod\, m)$.
  - $a \equiv b \,(mod\, m) \leftrightarrow m|(a - b)$

## Examples of Congruence and Modulus

- Determine whether $17 \equiv 8 \,(\mathrm{mod}\, 3)$.
  True, since $3|(17 - 8) \rightarrow 3|9$ √
- Determine whether $7 \equiv 8 \,(\mathrm{mod}\, 3)$.
  False, since $3 \nmid (7 - 8) \rightarrow 3 \nmid (-1)$ .
- Determine whether $-7 \equiv 8 \,(\mathrm{mod}\, 3)$.
  True, since $3|(-7 - 8) \rightarrow 3|(-15)$ √

Deference between $a \bmod m$ and $a \pmod m$

- In "$a \bmod m$", **mod** is an operation that solves the remainder of $a$ divided by $m$, so $a \bmod m$ will equals to a nonnegative integer that less than $m$.
  - Example: $5 \bmod 3 = 2$.
- In "$a \pmod m$", mod is a relation on the set of integers. $a \pmod m$ is a set of integers that have the same remainder when divides by $m$.
  - Example: $5 \pmod 3$ does not just represent $2$. It represents all the numbers that congruent to $5 \pmod 3$, i.e., $2$, $8$, $14$, etc.

Congruence Classes and LNR

- The congruence class of $a$ modulo $m$, denoted $a \pmod m$, is the set of all integers that are congruent to $a$ modulo $m$.
- The LNR (least Nonnegative Residue) of a modulo is the smallest nonnegative value in its congruence class.
  - Let's list out all the congruence classes modulo 5.

$$\cdots \equiv -10 \equiv -5 \equiv 0 \pmod 5 \equiv 5 \equiv 10 \equiv 15 \equiv \cdots$$
$$\cdots \equiv -9 \equiv -4 \equiv 1 \pmod 5 \equiv 6 \equiv 11 \equiv 16 \equiv \cdots$$
$$\cdots \equiv -8 \equiv -3 \equiv 2 \pmod 5 \equiv 7 \equiv 12 \equiv 17 \equiv \cdots$$
$$\cdots \equiv -7 \equiv -2 \equiv 3 \pmod 5 \equiv 8 \equiv 13 \equiv 18 \equiv \cdots$$
$$\cdots \equiv -6 \equiv -1 \equiv 4 \pmod 5 \equiv 9 \equiv 14 \equiv 19 \equiv \cdots$$

    - The numbers in each row belong to the same congruence class modulo $5$.
    - We can also see that the numbers in the same row have the same remainder when divided by $5$.
    - If you pick any two numbers in the same row, the different between them will be multiple of $5$.
    - From this, we can see that to generate another number in the same congruent class, we can add or subtract any multiple of the modulo.
    - $0, 1, 2, 3, 4$ are the LNR form of the modulo $5$, it's the same range as the remainders.
    - You can think the LNR form as the simplest/reduced form in fraction. For example, $\frac{2}{4} = \frac{3}{6} = \frac{5}{10} = \frac{100}{200} = \frac{123}{246} = \frac{1}{2}$ all those fractions have the same value, but different fraction forms. All those fractions can be reduced to $\frac{1}{2}$. So, in the congruence class of $3 \pmod 5$, we have $\{\ldots, -7, -2, 3, 8, 13, 18, \ldots\}$ that all congruent to each other, they can be treat the same under the modulo. To have one represented number for the set of numbers (congruence), we will choose the least nonnegative reduce form to represent the congruence.

Examples of Congruence and Modulus

- Find
  - $13 \bmod 7$. $= 6$
  - $13 \pmod 7$. $\equiv 6 \pmod 7$
  - $-13 \bmod 7$. $= 1$
  - $-13 \pmod 7$. $\equiv 1 \pmod 7$

- Find the LNR of $2022 \pmod{21}$.
  The LNR form of $2022 \pmod{21}$ will be in between 0 and 20. We know that to find another number that congruent to $2022 \pmod{21}$ we can keep adding or subtracting multiple of 21 the number until you get the number into the range you want it to be.
  $2022 - 2100 = -78 \rightarrow -78 + 84 = 6$, thus, $2022 \equiv 6 \pmod{21}$.

- Find the LNR of $37485 \pmod{22}$.
  $37485 - 4400 = -6515 \longrightarrow -6515 + 6600 = 85 \longrightarrow 85 - 66 = 19$, $37485 \equiv 19 \pmod{22}$.

- Find an integer that between 100 and 140 that congruent to $22 \pmod{41}$.
  $22 + 82 = 104,\ 22 \equiv 104 \pmod{41}$

- Find an integer that between -140 and -100 that congruent to $22 \pmod{41}$.
  $22 - 123 = -101,\ 22 \equiv -101 \pmod{41}$

Theorems
- Let $a$ and $b$ be integers, and let $m$ be a positive integer.
  Then $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$.
- Let $m$ be a positive integer. The integers $a$ and $b$ are congruent modulo $m$ if and only if there is an integer $k$ such that $a = b + km$.

Theorem
- Let $m$ be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.
  - Proof: We use a direct proof. Because $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, by the previous theorem there are integers $s$ and $t$ with $b = a + sm$ and $d = c + tm$. Hence, $b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$ and $bd = (a + sm)(c + tm) = ac + m(at + cs + stm)$.
    Hence, $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

Corollary
- Let $m$ be a positive integer and let $a$ and $b$ be integers. Then
  $(a + b) \bmod m = \big((a \bmod m) + (b \bmod m)\big) \bmod m$
  and
  $ab \bmod m = \big((a \bmod m)(b \bmod m)\big) \bmod m$.

Examples
- Find the LNR of $37485 + 467 \pmod{22}$.
  In the previous exercise we showed that $37485 \equiv 19 \pmod{22}$.
  And $467 - 440 = 27 \to 27 - 22 = 5,\ 467 \equiv 5 \pmod{22}$. Then,
  $37485 + 467 = 19 + 5 \equiv 24 \equiv 2 \pmod{22}$.

- Find the LNR of $37485 \cdot 467 \pmod{22}$.
  $37485 \cdot 467 \equiv 19 \cdot 5 \equiv 95 \equiv 7 \pmod{22}$.
  Or $37485 \cdot 467 \equiv 19 \cdot 5 \equiv (-3) \cdot 5 \equiv -15 \equiv 7 \pmod{22}$.

What to expect or prepare for the next class:
- Integer representation and divisibility rules
- Prime and composite (if we have time)

Suggested Problems (You don't need to hand in.)
- Discrete Mathematics and its Application 4.1 # 13,14,17,26-39
- zyBook Additional Exercises #1.1.3-6, 1.2.1