CSCI 220 | Spring 2022

Discrete Structure

Divisibility and Modular Arithmetic

Discrete Mathematics and its Application

Section 4.1

Division

Which of following are representing "a divides b"?

1) a/b
2) b/a
3) $a|b$
4) $b|a$
5) a is a multiple of b.
6) b is a multiple of a.

$a | b$

$2 | 4$

$2/4 = \frac{1}{2} = 0.5$

$4/2 = 2$

Division

$a \mid b$ if $\exists\, c \in \mathbb{Z} : b = ac$

- If a and b are integers with $a \neq 0$, we say that a divides b if there is an integer c such that $b = ac$ (or equivalently, if $\frac{b}{a}$ is an integer).
  When a divides b we say that a is a factor or divisor of b, and that b is a multiple of a. The notation $a \mid b$ denotes that a divides b.
  We write $a \nmid b$ when a does not divide b.

Examples of Division

$a|b$ when $b/a \in \mathbb{Z}$.

- Determine whether $7|25$.

$25 = 7 \cdot c$

No

$c = \frac{25}{7} \notin \mathbb{Z}$

- Determine whether $7|35$.

Yes

$35 = 7 \cdot 5$

c

Theorem

Try : $a|b$, $a|c \rightarrow a|(b-c)$

- Let a, b, and c be integers, where $a \neq 0$. Then
  - (i) if $a \mid b$ and $a \mid c$, then $a \mid (b+c)$;
  - (ii) if $a \mid b$, then $a \mid bc$ for all integers c;
  - (iii) if $a \mid b$ and $b \mid c$, then $a \mid c$.

$3|12$, $3|15 \rightarrow 3|12+15$

$3|27$ ✓

belongs to

set of integers

Pf (i) : $a|b$, $a|c$ $\rightarrow$ $\exists k \in \mathbb{Z} : b = ak$, $\exists s \in \mathbb{Z} : c = a \cdot s$ $\rightarrow$ $b+c = ak + a \cdot s$

$b+c = a(\underbrace{k+s}_{\in \mathbb{Z}})$

there exists

$\rightarrow a | b+c$

Theorem

- Let a, b, and c be integers, where $a \neq 0$. Then
  - (i) if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;
  - (ii) if $a \mid b$, then $a \mid bc$ for all integers c;
  - (iii) if $a \mid b$ and $b \mid c$, then $a \mid c$.

$3 \mid 12 \rightarrow 3 \mid 12 \cdot 4 \rightarrow 3 \mid 48$ ✓

Pf ii) $a \mid b \rightarrow \exists k \in \mathbb{Z} : b = a \cdot k$

$bc = (ak) \cdot c$

$bc = a \underbrace{(k \cdot c)}_{\in \mathbb{Z}.} \rightarrow a \mid bc$ ⊞

Theorem

- Let a, b, and c be integers, where $a \neq 0$. Then
  - (i) if $a \mid b$ and $a \mid c$, then $a \mid (b+c)$;
  - (ii) if $a \mid b$, then $a \mid bc$ for all integers c;
  - (iii) if $a \mid b$ and $b \mid c$, then $a \mid c$.

$3 \mid 12$, $12 \mid 48 \rightarrow 3 \mid 48$

Pf iii) $a \mid b \rightarrow \exists k \in \mathbb{Z} : b = a \cdot k \rightarrow c = \underset{ak}{b} \cdot s$

$b \mid c \qquad \exists s \in \mathbb{Z} : c = b \cdot s$

$c = (a k) s$

$c = a(\underbrace{k \cdot s}_{\in \mathbb{Z}})$

$\rightarrow a \mid c$ ■.

Corollary

- Let a, b, and c be integers, where $a \neq 0$. Then
  - (i) if $a \mid b$ and $a \mid c$, then $a \mid (b+c)$;
  - (ii) if $a \mid b$, then $a \mid bc$ for all integers c;
  - (iii) if $a \mid b$ and $b \mid c$, then $a \mid c$.
- If a, b, and c are integers, where $a \neq 0$, such that $a \mid b$ and $a \mid c$, then $a \mid mb + nc$ whenever m and n are integers.

$$\begin{matrix} a \mid b \\ a \mid c \end{matrix} \xrightarrow{\text{by (ii)}} \begin{matrix} a \mid mb \\ a \mid nc \end{matrix} \xrightarrow{\text{by (i)}} a \mid mb + nc$$

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.

$a = dq + r, \quad 0 \leq r < d$

$23 = 7(3) + (2) \quad 0 \leq 2 < 7$

$23 = 21 + 2$

- Let $a = -23$ and $d = 7$. Find q and r.

$-23 = 7(-3) + \cancel{(-2)}$

$-21 + -2$

$-2 < 0 \quad 0 \leq r < d.$

$-23 = 7(-4) + 5 \quad 0 \leq 5 < 7$

-28

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 $a = dq + r$.

- 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:

  $q = a \ \mathbf{div}\ d, \quad r = a \ \mathbf{mod}\ d.$

Examples of Division Algorithm

- Find $-220 \textbf{ div } 100$ and $-220 \textbf{ mod } 100$.

$q \uparrow$ -3

$r \uparrow$ 80

$a = dq + r$

$-220 = 100(-2) + (-20)$

$-220 = 100(-3) + 80$

$0 \leq 80 < 100$

-300

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 $a \not\equiv b\ (mod\ m)$.

$$a \equiv b \pmod{m} \quad \longleftrightarrow \quad m \mid a - b$$

Examples of Congruence and Modulus

- Determine whether $17 \equiv 8 \pmod{3}$.

True. $3 \mid 17-8 \rightarrow 3 \mid 9$ ✓

- Determine whether $7 \equiv 8 \pmod{3}$.

False $3 \mid 7-8 \rightarrow 3 \mid -1$ ✗

- Determine whether $-7 \equiv 8 \pmod{3}$.

True. $3 \mid -7-8 \rightarrow 3 \mid -15$ ✓

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.

$5 \bmod 3 = 2$

- 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.

$5 \pmod{3} \equiv 2 \equiv 8 \equiv 14$

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.

(mod 5)

$\cdots \equiv -10 \equiv -5 \equiv 0 \pmod 5 \equiv 5 \equiv 10 \equiv \cdots$

$\cdots \equiv -9 \equiv -4 \equiv 1 \pmod 5 \equiv 6 \equiv 11 \equiv \cdots$

$\cdots \equiv -8 \equiv -3 \equiv 2 \pmod 5 \equiv 7 \equiv 12 \equiv \cdots$

$\cdots \equiv -7 \equiv -2 \equiv 3 \pmod 5 \equiv 8 \equiv 13 \equiv \cdots$

$\cdots \equiv -6 \equiv -1 \equiv 4 \pmod 5 \equiv 9 \equiv 14 \equiv \cdots$

Examples of Congruence and Modulus

- Find
  - $13\ \boldsymbol{mod}\ 7$. $= 6$
  - $13 \pmod 7$. $\equiv 6 \pmod 7$
  - $-13\ \boldsymbol{mod}\ 7$. $= 1$
  - $-13 \pmod 7$. $\equiv 1 \pmod 7$

$\frac{2}{4} = \frac{100}{200} = \frac{222}{444} = \frac{15}{30} = \frac{1}{2}$

$\{ \ldots, -8, -1, 6, 13, 20, 27, \ldots \}$

$6 + 7k, \quad k \in \mathbb{Z}.$

Examples of Congruence and Modulus

- Find the LNR of $2022 \pmod{21}$.

$$
\begin{array}{r}
2022 \\
-2100 \\
\hline
-\ 78 \\
+\ 84 \\
\hline
6
\end{array}
$$

$2022 \equiv 6 \pmod{21}$

LNR

Examples of Congruence and Modulus

- Find the LNR of $37485 \pmod{22}$.

$$37485 \pmod{22} \equiv \boxed{19 \pmod{22}}$$

$$\begin{array}{r} 37485 \\ -22000 \\ \hline 15485 \\ -22000 \\ \hline -6515 \\ +6600 \\ \hline 85 \end{array} \qquad \begin{array}{r} 85 \\ -66 \\ \hline 19 \end{array}$$

Examples of Congruence and Modulus

- Find an integer that between 100 and 140 that congruent to $22 \pmod{41}$.

$\boxed{104}$

$$\begin{array}{r} 22 \\ +\ 82 \\ \hline 104 \end{array}$$

$$\begin{array}{r} 22 \\ +\ 123 \\ \hline 145 \\ -\ 41 \\ \hline 104 \end{array}$$

Examples of Congruence and Modulus

- Find an integer that between -140 and -100 that congruent to $22 \pmod{41}$.

$$\begin{array}{r} 22 \\ -123 \\ \hline -101 \\ -41 \\ \hline -142 \end{array}$$

$$\boxed{-101}$$

Theorems

- Let a and b be integers, and let m be a positive integer. Then $a \equiv b (\mathbf{mod}\, m)$ if and only if $a \,\mathbf{mod}\, m = b \,\mathbf{mod}\, m$.

- 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 $ac \equiv bd \pmod{m}$.

$$\begin{array}{r} 243 \\ 243 \\ 243 \\ \hline 26973 \end{array}$$

$111 + 243 \pmod 5$

$354 \equiv 4 \pmod 5$

$111 \cdot 243 \equiv 26973$

$\equiv 3 \pmod 5$

$111 \equiv 1 \pmod 5$

$243 \equiv 3 \pmod 5$

$111 + 243 \equiv 1 + 3 \equiv 4 \pmod 5$

$111 \cdot 243 \equiv 1 \cdot 3$

$\equiv 3 \pmod 5$

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 $ac \equiv bd \pmod{m}$.

$a = b + mk \qquad c = d + ms \quad , \quad k, s \in \mathbb{Z}.$

$a + c = b + mk + d + ms$
$= b + d + mk + ms$
$= (b + d) + m(k + s)$

$\rightarrow a + c \equiv b + d \pmod{m}$

$a \cdot c = (b + mk)(d + ms)$
$= bd + bms + dmk + mkms$
$ac = bd + m(bs + dk + mks)$

$\rightarrow ac \equiv bd \pmod{m}$

Corollary

- Let m be a positive integer and let a and b be integers. Then
  $$(a+b) \ \mathbf{mod}\ m \ = \ \big((a \ \mathbf{mod}\ m) + (b \ \mathbf{mod}\ m)\big) \ \mathbf{mod}\ m$$
  and
  $$ab \ \mathbf{mod}\ m \ = \ \big((a \ \mathbf{mod}\ m)(b \ \mathbf{mod}\ m)\big) \ \mathbf{mod}\ m \, .$$

Examples

- Find the LNR of $37485 + 467 \pmod{22}$.

$$37485 \equiv 19 \pmod{22}$$

$$467 \equiv 5 \pmod{22}$$

$$\begin{array}{r} 467 \pmod{22} \\ -440 \\ \hline 27 \\ -22 \\ \hline 5 \end{array}$$

$$37485 + 467 \equiv 19 + 5 \equiv 24 \equiv 2 \pmod{22}$$

- Find the LNR of $37485 \cdot 467 \pmod{22}$.

$$37485 \cdot 467 \equiv 19 \cdot 5 \equiv \underset{-88}{95} \equiv 7 \pmod{22}$$

$$\equiv (-3)(5) = -15 = 7 \pmod{22}$$