Lecture 11: Divisibility

Date: September 23, 2019.

Divides Relation. For integers \(a, b\), \(a\) divides \(b\) or \(a\) is a divisor of \(b\) or \(b\) is divisible by \(a\) or \(b\) is a multiple of \(a\) iff there is an integer \(k\) such that \(ak = b\). Notation: \(a \mid b\).

Question 1. Which of the following is necessarily true? (a) 173 \(\mid\) 0 \(\quad\) (b) 173 \(\mid\) 173 \(\quad\) (c) 1 \(\mid\) 173 \(\quad\) (d) \(-1\) \(\mid\) 173

\[\begin{align*}
\text{(e) } & 0 \mid 173 \\
\text{Proof: } & n \mid 0 \implies n = 0
\end{align*}\]

Lemma 1. Let \(a, b, c, s, t\) be any integers.
1. If \(a \mid b\) and \(b \mid c\) then \(a \mid c\).
2. If \(a \mid b\) and \(a \mid c\) then \(a \mid sb + tc\).
3. If \(c \neq 0\), \(a \mid b\) if and only if \(ac \mid cb\).

Assume \(a \mid b\), \(a \mid c\). By defn. \(j, k, s, t\) \(\quad a \mid j, k\). and \(ak = c\)

\[\begin{align*}
&sb + tc = s(j) + t(k) = a\left(s + t\right) \\
\implies & a \mid sb + tc
\end{align*}\]

Theorem 2 (Division Theorem). Let \(n\) and \(d\) be any integers such that \(d \neq 0\). Then there exist a unique pair of integers \(q\) and \(r\) such that

\[n = q \cdot d + r \quad \text{AND} \quad 0 \leq r < |d|\]

The number \(q\) is called the quotient (denoted \(\text{qcnt}(n, d)\)) and \(r\) is called the remainder (denoted \(\text{rem}(n, d)\)).

Problem 1. What are the quotient and remainder for the following pairs?

\[\begin{align*}
(32, 5) & : 32 = 6 \cdot 5 + 2 \\
(32, -5) & : 32 = (-6) \cdot (-5) + 2 \\
(-32, 5) & : -32 = 4 \cdot (-7) + 5 + 3
\end{align*}\]

Greatest Common Divisor. A common divisor of \(a\) and \(b\) is an integer that divides both \(a\) and \(b\). The greatest among the common divisors is written as \(\gcd(a, b)\).

Problem 2. What is the greatest common divisor for the following pairs?

\[\begin{align*}
gcd(18, 24) & = 6 \\
gcd(8, 1) & = 1 \\
gcd(3, 0) & = 3 \\
gcd(-3, 0) & = 3
\end{align*}\]

\[\begin{align*}
\text{Proof: } & n \in \mathbb{Z}, \ gcd(n, 1) = 1 \\
\text{Proof: } & n \neq 0, gcd(n, 0) = |n|
\end{align*}\]
Euclid's GCD Algorithm

Lemma 3. For any $a, b$ with $b \neq 0$, $\text{gcd}(a, b) = \text{gcd}(b, \text{rem}(a, b))$

\[
\text{rem}(a, b) = a - q \cdot \text{rem}(a, b) \mod b
\]

If $c \mid a$, $c \mid b$ then $c \mid \text{rem}(a, b)$

If $c \mid b$ and $c \mid \text{rem}(a, b)$ then $c \mid a$

\[
\text{CommonDiv}(n, b) = \text{CommonDiv}(b, \text{rem}(a, b))
\]

To compute $\text{gcd}(a, b)$, we can assume WLOG $a, b$ are positive, and $a \geq b$. Then $\forall a, b$, $\text{gcd}(a, b) = \text{gcd}(\lceil a/b \rceil, b)$

\[
\text{gcd}(a, b)
\]

while ($b > 0$)

\[
\begin{align*}
& r = \text{rem}(a, b) \\
& a = b \\
& b = r
\end{align*}
\]

return $a$

\[
\text{gcd}(5, 14) = \text{gcd}(14, 0) = 14
\]

\[
\text{gcd}(45, 21) = \text{gcd}(21, 9) = \text{gcd}(9, 3) = \text{gcd}(3, 0) = 3
\]

Congruence Modulo $n$. $a$ is congruent to $b$ modulo $n$ if $n \mid (a - b)$. This is written as $a \equiv b \pmod{n}$.

$32 \equiv 37 \pmod{5}$, because $5 \mid 37 - 32 = 5$

$98 \equiv 78 \pmod{10}$, because $10 \mid 98 - 78 = 20$

Lemma 4. $a \equiv b \pmod{n}$ iff $\text{rem}(a, n) = \text{rem}(b, n)$.

\[
\begin{align*}
& a = q_a n + r_a \\
& b = q_b n + r_b \\
& a \equiv b \pmod{n} \iff n \mid a - b \\
& \iff n \mid q_a n + r_a - (q_b n + r_b) \\
& \iff n \mid n (q_a - q_b) + (r_a - r_b) \\
& \iff n \mid r_a - r_b \quad -|n| < r_a - r_b < |n| \\
& \iff r_a - r_b = 0
\end{align*}
\]

Lemma 5. For any integers $a, b, c,$ and $n$ the following hold:

\[
\begin{align*}
& a \equiv a \pmod{n} & \text{[reflexivity]} \\
& a \equiv b \pmod{n} \iff b \equiv a \pmod{n} & \text{[symmetry]} \\
& (a \equiv b \pmod{n} \text{ AND } b \equiv c \pmod{n}) \text{ IMPLIES } a \equiv c \pmod{n} & \text{[transitivity]}
\end{align*}
\]

Let $R \subseteq A \times A$.

\[
\begin{align*}
& \text{Def: $R$ is reflexive iff } \forall a \in A. \quad (a, a) \in R. \\
& R \text{ is symmetric iff } \forall a, b, \quad (a, b) \in R \Rightarrow (b, a) \in R. \\
& R \text{ is transitive iff } \forall a, b, c, \quad (a, b) \in R \text{ AND } (b, c) \in R \Rightarrow (a, c) \in R.
\end{align*}
\]