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) $173 \mid 0$ T (b) $173 \mid 173$ T (c) $1 \mid 173$ T (d) $-1 \mid 173$ T (e) $0 \mid 173$ F | Prop: $\forall n.\ 0 \mid n$ IMPLIES $n=0$

Prop: $\forall n.\ n \mid 0$. because $n \cdot 0 = 0$

Prop: $\forall n.\ n \mid n$. because $n \cdot 1 = n$, $n \mid -n$ because $n \cdot (-1) = -n$

Prop: $\forall n.\ 1 \mid n$. because $1 \cdot n = n$, $-1 \mid n$

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 $a \mid sb + tc$.* | Linear combination of $b_1, b_2 \ldots b_k$ is $\sum s_i b_i$
3. *If $c \neq 0$, $a \mid b$ if and only if $ca \mid cb$.*

Assume $a \mid b$, $a \mid c$. By defn. $\exists j, k$ s.t. $aj = b$, and $ak = c$

$sb + tc = s(aj) + t(ak) = a\underline{(sj + tk)}$

$\Rightarrow a \mid sb + tc$

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*

$$n = q \cdot d + r \text{ AND } 0 \leq r < |d|.$$

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

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

$(32, 5)$: $32 = \underbrace{6}_{\text{quotient}} \cdot 5 + \underbrace{2}_{\text{remainder}}$ $\qquad (32, -5)$: $32 = \underline{(-6)} \cdot (-5) + \underline{2}$ $\qquad (-32, 5)$ $-32 = \cancel{7}\underline{(-7)} \cdot 5 + \underline{3}$

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?

$\gcd(18, 24) = 6$ $\qquad \gcd(8, 1) = 1$ $\qquad \gcd(3, 0) = 3$ $\qquad \gcd(-3, 0) = 3$

Prop: $\forall n \in \mathbb{Z}.\ \gcd(n, 1) = 1$

Prop: $\forall n \neq 0\ \gcd(n, 0) = |n|$

Euclid's GCD Algorithm

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

$\text{rem}(a,b) = a - \text{qcnt}(a,b) \cdot b$ $\qquad$ $a = \text{qcnt}(a,b)\, b + \text{rem}(a,b)$

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

$\text{Commondiv}(a,b) = \text{Commondiv}(b, \text{rem}(a,b))$

To compute $\gcd(a,b)$, we can assume WLOG a, b are positive, and $a \geq b$. $\mid \forall a,b,\ \gcd(a,b) = \gcd(|a|,|b|)$

```
gcd(a,b)
    while (b > 0)
        r = rem(a,b)
        a = b
        b = r
    return a
```

$\gcd(56, 14) = \gcd(14, 0) = 14$

$\gcd(93, 21) = \gcd(21, 9)$

$= \gcd(9, 3)$

$= \gcd(3, 0) = 3$

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

$32 \equiv 37 \pmod 5$. because $5 \mid 37 - 32 = 5$

$93 \equiv 28 \pmod{13}$ because $13 \mid 93 - 28 = 65$

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

$a = q_a n + r_a \qquad b = q_b n + r_b$.

$a \equiv b \pmod n \iff n \mid a - b$

$\iff n \mid q_a n + r_a - (q_b n + r_b)$

$\iff n \mid \underline{n(q_a - q_b)} + (r_a - r_b)$

$\iff n \mid r_a - r_b. \qquad -|n| < r_a - r_b < |n|$

$\iff r_a - r_b = 0$

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

$$a \equiv a \pmod{n} \quad \text{[reflexivity]}$$
$$a \equiv b \pmod{n} \text{ IFF } b \equiv a \pmod{n} \quad \text{[symmetry]}$$
$$(a \equiv b \pmod{n} \text{ AND } b \equiv c \pmod{n}) \text{ IMPLIES } a \equiv c \pmod{n} \quad \text{[Transitivity]}$$

Let $R \subseteq A \times A$.

Def: R is reflexive iff $\forall a \in A.\ (a,a) \in R$.

R is symmetric iff $\forall a, b,\ (a,b) \in R \Rightarrow (b,a) \in R$.

R is transitive iff $\forall a,b,c,\ (a,b) \in R$ AND $(b,c) \in R \Rightarrow (a,c) \in R$.