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) $173 \mid 0$ (b) $173 \mid 173$ (c) $1 \mid 173$ (d) $-1 \mid 173$ (e) $0 \mid 173$

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 $ca \mid cb$.*

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*

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

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?
$(32, 5)$ $(32, -5)$ $(-32, 5)$

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?
$\gcd(18, 24)$ $\gcd(8, 1)$ $\gcd(3, 0)$ $\gcd(-3, 0)$

Euclid's GCD Algorithm

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

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

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

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

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

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

$$\begin{aligned} a \equiv a &\pmod{n} \\ a \equiv b \pmod{n} \text{ IFF } b \equiv a &\pmod{n} \\ (a \equiv b \pmod{n} \text{ AND } b \equiv c \pmod{n}) \text{ IMPLIES } a \equiv c &\pmod{n} \end{aligned}$$