CS 173 Lecture 3a: Integers & Divisibility

(Elementary)
Number theory: (historically) the study of integers

Applications: High-speed numerical computation
modern cryptography. (primality / divisibility)

divisibility by 2.
Definition: An integer a is even if there exists an integer k such that $a = 2k$.

Definition: An integer a is divisible by an integer b if there exists an integer k such that $a = bk$.
(in notation: $b \mid a$)
b is a <u>factor</u> of a & a is a <u>multiple</u> of b.

Ex:

$9 \mid 81$	$-7 \mid 21$
$9 \mid 0$ $\quad 0 = 9 \cdot 0$	$7 \mid -21$
$0 \nmid 9$	$-7 \mid -21$
$0 \mid 0$	

Theorem. For all integers a, b, c:
(i) If $a \mid b$ and $a \mid c$, then $a \mid (b+c)$
$\longrightarrow$ (ii) If $a \mid b$, then $a \mid bc$
(iii) If $a \mid b$, and $b \mid c$, then $a \mid c$.

Proof. (i) Let a, b, c be integers and suppose that $a \mid b$ and $a \mid c$.
By definition of divisibility, there exist integers k & ℓ such that $b = ak$ and $c = a\ell$. Then $b + c = ak + a\ell = a(k+\ell)$.
Thus there exists an integer m, $m = k + \ell$, such that $b + c = am$. This $a \mid (b+c)$.

(ii), (iii): Exercise.

(ii)

(ii), (iii): Exercise.

(!!) Warning: don't treat divisibility as involving ratios/fractions

e.g. $a \mid b$ means $\frac{b}{a} \in \mathbb{Z}$.

What about $a=0$? (See §4.3)

Corollary. Let a, b, c be integers. If $a \mid b$ and $a \mid c$, then for all integers m, n, $a \mid (mb+nc)$.

Proof. Let a, b, c, m, n be integers, and suppose $a \mid b$ and $a \mid c$.

By part (ii) of the theorem, $\underline{a \mid mb}$ and $\underline{a \mid nc}$. Then using part (i), $a \mid (mb+nc)$. $\square$

Theorem (Division Algorithm): For all integers a, b, there exist <u>unique</u> integers q & r such that:

(1) $a = bq + r$

(2) $0 \leq r < b$

$q = \text{quot}(a,b)$ (quotient) $\quad$ $r = \text{rem}(a,b)$ (remainder)

Ex: $a = 173$, $b = 5$. $\to$ $q = 34$, $r = 3$.

$5 \cdot 34 = 170 \to 5 \cdot 34 + 3 = 173$ ✓

$a = 2401$, $b = -7$ $\to$ $q = -343$, $r = 0$

$(-7)(-343) = 2401$.