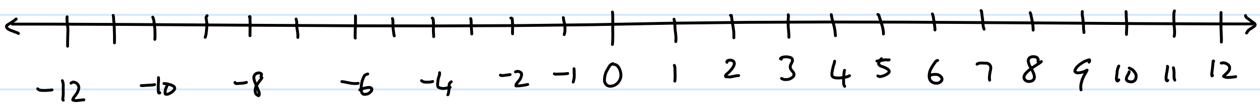
Number Theory

1/18/12

Integers – whole numbers written using the ten numerals 0, 1, ..., 9, where the position of a numeral dictates the value it represents.

The set of integers is denoted by $\mathbb{Z}$.

$\therefore\ \mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$



$\mathbb{N}$, Natural numbers: all positive integers / all nonnegative integers

$\therefore\ \mathbb{N} = \{1, 2, 3, \ldots\}$ or $\mathbb{N} = \{0, 1, 2, \ldots\}$

If a is an integer, $|a|$ denotes the absolute value of a.

if a is positive int, $|a| = a$

If a is negative, $|a| = -a$

If $a = 13$, $|a| = 13$

If $a = -13$, $|a| = 13$

Division

Let a and b are integers with $a \neq 0$.
a divides b, denoted $a \mid b$,
if there is an integer c such that $b = ac$.

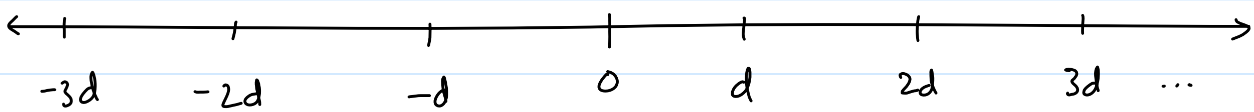
$\Rightarrow$ a is a factor of b
b is a multiple of a

Otherwise a does not divide b, or $a \nmid b$.

Example: Does 9 divide 36? yes 9 | 36

True or False: 11 | 120? False

Example: Let n and d be positive integers. How many positive integers not exceeding n are divisible by d?



Find an integer k such that
(i) $kd \leq n$ (ii) $(k+1)d > n$

That is the largest k that satisfies $kd \leq n$

$kd \leq n \Rightarrow k \leq n/d \Rightarrow k = \lfloor \frac{n}{d} \rfloor$

$\lceil x \rceil$ is the smallest integer $\geq$ x.

$\lfloor x \rfloor$ is the largest integer $\leq$ x.

$\lceil 11.7 \rceil = 12$; $\lfloor 11.7 \rfloor = 11$; $\lceil -5.3 \rceil = -5$; $\lfloor -5.3 \rfloor = -6$.

Show that $\lceil \frac{n}{k} \rceil < \frac{n}{k} + 1$

Theorem 1.
Let a, b, and c be integers and a ≠ 0.
(i) If a|b and a|c, then a|(b+c).
(ii) If a|b, then a|bc.
(iii) If a|b and b|c, b ≠ 0, then a|c.

Proof: (ii) Let $a|b$. By the def. of divisibility, there exists some integer k such that $b = k \cdot a$

$bc = (k \cdot a) \cdot c = (k \cdot c)\, a \Rightarrow bc$ is a multiple of a

$\Rightarrow a \mid bc$.

(i) Let $a|b$ and $a|c$.

$a|b \Rightarrow b = k \cdot a$, k is an integer

$a|c \Rightarrow c = l \cdot a$, l is an integer

$b+c = ka + la = (k+l)\, a \Rightarrow (b+c)$ is a multiple of a

$\Rightarrow a \mid b+c$.

(ii) If $a|b \Rightarrow b = ka$

$bc = (kc) \cdot a$

$\Rightarrow$ a is a multiple of bc or $a|bc$.

(iii) Let $\underbrace{a|b}_{b = ka}$ and $\underbrace{b|c}_{c = l \cdot b}$ for some integers k and l

$\therefore c = lb = l(ka) = (lk)\, a$

$\Rightarrow c$ is a multiple of $a \Rightarrow a|c$.

Problem 8 [KR, Section 4.1]. Prove or disprove: if a|bc, then a|b or a|c.

False: Try $a=4$, $b=2$, $c=6$

7. Let a, b, and c be integers, a ≠ 0, c ≠ 0. Prove or disprove: if ac|bc, then a|b.

If $ac \mid bc$, then $\underline{bc = k \cdot ac}$ (by def.)

$\Rightarrow b = k \cdot a$ when divided by c on both sides

$\Rightarrow a \mid b$. (by def)

Corollary 1. Let a, b, and c be integers and a ≠ 0. If a|b and a|c, then a|(mb+nc) whenever m and n are integers.

Proof: Let $a \mid b \Rightarrow \underline{a \mid m \cdot b}$ for any int. m (Theorem 1, Part ii)

Let $a \mid c \Rightarrow \underline{a \mid n \cdot c}$ for any int. n (Theorem 1, Part ii)

$a \mid mb$ and $a \mid nc \Rightarrow a \mid (mb+nc)$ (Theorem 1, part 1)

Division Algorithm

Let a and d be integers with $d \neq 0$. Then there exist unique integers q and r, $0 \leq r < |d|$, such that

$a = q.d + r$.

Terminology a = dividend, d = divisor, q = quotient, and r = remainder

q = a div d   &   r = a mod d

Example: Give the q and r for the following cases.

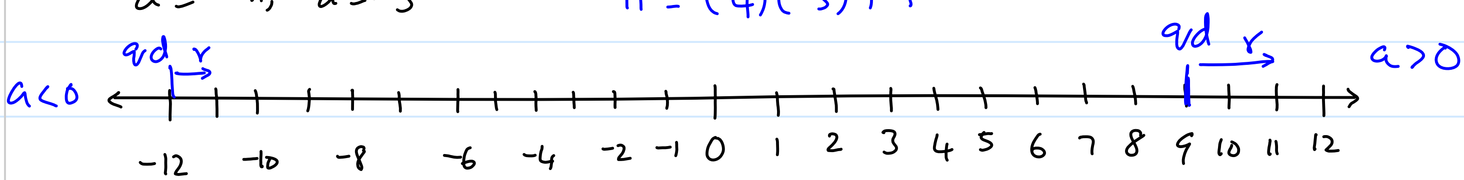
$a = \underline{q}\,\underline{d} + \underline{r}$, r is positive

$a = 11,\ d = 3$ $11 = 3 \times 3 + 2$ $q = 3,\ r = 2$

$a = -11,\ d = 3$ $-11 = \underline{(-4) \times 3} + 1$ $q = -4,\ r = 1$

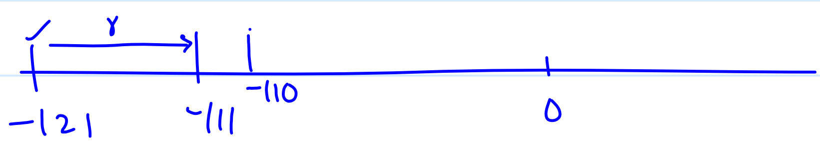
$a = 11,\ d = -3$ $11 = (-3) \times (-3) + 2$

$a = -11,\ d = -3$ $-11 = (4)(-3) + 1$



Problem 9 b. What are the quotient and remainder when -111 is divided by 11?

$-111 = (-11)(11) + 10$



21 (c). evaluate 155 mod 19 = 3 $8 \times 19 = 152 \rightarrow 155$

155 div 19 = 8 $= \left\lfloor \frac{155}{19} \right\rfloor$

Integer division $\frac{a}{d} = \left\lfloor \frac{a}{d} \right\rfloor$ $\frac{a+d-1}{d} = \left\lceil \frac{a}{d} \right\rceil$