Preliminaries

Number systems:

$\mathbb{Z}$: integers $= \{0, \pm 1, \pm 2, \pm 3, \ldots\}$

$\mathbb{Q}$: rationals $= \{ \frac{a}{b} \mid a, b \in \mathbb{Z},\ b \neq 0 \}$

$\mathbb{R}$: real numbers

$\mathbb{C}$: complex numbers $\rightsquigarrow \{ a+bi \mid a, b \in \mathbb{R},\ i = \sqrt{-1} \}$

Properties of integers

$a, b \in \mathbb{Z} \Rightarrow a+b \in \mathbb{Z},\quad a-b \in \mathbb{Z},\quad ab \in \mathbb{Z}$

"elements of"

Note: $\frac{a}{b}$ may <u>not</u> be in $\mathbb{Z}$. $\leftsquigarrow$ not closed under quotients

We say a <u>divides</u> b, denoted $a \mid b$, if there is some integer k s.t. $ak = b$.

"such that"

WARNING: in general, try to avoid writing

$$k = \frac{b}{a} \quad \ldots$$ can lead to confusion.

A prime is a number $p > 1$ whose only positive divisors are 1 and p.

Thm (Division algorithm)

"suppose"

Sps. $a, b \in \mathbb{Z}$ with $b > 0$. There exist unique $q, r \in \mathbb{Z}$ such that

quotient and remainder

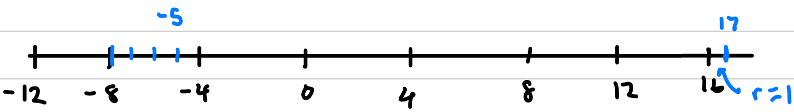
$$a = qb + r$$

where $0 \le r < b$

proof: omitted.

$* \; 0 \le r < 4$

Idea: Ex: $b = 4$ $\quad a = 17 = \overset{q}{4}(\overset{b}{4}) + \overset{r}{1}$ $\quad$ or $\quad a = -5 = \overset{q}{-2}(\overset{b}{4}) + \overset{r}{3}$



Note: proof is algebraic ... pictures good for intuition but don't suffice as a proof.