Numb3rs

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

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

$\mathbb{Z}^+ = \{ 1, 2, \ldots \}$

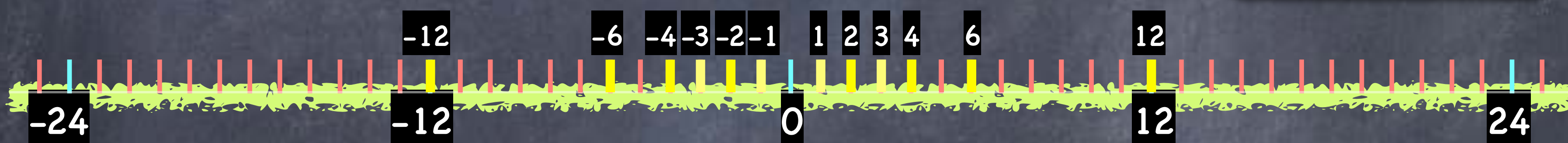
& addition, subtraction and multiplication

Quotient & Remainder

Divisibility

- Definition: For $n,d \in \mathbb{Z}$, $d|n$ (d divides n) if $\exists q \in \mathbb{Z}\ \ n = qd$
  - $d|n$ ≡ n is a multiple of d ≡ d is a divisor of n

a.k.a. a factor



  - e.g. Multiples(12) = { ..., -24, -12, 0, 12, 24, ... }.
  - e.g. Divisors(12) = { ±1, ±2, ±3, ±4, ±6, ±12 }.
- Divisors(0) = $\mathbb{Z}$ [$\forall d \in \mathbb{Z}\ \ d|0$]. Multiples(0) = {0} [$\forall n \in \mathbb{Z}\ \ 0|n \leftrightarrow n=0$]

Divisibility

- Proposition: $\forall\ m,n,n' \in \mathbb{Z}$ if $m|n$, then $m|nn'$

$n = qm$
$\Rightarrow nn' = q'm$, where $q'=qn'$

- Proposition: $\forall\ m,n,n' \in \mathbb{Z}$ if $m|n$ and $m|n'$, then $m|(n+n')$

$n = qm$ & $n' = q'm$
$\Rightarrow n+n' = q''m$, where $q''=q+q'$

- Proposition: $\forall\ m,n,n' \in \mathbb{Z}$ if $m|n$ and $n|n'$, then $m|n'$

$n = qm$ & $n' = q'n$
$\Rightarrow n' = q''m$, where $q''=qq'$

- Proposition: $\forall\ m,n,n' \in \mathbb{Z}$ if $mn'|nn'$ and $n' \neq 0$, then $m|n$

$nn' = qmn'$ & $n' \neq 0$
$\Rightarrow n = qm$

- Proposition: $\forall\ m,n \in \mathbb{Z}$ if $m|n$ and $n \neq 0$, then $|m| \leq |n|$

$n = qm$ & $n \neq 0 \Rightarrow |n| = |q| \cdot |m|$ where $|q| \geq 1$
$\Rightarrow |n| = |m| + (|q|-1) \cdot |m| \geq |m|$

Quotient-Remainder Theorem

> For any two integers m and n, $m \neq 0$, there is a <u>unique</u> quotient q and remainder r (integers), such that
>
> $$n = q \cdot m + r, \quad 0 \leq r < |m|$$

- <u>Proof of existence</u>
  - We shall prove it for all $n \geq 0$ and $m > 0$. Then, the other cases can be proven using $|n| = q \cdot |m| + r,\ 0 \leq r < |m|$
    - $n \geq 0, m < 0$: $n = q \cdot |m| + r = (-q)m + r.\ \ 0 \leq r < |m|$
    - $n < 0, m > 0$: $n = -|n| = -(q \cdot m + r) = -(q+1)m + (m-r).\ \ 0 \leq m-r < m$
    - $n < 0, m < 0$: $n = -|n| = -(q(-m)+r) = (q+1)m + (|m|-r).\ 0 \leq |m|-r < |m|$

    > <u>Assuming $r > 0$.</u>
    > <u>If $r = 0$, $n = \pm qm$</u>

  - Fix any $m>0$. We use strong induction on n.
  - Base cases: $n \in [0,m)$. Then let $q=0$ and $r=n$: $n = 0.m + n$.
  - Induction step: We shall prove that for all $k \geq m$,
    - <u>(induction hypothesis):</u> if $\forall n \in \mathbb{Z}^+$ s.t. $n<k$, $\exists q,r$ s.t $n=qm+r$ & $0 \leq r < m$
    - <u>(to prove):</u> then $\exists q^*, r^*$ s.t. $k = q^* \cdot m + r^*$ & $0 \leq r^* < m$.
  - Consider $k' = k-m$. $0 \leq k' < k$. By ind. hyp. $k' = q'm + r'$. Let $q^* = q'+1$, $r^* = r'$. □

Quotient-Remainder Theorem

For any two integers m and n, $m \neq 0$, there is a unique quotient q and remainder r (integers), such that

$$n = q \cdot m + r, \quad 0 \leq r < |m|$$

- Proof of existence
  - Also known as "Division Algorithm" (when you unroll the inductive argument, you get a (naïve) algorithm)
- Proof of uniqueness:
  - Claim: if $n = q_1 \cdot m + r_1 = q_2 \cdot m + r_2$, where $0 \leq r_1, r_2 < |m|$, then $q_1 = q_2$ and $r_1 = r_2$
    - Suppose, $q_1 m + r_1 = q_2 m + r_2$.
    - W.l.o.g, $r_1 \geq r_2$. So, $0 \leq (r_1 - r_2) < |m|$. Also, $(r_1 - r_2) = (q_2 - q_1)m$. Now, the only multiple of m in the range $[0,|m|)$ is 0. So $r_1 = r_2$.
    - Then $(q_1 - q_2)m = 0$. Since $m \neq 0$, $q_1 = q_2$.

Quotient-Remainder Theorem

For any two integers m and n, m≠0, there is a unique quotient q and remainder r (integers), such that

$$n = q \cdot m + r, \quad 0 \le r < |m|$$