Note Title 10/22/2014

Proof of correctness for Power(a, n).

Power(a, n) $\longrightarrow a^n$. a real #

n non-neg int.

- $\Rightarrow$ if $(n=0)$ return 1.

$\Rightarrow$ if (n is even)
    Return((Power $(a, n/2))^2$)
if (n is odd
    Return (Power $(a, \lfloor n/2 \rfloor))^2 \cdot a$);

End.

Theorem For any real # a, and any non-neg int n, Power(a, n) return $a^n$

$\forall n \; \underbrace{\forall a \; \text{Power}(a, n) = a^n}_{Q(n)}$.

Proof By induction on n.

Base: $n=0$ $a^0 = 1$.
Power(a, 0) returns 1

Induction step: Assume for $k = 0, 1, \ldots, n-1$, and $n \geq 1$.
Power(a, k) returns $a^k$.
Prove Power(a, n) returns $a^n$.

Case 1 n is even and $n \geq 1$.

$n = 2k$ for some int $k$. $n \geq 2$

$k \geq 1$.

Recursive call on $Power(a, n/2)$

$= Power(a, k)$. $\Rightarrow$

Show $k \in \{0, 1, \ldots, n-1\}$.

$0 \leq k \leq n-1$.

Show $k \leq n-1$. $n \geq 2$.

$\frac{n}{2} \leq n-1$.

$2 \leq n$ $+n$

$2+n \leq n+n$

$n \leq 2n-2$

$n \leq 2(n-1)$

$n/2 \leq n-1$

By the I.H.

$Power(a, n/2) = a^{n/2}$

$Power(a, n)$ returns $[Power(a, n/2)]^2$

$= (a^{n/2})^2 = a^{n/2 \cdot 2} = a^n$

Case 2: n is odd and $n \geq 1$

$2k+1 = n$ $k \geq 0$.

Recursive call: $\lfloor n/2 \rfloor = \lfloor \frac{2k+1}{2} \rfloor$

$= \lfloor k + 1/2 \rfloor = k$.

$n = 2k+1$ $\quad k \geq 0 \quad n \geq 1.$

Recursive call $\quad Power(a, \lfloor n/2 \rfloor) = Power(a, k)$

$0 \leq k \leq n-1$

$n = 2k+1$

$n-1 = 2k \geq k$

By the I.H. $\quad Power(a, \lfloor n/2 \rfloor) = Power(a,k) = a^k$

Power(a,n) returns $\left[Power(a,k)\right]^2 \cdot a$

$= (a^k)^2 \cdot a =$

$a^{2k} \cdot a = a^{2k+1} = a^n \quad \boxtimes$

Recursive def of nested parens.

Base: ( ) properly nested

Recursive rule: If $x$ is properly nested then $(x)$ is P.N.

If $x$ & $y$ are P.N. then $xy$ is P.N.

Theorem: If $s$ is properly nested then # of left parens in $s$ is equal to the # of right parens in $s$.

If $s$ is a sequence of parens, $N[(, s] =$ # of left parens in $s$.

$N[), s]$ = # right parens.

**Thm** $\forall n \geq 2$ ~~If~~ $s$ is properly nested seq of parens w/ $n$ symbols
then $N[(, s] = N[), s]$.

**Proof** By ind on the length of the seq.

Base case: $n=2$ $\quad s = ()$

$N[(, s] = N[), s] = 1$.

Assume for $k = 2, \ldots, n-1$.
any properly nested seq of length $k$ has the same # of left parens & right parens.
Prove claim holds true for length $n$ sequences.

If $s$ is properly nested & length $n$.

① $s = (x)$ where $\underline{x}$ is properly nested.

② $s = xy$ where $\underline{x}$ & $y$ are properly nested.

Case 1 $\quad s = (x)$ $\quad$ By I.H. $N[(, x] = \underline{N[), x]}$

$$N[(, s] = 1 + \underline{N[(, x]} = \underline{1 + N[), x]} = N[), s].$$

Case 2 $\quad s = xy$. $\quad$ By I.H. $N[(, x] = N[), x]$

$N[(, y] = N[), y]$

$$N[(, s] = N[(, x] + N[(, y] = \underline{N[), x] + N[), y]}$$
$$= N[), s] \quad \otimes.$$

Number theory: $a$ & $b$.

$a \mid b$ $\quad$ $a$ "divides" $b$.

$b$ is a multiple of $a$.
$a$ is a factor / divisor of $b$.
$b = k \cdot a$ $\quad$ $k$ int.

$6 \mid 48$ $\quad$ $48 = 6 \cdot 8$.

$6 \nmid 49$

$-3 \mid 90$ $\quad$ $90 = -3(-30)$

$5 \mid -45$

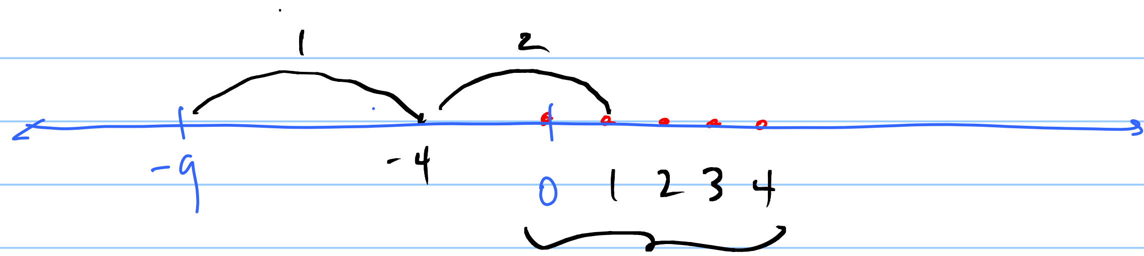
Modular arithmetic $\quad$ $17 \bmod 3 = 2$.

$-17 \bmod 3 = 1$

For any int $n$ and any $d \geq 1$.
There are unique integers $q, r$

$$n = q \cdot d + r \qquad r \in \{0, \ldots, d-1\}.$$

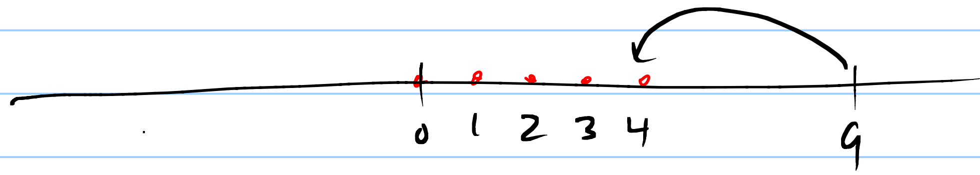
$-9 \bmod 5$




$-9 \bmod 5 = 1$
$-9 \text{ div } 5$

$$-9 = \underset{q}{\boxed{-2}} \cdot 5 + 1.$$

9 mod 5 = 4
9 div 5 = 1




$$n \text{ div } d = \left\lfloor n/d \right\rfloor \qquad \left\lfloor -9/5 \right\rfloor = -2$$

$$n \ \underline{\text{mod}} \ d = n - (n \text{ div } d) \cdot d.$$

$$-9 - (-2) \cdot 5 = 1.$$