Proof. A correction for Power(a, n).

\[ \text{Power}(a, n) \quad a \text{ real } \quad a^n \]

\[ n \text{ non-neg int.} \]

- \[ \Rightarrow \text{ if } (n = 0) \text{ return 1}. \]

- \[ \Rightarrow \left\{ \begin{array}{l}
\text{if } (n \text{ is even}) \rightarrow \text{ \text{Power}(\text{Power}(a, \frac{n}{2}))^2) \\
\text{if } (n \text{ is odd}) \rightarrow \text{ \text{Power}(a, \frac{n-1}{2})^2 \cdot a)}
\end{array} \right. \]

End.

Theorem. For any real \# a, and any non-neg int \( n \), Power(a, n) returns \( a^n \)

\[ \forall n \quad \text{Power}(a, n) = a^n \quad (Q(n)) \]

Proof. By induction on \( n \).

Base. \( n = 0 \)

\[ a^0 = 1 \]

\[ \text{Power}(a, 0) \text{ returns 1} \]

Induction step. Assume for \( k = 0, 1, \ldots, n-1 \), and \( n \geq 1 \).

\[ \text{Power}(a, k) \text{ returns } a^k \]

Prove \[ \text{Power}(a, n) \text{ returns } a^n \].
Case 3: \( n \) is even and \( n \geq 1 \).
\[
n = 2k \text{ for some integer } k. \quad n \geq 2 \quad k \geq 1.
\]

Rewrite \( n = 2k \) as \( n = 2k \).

Show \( k \leq \frac{n}{2}, \ldots, n-1 \).
\[
0 \leq k \leq n-1.
\]

Show \( k \leq n-1. \quad n \geq 2. \quad \frac{n}{2} \leq n-1. \)

By the I.H.

\[
\text{Power}(a, \frac{n}{2}) = a^{\frac{n}{2}}
\]

\[
\text{Power}(a, n) \text{ when } \left[\text{Power}(a, \frac{n}{2})\right]^2
\]

\[
\Rightarrow \left(a^{\frac{n}{2}}\right)^2 = a^{n/2 \cdot 2} = a^n
\]

Case 2: \( n \) is odd and \( n \geq 1 \)

\[
2k+1 = n \quad k \geq 0.
\]

Rewrite \( n = 2k+1 \) as \( \left[\frac{n}{2}\right] = \left\lfloor \frac{2k+1}{2} \right\rfloor \)

\[
\Rightarrow \left\lfloor k + \frac{1}{2} \right\rfloor = -k.
\]
\[ n = 2k + 1 \quad k \geq 0 \quad m \geq 1. \]

Reason: all \( P_{\text{noun}}(a, L^{m+1}) = P_{\text{noun}}(a, k) \)

\[ 0 \leq k \leq n - 1 \]

\[ n = 2k + 1 \]

\[ n - 1 = 2k \geq a \]

By the I.H. \( P_{\text{noun}}(a, L^{m+1}) = P_{\text{noun}}(a, k) = a^k \)

\[ P_{\text{noun}}(a, n) \text{ returns } \left[ \left( P_{\text{noun}}(a, k) \right)^2 \cdot a \right] = (a^k)^2 \cdot a = a^{2k} \cdot a = a^{2k+1} = a^n \]

Reasoning definition of nested paren.

Base: () properly nested

Reason rule: If \( x \) is properly nested then \( (x) \) is P.N.

If \( x+y \) are P.N.

then \( xy \) is P.N.

There: If \( s \) is properly nested then \# of left paren in \( s \) is equal to the \# of right paren in \( s \).

If \( s \) is a sequence of paren,

\[ N[((), s)] = \# \text{ of left paren in } s. \]
\[ N[(),s] = \# \text{ right parens}. \]

Then for \( n \geq 2 \), if \( s \) is properly nested seq of parens of length \( n \) symbols then \( N[(,s)] = N[(),s] \).

Proof: By induction on the length of the seq.

**Base case:** \( n = 2 \), \( s = () \).
\[ N[(,())] = N[(),()] = 1. \]

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 \( n \),
\( s = (x) \) where \( x \) is properly nested,
\( s = xy \) where \( x + y \) are properly nested.

**Case 1:** \( s = (x) \) By I.H. \( N[(,x)] = N[(),x] \)
\[ N[(,s)] = 1 + N[(,x)] = 1 + N[(),x] = N[(),s]. \]

**Case 2:** \( s = xy \) By I.H. \( N[(,x)] = N[(),x] \)
\( N[(,y)] = N[(),y] \)
\[ N[(,s)] = N[(,x)] + N[(,y)] = N[(),x] + N[(),y] = N[(),s]. \]

\( \Box \)
Number Theory: \( a \divides b \).

\[ a \divides b \quad \text{a "divides" b.} \]

\[ b \text{ is a multiple of } a. \]

\[ a \text{ is a factor/divisor of } b. \]

\[ b = k \cdot a \quad k \text{ int.} \]

\[ 6 \divides 48 \quad 48 = 6 \cdot 8. \]

\[ 6 \divides 49 \]

\[ -3 \divides 90 \quad 90 = -3(-30) \]

\[ 5 \divides -45 \]

Modular arithmetic

\[ 17 \text{ mod } 3 = 2. \]

\[ -17 \text{ mod } 3 = 1 \]

For any \( n \) and any \( d \geq 1 \).

There are unique integers \( q, r \)

\[ n = q \cdot d + r \quad r \in \{0, \ldots, d-1\} \]

\[ n = 9 \quad d = 5 \]

\[ -9 = \frac{-12}{5} + 1 \quad -9 \text{ mod } 5 = 1 \]

\[ -9 \text{ div } 5 \]
\[ n \mod d = \left\lfloor \frac{n}{d} \right\rfloor \quad \left\lfloor \frac{-9}{5} \right\rfloor = -2 \]

\[ n \mod d = n - (n \div d) \cdot d. \]

\[-9 - (-2) \cdot 5 = 1.\]