3. Prove that $m^{n+k} = m^n \cdot m^k$. (You may assume all the laws of successor and addition that we proved.)

Lemma 0.1. *Distributivity of Mulitplication over Addition:* $m(n+k) = m \cdot n + m \cdot k$

Proof. We induct on k for fixed m and n.

Base Case $k = 0$:

$$\begin{aligned} m \cdot (n+0) &= m \cdot n && \text{(IC of Addition)} \\ &= m \cdot n + 0 && \text{(IC of Addition)} \\ &= m \cdot n + m \cdot 0 && \text{(IC of Multiplication).} \end{aligned}$$

Assume

$$m \cdot (n+k) = m \cdot n + m \cdot k \text{ (I.H.).}$$

Inductive Step: We want to show that $m(n + S(k)) = m \cdot n + m \cdot S(k)$.
We have

$$\begin{aligned} m \cdot (n + S(k)) &= m \cdot (S(n+k)) && \text{(RR of Addition)} \\ &= m \cdot (n+k) + m && \text{(RR of Multiplication)} \\ &= (m \cdot n + m \cdot k) + m && \text{(I.H.)} \\ &= m \cdot n + (m \cdot k + m) && \text{(Associative Law of Addition)} \\ &= m \cdot n + m \cdot S(k) && \text{(RR of Multiplication).} \end{aligned}$$

□

Lemma 0.2. *Associative Law of Multiplication* $m \cdot (n \cdot k) = (m \cdot n) \cdot k$.

Proof. We induct on k for fixed m and n.

Base Case $k = 0$: We have that $m \cdot (n \cdot 0) = m \cdot 0 = 0$ and $(m \cdot n) \cdot 0 = 0$ by the base case in the recursive definition of multiplication

Inductive Step:
Assume

$$(m \cdot n) \cdot k = m \cdot (n \cdot k) \text{ (I.H.).}$$

$$\begin{aligned} m \cdot (n \cdot S(k)) &= m \cdot (n \cdot k + n) && \text{(RR of Multiplication)} \\ &= m \cdot (n \cdot k) + m \cdot n && (\textbf{Lemma 0.1}) \\ &= (m \cdot n) \cdot k + m \cdot n && (\textbf{I.H.}) \\ &= (m \cdot n) \cdot S(k) && \text{(RR of Multiplication).} \end{aligned}$$

□

Robert Green
Jasmin Rodriguez

Lemma 0.3. *Unit Law for 1 of Multiplication* $m \cdot 1 = 1 \cdot m = m$ *(where* $1 = S(0)$ *).*

Proof. By the first recursive case of the Multiplication definition, we have that

$$m \cdot 1 = m \cdot 0 + m$$

By the base case of the definition of Multiplication, we have that $m \cdot 0 = 0$, so then by the additive identity of 0, we have that

$$m \cdot 1 = m$$

□

Proof. We induct on k given m and n.

Base case $k = 0$: We need to show that $m^{n+0} = m^n \cdot m^0$.

We have: $m^{n+0} = m^n$ by the base case of the definition of Addition. This is then equal to $m^n \cdot 1$ by the Unit Law for 1 of Multiplication. By the Initial Case of the Exponentiation definition, we have that $1 = m^0$. This gives us that $m^n = m^n \cdot m^0$.

Putting this all together,

$$\begin{aligned} m^{n+0} &= m^n && \text{(IC of Addition)} \\ &= m^n \cdot 1 && (\textbf{Lemma 0.3}) \\ &= m^n \cdot m^0 && \text{(IC of Exponentiation).} \end{aligned}$$

Inductive Step: Suppose that it is true for some k that $m^{n+k} = m^n \cdot m^k$. We want to show that $m^{n+S(k)} = m^n \cdot m^{S(k)}$.

$$\begin{aligned} m^{n+S(k)} &= m^{S(n+k)} && \text{(RR Addition)} \\ &= m^{n+k} \cdot m && \text{(RR Exponentiation)} \\ &= (m^n \cdot m^k) \cdot m && \text{(I.H.)} \\ &= m^n \cdot (m^k \cdot m) && \text{(Associative Law of Multiplication)} \\ &= m^n \cdot m^{S(k)} && \text{(RR Exponentiation).} \end{aligned}$$

Therefore, by induction $m^{n+S(k)} = m^n m^{S(k)}$.

□