**Solutions to HW 4.**

In the solutions below I will assume the truth of all the Laws of Addition from the February 14 handout arithmetic.pdf. Following a common convention, I may denote the product of $m, n \in \mathbb{N}$ by either $mn$ or by $m \cdot n$. Also, I will use the following abbreviations:

- IC = Initial Condition
- RR = Recurrence Relation
- IH = Inductive Hypothesis

1. Prove that $m(n + k) = (mn) + (mk)$ holds for all $m, n, k \in \mathbb{N}$.

This is a proof by induction on $k$.
(Base Case: $k = 0$)

$$\begin{aligned} m(n+0) &= mn && \text{(IC, +)} \\ &= mn + 0 && \text{(IC, +)} \\ &= mn + m0 && \text{(IC, }\cdot\text{)} \end{aligned}$$

(Inductive Step: Assume true for $k$, prove true for $S(k)$)

$$\begin{aligned} m(n+S(k)) &= m \cdot S(n+k) && \text{(RR, +)} \\ &= m \cdot (n+k) + m && \text{(RR, }\cdot\text{)} \\ &= ((mn) + (mk)) + m && \text{(IH)} \\ &= (mn) + ((mk) + m) && \text{(Associative Law, +)} \\ &= (mn) + mS(k) && \text{(RR, }\cdot\text{)} \end{aligned}$$

2. Prove that $m(nk) = (mn)k$ holds for all $m, n, k \in \mathbb{N}$.

This is a proof by induction on $k$.
(Base Case: $k = 0$)

$$\begin{aligned} m(n0) &= m0 && \text{(IC, }\cdot\text{)} \\ &= 0 && \text{(IC, }\cdot\text{)} \\ &= (mn)0 && \text{(IC, }\cdot\text{)} \end{aligned}$$

(Inductive Step: Assume true for $k$, prove true for $S(k)$)

$$\begin{aligned} m(n \cdot S(k)) &= m(nk+n) && \text{(RR, }\cdot\text{)} \\ &= m(nk) + mn && \text{(Distributive Law, Problem 1)} \\ &= (mn)k + mn && \text{(IH)} \\ &= (mn) \cdot S(k) && \text{(RR, }\cdot\text{)} \end{aligned}$$

3. Prove that $mn = nm$ holds for all $m, n \in \mathbb{N}$. (Some lemmas will be needed.)

I am going to give two proofs, both by induction on $n$.

**Proof 1.**

**Lemma 1.** $0k = 0$.

*Proof.* This is a proof by induction on $k$.
(Base Case: $k = 0$)

$$00 = 0 \qquad \text{(IC, } \cdot\text{)}$$

(Inductive Step: Assume true for $k$, prove true for $S(k)$)

$$\begin{aligned} 0 \cdot S(k) &= (0k) + 0 && (\text{RR}, \cdot) \\ &= 0 + 0 && (\text{IH}) \\ &= 0 && (\text{IC}, +) \end{aligned}$$

**Lemma 2.** $1m = m$.

*Proof.* This is a proof by induction on $m$.
(Base Case: $m = 0$)

$$10 = 0 \qquad \text{(IC, } \cdot\text{)}$$

(Inductive Step: Assume true for $m$, prove true for $S(m)$)

$$\begin{aligned} 1 \cdot S(m) &= (1m) + 1 && (\text{RR}, \cdot) \\ &= m + 1 && (\text{IH}) \\ &= S(m) && (\text{Law (a) of Addition}) \end{aligned}$$

**Lemma 3.** (Right distributivity) $(m + n)k = mk + nk$.

*Proof.* This is a proof by induction on $k$.
(Base Case: $k = 0$)

$$\begin{aligned} (m+n)0 &= 0 && (\text{IC}, \cdot) \\ &= 0 + 0 && (\text{IC}, +) \\ &= m0 + n0 && (\text{IC}, \cdot\text{; used twice}) \end{aligned}$$

(Inductive Step: Assume true for $k$, prove true for $S(k)$)

$$\begin{aligned} (m+n) \cdot S(k) &= (m+n)k + (m+n) && (\text{RR}, \cdot) \\ &= (mk + nk) + (m+n) && (\text{IH}) \\ &= mk + (nk + (m+n)) && (\text{Associative Law}, +) \\ &= mk + ((nk + m) + n)) && (\text{Associative Law}, +) \\ &= mk + ((m + nk) + n)) && (\text{Commutative Law}, +) \\ &= mk + (m + (nk + n)) && (\text{Associative Law}, +) \\ &= (mk + m) + (nk + n) && (\text{Associative Law}, +) \\ &= (m \cdot S(k)) + (n \cdot S(k)) && (\text{RR}, \cdot\text{; used twice}) \end{aligned}$$

**Solution to the Problem.**

*Proof.* We prove that $mn = nm$ by induction on $n$.

(Base Case: $n = 0$)

$$\begin{aligned} m0 &= 0 && \text{(IC, }\cdot\text{)} \\ &= 0m && \text{(Lemma 1)} \end{aligned}$$

(Inductive Step: Assume true for $n$, prove true for $S(n)$)

$$\begin{aligned} m \cdot S(n) &= (mn) + m && \text{(RR, }\cdot\text{)} \\ &= (nm) + m && \text{(IH)} \\ &= (nm) + (1m) && \text{(Lemma 2)} \\ &= (n+1) \cdot m && \text{(Lemma 3)} \\ &= S(n) \cdot m && \text{(Law (a) of Addition)} \end{aligned}$$

**Proof 2.**

**Lemma 1*.** $0k = 0$. (This is the same as Lemma 1 from the first proof.)

**Lemma 2*.** $S(n)m = nm + m$

*Proof.* This is a proof by induction on $m$.

(Base Case: $m = 0$)

$$\begin{aligned} S(n)0 &= 0 && \text{(IC, }\cdot\text{)} \\ &= 0 + 0 && \text{(IC, +)} \\ &= n0 + 0 && \text{(IC, }\cdot\text{)} \end{aligned}$$

(Inductive Step: Assume true for $m$, prove true for $S(m)$)

$$\begin{aligned} S(n)S(m) &= (S(n)m) + S(n) && \text{(RR, }\cdot\text{)} \\ &= (nm + m) + S(n) && \text{(IH)} \\ &= (nm + m) + (n+1) && \text{(Law (a) of Addition)} \\ &= ((nm + m) + n) + 1 && \text{(Associative Law, +)} \\ &= (nm + (m + n)) + 1 && \text{(Associative Law, +)} \\ &= (nm + (n + m)) + 1 && \text{(Commutative Law, +)} \\ &= ((nm + n) + m) + 1 && \text{(Associative Law, +)} \\ &= (nm + n) + (m + 1) && \text{(Associative Law, +)} \\ &= (nm + n) + S(m) && \text{(Law (a) of addition +)} \\ &= nS(m) + S(m) && \text{(RR, }\cdot\text{)} \end{aligned}$$

**Solution to the Problem.**

*Proof.* We prove that $mn = nm$ by induction on $n$.

(Base Case: $n = 0$) This part is the same as for Solution 1.

$$\begin{aligned} m0 &= 0 && \text{(IC, }\cdot\text{)} \\ &= 0m && \text{(Lemma 1*)} \end{aligned}$$

(Inductive Step: Assume true for $n$, prove true for $S(n)$)

$$
\begin{aligned}
m \cdot S(n) &= (mn) + m && \text{(RR, } \cdot \text{)} \\
&= (nm) + m && \text{(IH)} \\
&= S(n) \cdot m && \text{(Lemma 2*)}
\end{aligned}
$$