Recall the proof system we examined in class.

**Rule of Sequence:** 
\[
\begin{array}{c}
\{P\} S \{Q\} \\
\{Q\} T \{R\} \\
\{P\} S T \{R\}
\end{array}
\]

**Rule of Consequence:** 
\[
P \text{ implies } Q \\
\{P\} \{Q\}
\]

**Rule of Assignment:** 
\[
\{P \rightarrow E\} x := E ; \{P\}
\]

**Rule of Condition:** 
\[
\{P \land B\} S \{Q\} \\
\{P \land \neg B\} T \{Q\} \\
\{P\} \text{ if } B \text{ then } S \text{ else } T \text{ end if}; \{Q\}
\]

**Rule of Iteration:** 
\[
\{I \land B\} S \{I\} \\
\{I\} \text{ while } B \text{ loop } S \text{ end loop}; \{I \land \neg B\}
\]

Using this proof system, provide a step-by-step partial correctness proof for the following hypothesis. Justify each step with one of the axioms, or “mathematical fact” if the conclusion is algebraically true and involves no assertions. (Your proof may be typed or handwritten; it should not include abbreviations.)

\[
\{x = m \land y = n\} \\
z := 1; \\
\text{while } y \neq 0 \text{ loop} \\
\quad \text{if } y \mod 2 = 0 \text{ then} \\
\qquad x := x \ast x; \\
\qquad y := y / 2; \\
\text{else} \\
\qquad z := z \ast x; \\
\qquad x := x \ast x; \\
\qquad y := (y - 1) / 2; \\
\text{end if}; \\
\text{end loop}; \\
\{z = m^n\}
\]

**Hint:** A good invariant to choose is \(z \cdot x^2 = m^n\).