Homework III

1. [30 points]
It is commonly the case that correctness of programs that stress efficiency is less clear than those employing a direct approach. Since it must be understood informally first, this observation definitely applies when formally proving a program. Provide the partial correctness proof of the program fragment below which uses \(1+N/2\) rather than \(N\) multiplications to compute \(X^N\).

\[
\{N \geq 0\} \\
M := 0; \quad POW := 1; \\
\text{while } 2*M < N-1 \text{ do} \\
\quad \text{begin } M := M+1; \quad POW := POW*X \quad \text{end;}
\]

if \(2*M = N\)
then \(POW := POW*POW\)
else \(POW := POW*POW*X;\)

\(\{POW = X^N\}\)

2. [30 points]
Provide a program fragment \(\phi\) using Diller’s language that always halts for integer values \(N \geq 8\). In words, your program is to compute integer values of variables \(P\) and \(Q\) so that \(N = 3*P+5*Q\) (and of course, not change \(N\)). Employ Diller’s axioms and proof rules to prove the partial correctness of

\[
\text{if } \{N \geq 8\} \\
\phi \quad \{N = 3*P+5*Q\}
\]

3. [10 points]
Suppose that we define the set \((\mathbb{Z}\) is the type of all signed integers) \(\text{PosEven} = \{x: \mathbb{Z} \mid \exists y: \mathbb{Z} \cdot y > 0 \quad x = 2*y\}\) and declare

\[
\begin{align*}
\text{x: } \mathbb{P} \quad \text{PosEven} \\
\text{y: } \text{PosEven} \\
\text{z: } \mathbb{P} \quad \{0,1\} \subset \mathbb{N}_1
\end{align*}
\]

(a) what are the types of \(x, y,\) and \(z\)
(b) which expressions are incorrectly typed and why

\(\begin{align*}
(2,1,3) & \in z \in x \\
2 & \in z \\
\{2\} & \in z \\
\{1,2\} & \in z \\
(0,x) & \in y
\end{align*}\)