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≥0}
M:= 0;  POW:= 1;
   while 2*M<N-1 do
    begin   M:= M+1;   POW:= POW*X   end;
if 2*M=N
   then POW:= POW*POW
   else POW:= POW*POW*X;
    {POW = X^N}
```

2. [30 points]
Provide a program fragment □ using Diller's language that always halts for integer values N≥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

```
      |□  {N ≥ 8}
         □
      {N = 3*P+5*Q}
```

3. [10 points]
Suppose that we define the set ($\mathbb{Z}$ is the type of all signed integers)
PosEven == {x:$\mathbb{Z}$ | □y:$\mathbb{Z}$•y>0 □ x=2*y} and declare
x: $\mathbb{P}$ PosEven y: PosEven □ $\mathbb{Z}$ z: $\mathbb{P}$ ({0,1} □ $\mathbb{N}_1$)
(a) what are the types of x, y, and z
(b) which expressions are incorrectly typed and why
(2,1,3) □ z □ x
2 □ z
{2} □ z
{1,2} □ z
(0,x) □ y