1. We begin the proof by defining the loop invariant, \( P \), used for the while loop
\[
P = \{(0 \leq M \leq \frac{N}{2}) \land (POW = X^M)\}
\]
1) \( \vdash \{N \geq 0\}
\[
M := 0;
\{N \geq 0 \land M = 0\}
\]
by the Axiom of Assignment
2) \( \vdash \{N \geq 0 \land M = 0\}
\[
POW := 1;
\{N \geq 0 \land M = 0 \land POW = 1\}
\]
by the Axiom of Assignment
3a) \( \{N \geq 0 \land M = 0 \land POW = 1\} \Rightarrow \{N \geq 0 \land M = 0 \land POW = X^M\} \)
3b) Through Weakening, we have
\[
\{N \geq 0 \land M = 0\}
\[
POW := 1;
\{(0 \leq M \leq \frac{N}{2}) \land (POW = X^M)\}, which is \( P \)
\]
4) \( \vdash \{N \geq 0\}
\[
M := 0;
POW := 1;
\{P\}
\]
by the Sequential Rule on 1 and 3
We now move on to the while loop
5) \( \vdash \{(0 \leq M \leq \frac{N}{2}) \land (POW \times X = X^M)\}
\[
POW := POW \times X
\{0 \leq M \leq \frac{N}{2}) \land (POW = X^M)\}
\]
by the Axiom of Assignment
6) \( \vdash \{(0 \leq M+1 \leq \frac{N}{2}) \land (POW \times X = X^{M+1})\}
\[
M := M+1;
\{(0 \leq M \leq \frac{N}{2}) \land (POW = X^{M+1})\}
\]
by the Axiom of Assignment
7) \( \vdash \{(0 \leq M+1 \leq \frac{N}{2}) \land (POW \times X = X^{M+1})\}
\[
M := M+1;
POW := POW \times X
\{(0 \leq M \leq \frac{N}{2}) \land (POW = X^M)\}
\]
by the Sequential Rule on 5 and 6
8) \( \{(0 \leq M+1 \leq \frac{N}{2}) \land (POW \times X = X^{M+1})\} \Rightarrow \{P \land (2 \times M < N-1)\} \) by Strengthening, so \( P \) is a valid loop invariant.
9) \( \vdash \{P\}
\[
while 2 \times M < N-1 do
\begin{itemize}
\item \( M := M+1; \)
\item \( POW := POW \times X \)
\end{itemize}
\{P \land \neg (2 \times M < N-1)\}

by 8 and the While Rule

10) \vdash \{N \geq 0\}

M := 0;
POW := 1;
while 2 \times M < N-1 do
begin
    M := M+1;
    POW := POW \times X
end;
\{P \land \neg (2 \times M < N-1)\}

by the Sequential Rule on 4 and 9

11) \{P \land \neg (2 \times M < N-1)\} \Rightarrow \{(2 \times M = N \lor 2 \times M = N-1) \land (POW = X^M)\}

by Strengthening and logical equivalence

12a) \vdash \{2 \times M = N \land POW \times POW = X^N\}

POW := POW \times POW
\{POW = X^N\}

by the Axiom of Assignment

12b) \{2 \times M = N \land POW \times POW = X^N\} \Rightarrow \{2 \times M = N \land POW \times POW = X^{2M}\} \Rightarrow
\{2 \times M = N \land POW = X^M\}

13a) \vdash \{2 \times M \neq N \land POW \times POW \times X = X^N\}

POW := POW \times POW \times X;
\{POW = X^N\}

by the Axiom of Assignment

13b) A simple check of our precondition assures us that if \(2 \times M \neq N\), \(2 \times M = N-1\). Hence,

\vdash \{2 \times M = N-1 \land POW \times POW \times X = X^N\}

POW := POW \times POW \times X;
\{POW = X^N\}

13c) \{2 \times M = N-1 \land POW \times POW \times X = X^N\} \Rightarrow \{2 \times M = N-1 \land POW \times POW \times X = X^{2M+1}\} \Rightarrow
\{2 \times M = N-1 \land POW = X^M\}

14) \vdash \{(2 \times M = N \lor 2 \times M = N-1) \land (POW = X^M)\}

if 2 \times M = N
    then POW := POW \times POW
    else POW := POW \times POW \times X;
\{POW = X^N\}

by the Conditional Rule and logical equivalence

15) \vdash \{N \geq 0\}

M := 0;
POW := 1;
while 2 \times M < N-1 do
begin
    M := M+1;
    POW := POW \times X
end;
if 2 \times M = N
then $POW := POW \times POW$
else $POW := POW \times POW \times X$;

{POW = X^N}
by the Sequential Rule on 11 and 14

2. This is a sample program, and not the only correct one

{N \geq 8}
Q := 1;
P := 1;
while $P \times 3 + Q \times 5 < N$ do
  if $Q > 0$
    then begin
      P := P+2;
      Q := Q-1
    end
  else begin
    P := P-3;
    Q := Q+2
  end

{N = 3 \times P + 5 \times Q}

We will take as our while loop invariant

$P = \{P \times 3 + Q \times 5 \leq N\}$

1) $\vdash \{N \geq 8\}$
   Q := 1
   \{N \geq 8 \land Q = 1\}
   by the Axiom of Assignment and logical equivalence

2) $\vdash \{N \geq 8 \land Q = 1\}$
   P := 1;
   \{N \geq 8 \land Q = 1 \land P = 1\}
   by the Axiom of Assignment and logical equivalence

3) $\vdash \{N \geq 8\}$
   Q := 1;
   P := 1;
   \{N \geq 8 \land Q = 1 \land P = 1\}
   by the Sequential Rule on 1 and 2

4) By logical equivalence, \{N \geq 8 \land Q = 1 \land P = 1\} $\Rightarrow \{P \times 3 + Q \times 5 \leq N\}$

5) $\vdash \{P \times 3 + (Q-1) \times 5 \leq N\}$
   Q := Q-1
   \{P \times 3 + Q \times 5 \leq N\}
   by the Axiom of Assignment

6) $\vdash \{(P+2) \times 3 + (Q-1) \times 5 \leq N\}$
   P := P+2;
   \{P \times 3 + (Q-1) \times 5 \leq N\}
   by the Axiom of Assignment
7) ⊢ \{(P+2)\times 3+(Q-1)\times 5 \leq N\}
    P := P+2;
    Q := Q-1
    \{P\times 3+Q\times 5 \leq N\}
    by the Sequential Rule on 5 and 6

8) By Strengthening and logical equivalence, \{(P+2)\times 3+(Q-1)\times 5 \leq N\} ⇒
    \{P\times 3+Q\times 5+1 \leq N \land Q > 0\}

9) ⊢ \{P\times 3+(Q+2)\times 5 \leq N\}
    Q := Q+2
    \{P\times 3+Q\times 5 \leq N\}
    by the Axiom of Assignment

10) ⊢ \{(P-3)\times 3+(Q+2)\times 5 \leq N\}
     P := P-3;
     \{P\times 3+(Q+2)\times 5 \leq N\}
     by the Axiom of Assignment

11) ⊢ \{(P-3)\times 3+(Q+2)\times 5 \leq N\}
     P := P-3;
     Q := Q+2
     \{P\times 3+Q\times 5 \leq N\}
     by the Sequential Rule on 9 and 10

12) By Strengthening and logical equivalence, \{(P-3)\times 3+(Q+2)\times 5 \leq N\} ⇒
    \{P\times 3+Q\times 5+1 \leq N \land Q \leq 0\}

13) ⊢ \{P\times 3+Q\times 5+1 \leq N\}
    if Q > 0
        then begin
            P := P+2;
            Q := Q-1
        end
    else begin
        P := P-3;
        Q := Q+2
    end
    \{P\times 3+Q\times 5 \leq N\}
    by the Conditional Rule on 8 and 12

14) \{P\times 3+Q\times 5+1 \leq N\} ⇒ \{P \land P\times 3+Q\times 5 < N\} by logical equivalence and Strengthening, so
    P is a valid loop invariant.

15) ⊢ \{P\}
    while P\times 3+Q\times 5 < N do
        if Q > 0
            then begin
                P := P+2;
                Q := Q-1
            end
        else begin
            P := P-3;
        end
Q := Q + 2
end

{P \land \neg (P \times 3 + Q \times 5 < N)}
by the While Rule

16) {P \land \neg (P \times 3 + Q \times 5 < N)} \Rightarrow \{P \times 3 + Q \times 5 \leq N \land P \times 3 + Q \times 5 \geq N\} \Rightarrow \{P \times 3 + Q \times 5 = N\}
by logical equivalence

17) \vdash \{N \geq 8\}
Q := 1;
P := 1;
while P \times 3 + Q \times 5 < N do
if Q > 0
then begin
P := P + 2;
Q := Q - 1
end
else begin
P := P - 3;
Q := Q + 2
end

{N = 3 \times P + 5 \times Q}
by the Sequential Rule on 4 and 16

3a. x: the set of positive even integers
y: the set of ordered pairs (\alpha, \beta) where \alpha \in x and \beta is a signed integer
z: the set of ordered pairs (\alpha, \beta) where \alpha is a boolean (0 or 1) and \beta is a natural number

b. (2, 1, 3) \in z \times x: incorrectly typed, the first number must be a boolean and the last number must be even.
2 \in z: incorrectly typed, z must be an ordered pair.
\{2\} \in z: incorrectly typed, z must be an ordered pair.
\{1, 2\} \in z: incorrectly typed, \{1, 2\} is not an ordered pair.
(0, x) \in y: incorrectly typed, the second element of the ordered pair cannot be a set.