Question 2

(a)

LoopInv: $(j \le N+1) \land (S = 2j(j-1)(2(j-1)+1))$

Proof: That LoopInv is a loop invariant

(1) Let $N \ge 1$ be arbitrary. Assume that pre is true in line 1. Let P(n) be the predicate "if the loop condition is being checked for the n-th time, then LoopInv is true." We will prove $\forall n \ge 1$, P(n).

(2) Base Case: $n = 1$. After line 2 executes j has value 1, and after line 3 executes S has value 0. Thus, $j_1 = 1$ and $S_1 = 0$ when line 5 is reached for the first time.

(3) By the precondition $N \ge 1$, which implies $j_1 \le N+1$. Further, $S_1 = 0$ and $2j_n(j_n-1)(2(j_n-1)+1) = 2(1)(0)(2(0)+1) = 0$. So,

$$S_1 = 2j_1(j_1-1)(2(j_1-1)+1)$$

This proves that LoopInv is true when line 5 is reached for the first time, i.e: P(1) is true.

(4) Induction Step: Let $n > 1$ be arbitrary and assume P(n). That is, assume $j_n \le N+1$ and $S_n = 2j_n(j_n-1)(2(j_n-1)+1)$. We will prove P(n+1), that is,

$$j_{n+1} \le N+1 \land S_{n+1} = 2j_{n+1}(j_{n+1}-1)(2(j_{n+1}-1)+1)$$

(5) Suppose the loop condition is being checked for the n+1st time. Then it was previously checked for the n-th time and evaluated to true. Thus $j_n \le N$. Further, by the inductive hypothesis, LoopInv was true when the loop condition was checked for the n-th time, so $S_n = 2j_n(j_n-1)(2(j_n-1)+1)$.

(6) Within the while-loop, the only line that changes the value of j is line 7, which increments it by 1. So, $j_{n+1} = j_n + 1$. From (5), $j_n \le N$, so, $j_{n+1} = j_n + 1 \le N+1$.

(7) Within the while-loop, line 6 is the only line that changes the value of S, which increases it by $3(2j)(2j) = 12j^2$. From (6), $j_n = j_{n+1} - 1$. So,

$$S_{n+1} = S_n + 12j_n^2$$

$$= 2j_n(j_n-1)(2(j_n-1)+1) + 12j_n^2 \quad by I.H$$

$$= 2(j_{n+1}-1)((j_{n+1}-1)-1)(2((j_{n+1}-1)-1)+1) + 12(j_{n+1}-1)^2$$

$$= 2(j_{n+1} - 1)(j_{n+1} - 2)(2j_{n+1} - 3) + 12(j_{n+1}^2 - 2j_{n+1} + 1)$$

$$= (2j_{n+1} - 2)(2j_{n+1}^2 - 4j_{n+1} - 3j_{n+1} + 6) + 12(j_{n+1}^2 - 2j_{n+1} + 1)$$

$$= 4j_{n+1}^3 - 4j_{n+1}^2 - 14j_{n+1}^2 + 14j_{n+1} + 12j_{n+1} - 12 + 12j_{n+1}^2 - 24j_{n+1} + 12$$

$$= 4j_{n+1}^3 - 6j_{n+1}^2 + 2j_{n+1}$$

$$= 2j_{n+1}(2j_{n+1}^2 - 3j_{n+1} + 1)$$

$$= 2j_{n+1}(2j_{n+1}^2 - 2j_{n+1} - 1j_{n+1} + 1)$$

$$= 2j_{n+1}(2j_{n+1}(j_{n+1} - 1) - 1(j_{n+1} - 1))$$

$$= 2j_{n+1}(2j_{n+1} - 1)(j_{n+1} - 1)$$

$$= 2j_{n+1}(j_{n+1} - 1)(2(j_{n+1} - 1) + 1)$$

as needed. Thus, P(n) $\implies$ P(n+1).

(8) By (6) and (7), P(1) $\wedge$ (P(n) $\implies$ P(n+1)), so, by induction, LoopInv is a loop invariant, specifically stating that

$$(j \leq N + 1) \wedge (S = 2j(j - 1)(2(j - 1) + 1))$$

(b)

Proof: That the program is partially correct

(1) Assume that LoopInv is a loop invariant and that line 8 is reached. We will show that post is true when line 8 is reached.

(2) Since line 8 was reached, the loop condition was checked for a final time and it evaluated to false. So, $j > N \implies j \geq N + 1$ when line 8 is reached. Since LoopInv is a loop invariant, it was true when this final check occurred, so $(j \leq N + 1) \wedge (S = 2j(j - 1)(2(j - 1) + 1))$ when line 8 is reached.

(3) Since $j \geq N+1$ and $j \leq N+1$, it must be true that $j = N+1$. Now,

$$S = 2j(j-1)(2(j-1)+1)$$

$$= 2(N+1)(N+1-1)(2(N+1-1)+1)$$

$$= 2N(N+1)(2N+1)$$

$$= (2N^2+2N)(2N+1)$$

$$= 4N^3+4N^2+2N^2+2N$$

$$= 4N^3+6N^2+2N$$

proving that the post condition is true. Thus, the program is partially correct.