1. Invariant: after iteration i,

1st Iteration: Before the first iteration, . During the first iteration, Thus, after iteration 1, since .

Kth Iteration: Suppose that after the kth iteration. In the iteration, . This polynomial may be factored into , or , which proves that for the iteration.

When , is returned and is correct, since For all other cases, by the loop invariant, after every iteration of the for loop, so after the nth iteration, and thus this function returns whenever the loop iterates.

1. B/C: When , QuickPow returns 1 which is correct, since QuickPow outputs and

I/S: Given some particular but arbitrary value x in n such that , if P(x) is true for all , must be true. must, for any value of k – either even or odd – return

If k is even, then which, under assumption of the induction hypothesis, is equal to . If , QuickPow returns .

If k is odd, then which, under assumption of the induction hypothesis, is equal to . If , QuickPow returns .

Given , it must follow that , for some k .

If is even, then which, under assumption of the induction hypothesis, is equal to . If , QuickPow returns .

If is odd, then which, under assumption of the induction hypothesis, is equal to . If , QuickPow returns .

Therefore, for all values x in n such that , since for all values k and in n, QuickPow returns and , respectively.