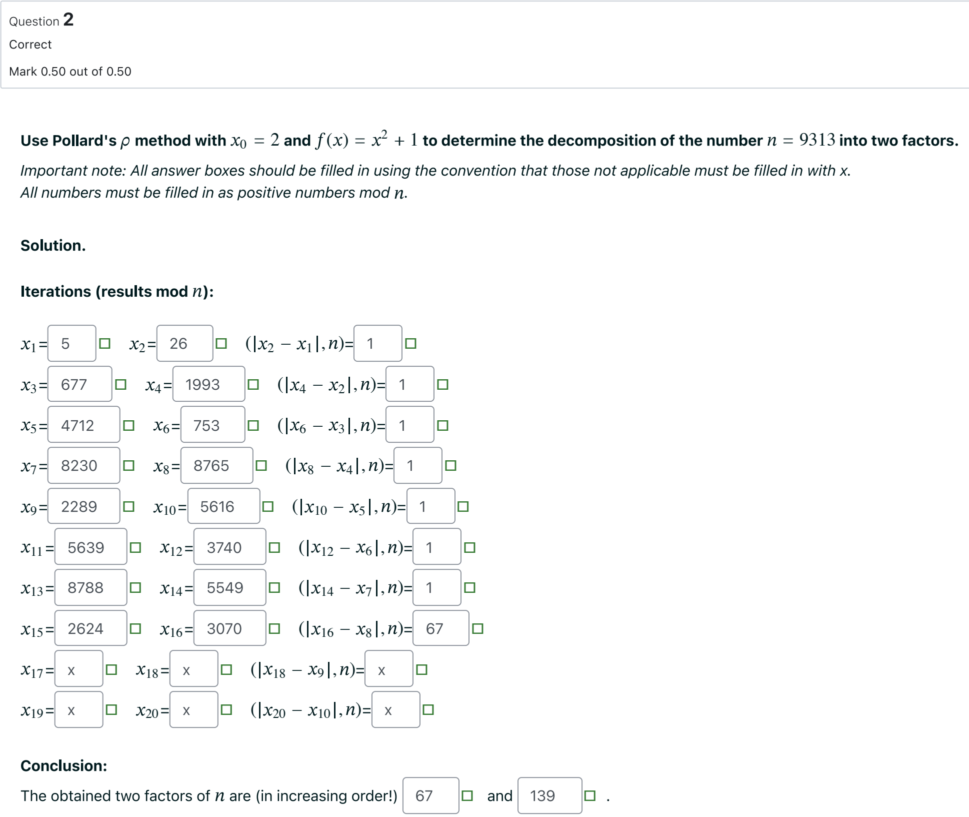

Question **2**

Correct

Mark 0.50 out of 0.50

Use Pollard's ρ method with $x_0 = 2$ and $f(x) = x^2 + 1$ to determine the decomposition of the number $n = 9313$ into two factors.

Important note: All answer boxes should be filled in using the convention that those not applicable must be filled in with x.
All numbers must be filled in as positive numbers mod n.

Solution.

Iterations (results mod n):

x_1= 5 □ x_2= 26 □ $(|x_2 - x_1|, n)$= 1 □

x_3= 677 □ x_4= 1993 □ $(|x_4 - x_2|, n)$= 1 □

x_5= 4712 □ x_6= 753 □ $(|x_6 - x_3|, n)$= 1 □

x_7= 8230 □ x_8= 8765 □ $(|x_8 - x_4|, n)$= 1 □

x_9= 2289 □ x_{10}= 5616 □ $(|x_{10} - x_5|, n)$= 1 □

x_{11}= 5639 □ x_{12}= 3740 □ $(|x_{12} - x_6|, n)$= 1 □

x_{13}= 8788 □ x_{14}= 5549 □ $(|x_{14} - x_7|, n)$= 1 □

x_{15}= 2624 □ x_{16}= 3070 □ $(|x_{16} - x_8|, n)$= 67 □

x_{17}= x □ x_{18}= x □ $(|x_{18} - x_9|, n)$= x □

x_{19}= x □ x_{20}= x □ $(|x_{20} - x_{10}|, n)$= x □

Conclusion:

The obtained two factors of n are (in increasing order!) 67 □ and 139 □ .