Started on	Monday, 14 November 2022, 3:35 PM
State	Finished
Completed on	Monday, 14 November 2022, 4:10 PM
Time taken	34 mins 57 secs
Grade	**1.50** out of 1.50 (**100**%)

Question **1**

Correct

Mark 0.75 out of 0.75

Use Fermat's method to determine the decomposition of the number $n = 6811$ 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.

Solution.

Initialization:

$t_0 = [\sqrt{n}]$= 82 ✔

Iterations:

$t = t_0 + 1$: $t^2 - n$= 78 ✔ perfect square (yes/no) no ✔

$t = t_0 + 2$: $t^2 - n$= 245 ✔ perfect square (yes/no) no ✔

$t = t_0 + 3$: $t^2 - n$= 414 ✔ perfect square (yes/no) no ✔

$t = t_0 + 4$: $t^2 - n$= 585 ✔ perfect square (yes/no) no ✔

$t = t_0 + 5$: $t^2 - n$= 758 ✔ perfect square (yes/no) no ✔

$t = t_0 + 6$: $t^2 - n$= 933 ✔ perfect square (yes/no) no ✔

$t = t_0 + 7$: $t^2 - n$= 1110 ✔ perfect square (yes/no) no ✔

$t = t_0 + 8$: $t^2 - n$= 1289 ✔ perfect square (yes/no) no ✔

$t = t_0 + 9$: $t^2 - n$= 1470 ✔ perfect square (yes/no) no ✔

$t = t_0 + 10$: $t^2 - n$= 1653 ✔ perfect square (yes/no) no ✔

$t = t_0 + 11$: $t^2 - n$= 1838 ✔ perfect square (yes/no) no ✔

$t = t_0 + 12$: $t^2 - n$= 2025 ✔ perfect square (yes/no) yes ✔

$t = t_0 + 13$: $t^2 - n$= x ✔ perfect square (yes/no) x ✔

$t = t_0 + 14$: $t^2 - n$= x ✔ perfect square (yes/no) x ✔

$t = t_0 + 15$: $t^2 - n$= x ✔ perfect square (yes/no) x ✔

$t = t_0 + 16$: $t^2 - n$= x ✔ perfect square (yes/no) x ✔

$t = t_0 + 17$: $t^2 - n$= x ✔ perfect square (yes/no) x ✔

$t = t_0 + 18$: $t^2 - n$= x ✔ perfect square (yes/no) x ✔

$t = t_0 + 19$: $t^2 - n$= x ✔ perfect square (yes/no) x ✔

$t = t_0 + 20$: $t^2 - n$= x ✔ perfect square (yes/no) x ✔

Values:

s= 45 ✔ t= 94 ✔

Conclusion:

The obtained two factors of n are (in increasing order!) 49 ✔ and 139 ✔ .

Question **2**

Correct

Mark 0.75 out of 0.75

Use Pollard's ρ method with $x_0 = 2$ and $f(x) = x^2 + 1$ to determine the decomposition of the number $n = 5539$ 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 $x_4 =$ 4132 $(|x_4 - x_2|, n) =$ 1

$x_5 =$ 2227 $x_6 =$ 2125 $(|x_6 - x_3|, n) =$ 1

$x_7 =$ 1341 $x_8 =$ 3646 $(|x_8 - x_4|, n) =$ 1

$x_9 =$ 5256 $x_{10} =$ 2544 $(|x_{10} - x_5|, n) =$ 1

$x_{11} =$ 2385 $x_{12} =$ 5212 $(|x_{12} - x_6|, n) =$ 1

$x_{13} =$ 1689 $x_{14} =$ 137 $(|x_{14} - x_7|, n) =$ 1

$x_{15} =$ 2153 $x_{16} =$ 4806 $(|x_{16} - x_8|, n) =$ 29

$x_{17} =$ 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!) 29 and 191 .

◄ Assignment A (to submit by Week 8) Jump to... Assignment B (to submit by Week 10) ►