Home / My courses / PKC / Assignment B (Week 6) - max. 1.5 points / Assignment B (to submit by Week 8)

**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 1Use Fermat's method to determine the decomposition of the number n=6811 into two factors. Correct Important note: All answer boxes should be filled in using the convention that those not applicable must be filled in with x. Mark 0.75 out of 0.75 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  $t = t_0 + 16$ :  $t^2 - n =$ ✓ 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: **✓** t= 94 s = 45**Conclusion: ✓** and 139 The obtained two factors of n are (in increasing order!) 49

**\$** 

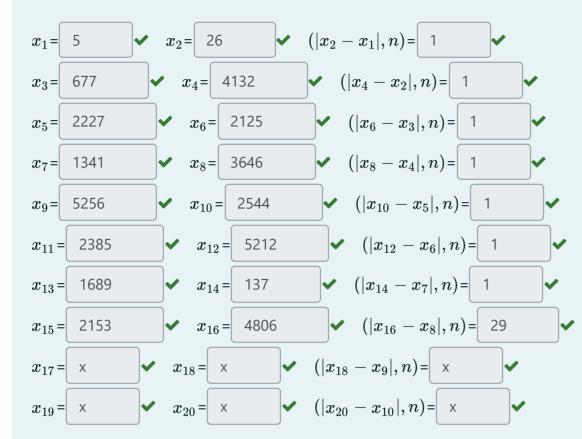
Question **2**Correct
Mark 0.75 out of 0.75

Use Pollard's ho 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 $\operatorname{mod} n$ ):



## **Conclusion:**

The obtained two factors of n are (in increasing order!) 29  $\checkmark$  and 191

→ Assignment A (to submit by Week 8)

Jump to...

Assignment B (to submit by Week 10) ►