<u>Home</u>	/ <u>My co</u>	<u>urses</u>	/ <u>PKC</u>	/ Assignment B (Week 6) - max. 1.5 points	/ Assignment B (to submit by Week 8)
	Started on	ed on Wednesday, 23 November 2022, 11:25 PM			
	State	Finished			
Co	ompleted on	on Wednesday, 23 November 2022, 11:29 PM			
	Time taken	4 mins 29	secs		
	Grade	<b>1.49</b> out	of 1.50 ( <b>99</b> %)		

Question 1

Correct

Mark 0.75 out of 0.75

Use Pollard's  $\rho$  method with  $x_0=2$  and  $f(x)=x^2+1$  to determine the decomposition of the number n=9553 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 x.

#### Solution.

### Iterations (results mod n):

# **Conclusion:**

The obtained two factors of n are (in increasing order!) 41

and

233

Question **2** 

Partially correct

Mark 0.74 out of 0.75

# Use Fermat's method to determine the decomposition of the number n=9231 into two factors.

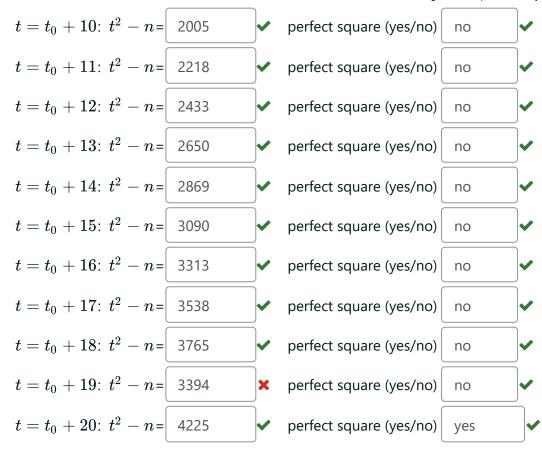
Important note: All answer boxes should be filled in using the convention that those not applicable must be filled in with x.

#### Solution.

#### **Initialization:**

$$t_0 = [\sqrt{n}] = 96$$

### **Iterations:**



### Values:

$$s = 65$$
  $\checkmark$   $t = 116$ 

### **Conclusion:**

The obtained two factors of n are (in increasing order!)  $\boxed{51}$  and  $\boxed{181}$ 

## → Assignment A (to submit by Week 8)

Jump to...

Assignment B (to submit by Week 10) ►