Started on	Tuesday, 8 November 2022, 7:04 PM
State	Finished
Completed on	Wednesday, 9 November 2022, 12:24 AM
Time taken	5 hours 20 mins
Grade	**1.29** out of 1.50 (**86**%)

Question **1**

Partially correct

Mark 0.69 out of 0.75

Use the Miller-Rabin test to decide whether the number $n = 2193$ is prime or not. Check for 3 different bases only if necessary.

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.

Decomposition:

s= 4 ✔ t= 137 ✔ t in binary= 10001001 ✔

Iteration $k = 1$ for $a = 2$ (results mod n):

$2^{(2^0)}$= 2 ✔ $2^{(2^1)}$= 4 ✔ $2^{(2^2)}$= 16 ✔ $2^{(2^3)}$= 256 ✔ $2^{(2^4)}$= 1939 ✔

$2^{(2^5)}$= 919 ✔ $2^{(2^6)}$= 256 ✔ $2^{(2^7)}$= 1939 ✔ $2^{(2^8)}$= x ✔ $2^{(2^9)}$= x ✔

2^t= 1532 ✔ 2^{2t}= 514 ✔ 2^{2^2t}= 1036 ✔ 2^{2^3t}= 919 ✔ 2^{2^4t}= x ✖

Iteration $k = 2$ for $a = 3$ (results mod n):

3^t= x ✔ 3^{2t}= x ✔ 3^{2^2t}= x ✔ 3^{2^3t}= x ✔ 3^{2^4t}= x ✔

Iteration $k = 3$ for $a = 5$ (results mod n):

5^t= x ✔ 5^{2t}= x ✔ 5^{2^2t}= x ✔ 5^{2^3t}= x ✔ 5^{2^4t}= x ✔

Conclusion:

n is prime (yes/no)= no ✔

Question **2**

Partially correct

Mark 0.60 out of 0.75

Use the Miller-Rabin test to decide whether the number $n = 1657$ is prime or not. Check for 3 different bases only if necessary.

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.

Decomposition:

s= 3 ✔ t= 207 ✔ t in binary= 11001111 ✔

Iteration $k = 1$ for $a = 2$ (results mod n):

$2^{(2^0)}$= 2 ✔ $2^{(2^1)}$= 4 ✔ $2^{(2^2)}$= 16 ✔ $2^{(2^3)}$= 256 ✔ $2^{(2^4)}$= 913 ✔

$2^{(2^5)}$= 98 ✔ $2^{(2^6)}$= 1319 ✔ $2^{(2^7)}$= 1568 ✔ $2^{(2^8)}$= x ✔ $2^{(2^9)}$= x ✔

2^t= 874 ✔ 2^{2t}= -1 ✖ 2^{2^2t}= 1 ✔ 2^{2^3t}= 1 ✔ 2^{2^4t}= 1 ✖

Iteration $k = 2$ for $a = 3$ (results mod n):

3^t= 1 ✔ 3^{2t}= 1 ✔ 3^{2^2t}= 1 ✔ 3^{2^3t}= 1 ✔ 3^{2^4t}= 1 ✖

Iteration $k = 3$ for $a = 5$ (results mod n):

5^t= 239 ✔ 5^{2t}= 783 ✔ 5^{2^2t}= -1 ✖ 5^{2^3t}= 1 ✔ 5^{2^4t}= 1 ✖

Conclusion:

n is prime (yes/no)= yes ✔

◄ Lab 2 (Weeks 3-4) - max. 1 point Jump to... Assignment A (to submit by Week 8) ►