Question **1**

Correct

Mark 0.50 out of 0.50

**Use the Miller-Rabin test to decide whether the number $n = 5297$ 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 $t$= 331 $t$ in binary= 0101001011

**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 $2^{(2^4)}$= 1972

$2^{(2^5)}$= 786 $2^{(2^6)}$= 3344 $2^{(2^7)}$= 369 $2^{(2^8)}$= 3736 $2^{(2^9)}$= x

$2^t$= 5296 $2^{2t}$= 1 $2^{2^2t}$= 1 $2^{2^3t}$= 1 $2^{2^4t}$= 1

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

$3^t$= 3253 $3^{2t}$= 3900 $3^{2^2t}$= 2313 $3^{2^3t}$= 5296 $3^{2^4t}$= 1

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

$5^t$= 2044 $5^{2t}$= 3900 $5^{2^2t}$= 2313 $5^{2^3t}$= 5296 $5^{2^4t}$= 1

**Conclusion:**

$n$ is prime (yes/no)= yes

Question **2**

Correct

Mark 0.50 out of 0.50

**Use the Miller-Rabin test to decide whether the number $n = 1513$ 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 $t$= 189 $t$ in binary= 0010111101

**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 $2^{(2^4)}$= 477

$2^{(2^5)}$= 579 $2^{(2^6)}$= 868 $2^{(2^7)}$= 1463 $2^{(2^8)}$= x $2^{(2^9)}$= x

$2^t$= 627 $2^{2t}$= 1262 $2^{2^2t}$= 968 $2^{2^3t}$= 477 $2^{2^4t}$= 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