Prime number homework

Given the brute force prime number function:

isPrime(n)

for i ← 2 to sqrt(n)

if n mod i == 0

return false

end

end

return true

end

How many numbers are tested for

isPrime(36)

isPrime(49)

isPrime(101)

For gcd(3000, 950) the next step is:  
gcd(950, \_\_\_\_\_\_)

and at last:  
gcd(\_\_\_\_\_\_, 0)

For a prime number wheel 2,3,5, show which of the following numbers must be tested for primes:

97 98 99 100 101 102 103 104 105 106

107 108 109 110 111 112 113 114 115 116

117 118 119 120 121 122 123 124 125 126

For Fermat(1001), given a witness a = 2

compute \_\_\_\_\_\_\_\_\_\_\_ = 1 means that

\_\_\_\_\_ is \_\_\_\_\_\_\_\_\_\_\_\_\_ prime.

For Fermat(561), given a witness a = 19

compute \_\_\_\_\_\_\_\_\_\_\_ = 1 means that   
561 is \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

RSA: suppose we pick two random prime numbers: 71 and 89

n = \_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_

e = 17 (a random prime 1 < e << lcm(

d = multiplicative inverse of e =

Miller-Rabin(91)

select random witness a = 65

break p-1 down into d\*2s

d=\_\_\_\_\_\_ s = \_\_\_\_\_\_\_

if ad mod p == 1 or ad mod p = \_\_\_\_\_  
 p is probably prime

repeat \_\_\_\_\_\_ times