Vivek Patel

CSC 440

Assignment 3

* 1. gcd(30030, 257) = gcd(257, 218) = gcd(218, 39) = gcd(39, 23) = gcd(23, 16) = gcd(16, 7) = gcd(7, 2) = gcd(2, 1) = gcd(1, 0) = 1

gcd(30030, 257) = 1

* 1. gcd(30030, 257) = 1 and 30030 = 2 \* 3 \* 5 \* 7 \* 11 \* 13.

gcd(2 \* 3 \* 5 \* 7 \* 11 \* 13, 257) = 1

using the next prime in the list and squaring it, you get 17^2 = 289

289 > 257

Therefore 257 is a prime number.

1. 1. gcd(4883, 4369) = gcd(4369, 514) = gcd(514, 257) = gcd(257, 0) = 257

gcd(4883, 4369) = 257

* 1. 4883 = 257 \* 19 4369 = 257 \* 17

1. If a is divisible by p, then both are 0 (mod p). If a is not divisible by p, then a^(p-1) = 1 (mod p) which means a^p = a (mod p) using Fermat’s Little Theorem.
2. Using Fermat’s Little Theorem, 2^100 = 1 (mod 101)

That means 2^10200 = 1 (mod 101)

2^10203 = 2^3 \* 2^10200 = 8 (mod 101)

1. 100 = 2^5 \* 5^ 2 and ϕ(100) = 100(1 – ½)(1 – 1/5) = 10

123^562 = 123^(562 (mod 10)) = 123^2 = 29 (mod 100)

The last 2 digits are 29.