Assignment # 2 COL 759 (Cryptography & Computer Security)

1. Prove that if $\gcd(a, b) = 1$ and $a|bc$, then $a|c$.
2. Prove that if a number is relatively prime to two numbers, then it is relatively prime to their product.
3. Prove that $\gcd(2^m - 1, 2^n - 1) = 2^{\gcd(m,n)}$
4. Prove that $\gcd(a^2 + m^2, (a-1)^2 + m^2) = 1$ if $\gcd(2a - 1, 4m^2 + 1) = 1$.
5. Prove that for some positive integer n, if 2^n -1 is prime, then n is also prime.
6. Prove that for primes p of the form $4k + 3$, p divides $(a^2 + b^2)$ if and only if p divides a and p divides b. Also justify that this property not shared by $p = 2$ and by primes of the form $4k + 1$.
7. Find three consecutive positive integers which are not square-free. A number n is said to be square-free if it is not divisible by m^2 for any $m > 1$. (Hind: Use Chinese Remainder Theorem)
8. Find a primitive root of the prime 13.
9. Find the least non-negative residue of $19! + (13!)^{44}$ mod 23.
10. Find φ(125). Let $N = 3^{10!} - 1$. Is N divisible by 125? Justify your answer and state any theorems that you use.
11. Let g be a primitive root modulo 29.
    - (i) How many primitive roots are there modulo 29?
    - (ii) Find a primitive root g modulo 29.
    - (iii) Use g mod 29 to find all the primitive roots modulo 29.
    - (iv) Use the primitive root g mod 29 to express all the quadratic residues modulo 29 as powers of g.
    - (v) Find all the quadratic residues modulo 29, and all the quadratic non-residues modulo 29.
    - (vi) Is 5 a quadratic residue modulo 29? If so, is 5 congruent to a fourth power modulo 29?
    - (vii) Use the primitive root g mod 29 to calculate all the congruence classes that are congruent to a fourth power.
    - (viii) Show that the equation $x^4 - 29y^4 = 5$ has no integral solutions.
12. Simplify 146! (mod 149) to a number in the range {0, 1, 2, ..., 148}.