Math 115A Homework 8

1) Let n and k be positive integers. Prove that $\phi(n^k) = n^{k-1} \cdot \phi(n)$.

2) Let $n \in \mathbb{Z}$ with $n > 1$. Prove that the sum of all positive integers k with $1 \le k < n$ and $(k, n) = 1$ is $\frac{1}{2} n\phi(n)$.

3) Consider the RSA encryption scheme with public key $N = 3127, e = 9$.

a) Encode the message SEND ENVOY TODAY.

b) Decode the message 2490 769 2502 978 428 1142 1210 2417 2778.

4) Assume all notation in the RSA encryption and decryption schemes from class. Show that the decryption scheme $C^d \equiv P \pmod{N}$ given the encryption scheme $P^e \equiv C \pmod{N}$ still works even if $(P, N) \neq 1$. *(Hint: if $N = pq$, prove that $C^d \equiv P \pmod{p}$ and $C^d \equiv P \pmod{q}$)* A reminder: N and e are the public keys, d is the multiplicative inverse of e modulo $\phi(N)$, and P is the message that needs to be encoded.

5) Assume all notation in the RSA encryption scheme from class (see problem 4 for a refresher).

a) Prove that the primes p and q such that $N = pq$ are easily found if both N and $\phi(N)$ are known.

b) Find p and q if $N = 176399$ and $\phi(N) = 175560$.

c) Find p and q if $N = 551923$ and $\phi(N) = 550368$.

6) Decide whether each of the following sequences is super-increasing.

a) 3,5,9,19,40

b) 2,6,10,15,36

c) 3,7,17,30,59

d) 11,21,41,81,151

7) Find all subsets of the integers 2,3,4,7,11,13,16 that have 18 as their sum.

8) Encrypt the message GO AGGIES using the knapsack cipher based on the sequence 17,19,37,81,160, by performing modular multiplication with multiplier $w = 29$ and modulus $m = 331$.

9) How difficult was this homework? How long did it take?