Dr. Z.'s Number Theory Homework assignment 16

Version of Oct. 31, 2013 [PLEASE DISREGARD EARLIER VERSION]

1. Check Euler's theorem for (**a.**) $n = 15$ (**b.**) $n = 24$ (**c.**) $n = 21$

2. For the following primes p and q (let $n = pq$) public key e, and encrypted message c

(i) Check that e is an OK key, i.e. that it is coprime to $\phi(n)$.

(ii) Find the deciphering key, d, such that $de \equiv 1 \pmod{\phi(n)}$

(iii) Suppose Alice sent you the encrypted message c. Check that this is an OK message (coprime to n), and if it is find her original message?, m

a. $p = 11 \quad , \quad q = 7 \quad , \quad e = 7 \quad , \quad c = 20$

b. $p = 11 \quad , \quad q = 5 \quad , \quad e = 9 \quad , \quad c = 19$

c. $p = 3 \quad , \quad q = 13 \quad , \quad e = 7 \quad , \quad c = 16$

d. $p = 7 \quad , \quad q = 17 \quad , \quad e = 5 \quad , \quad c = 11$

e. $p = 7 \quad , \quad q = 17 \quad , \quad e = 3 \quad , \quad c = 11$

f. $p = 7 \quad , \quad q = 17 \quad , \quad e = 5 \quad , \quad c = 17$

3. State and prove Euler's Theorem.