Homework Problems : Algebra and Number Theory

1. Study the Division Algorithm and the Euclidean Algorithms in details, and solve the following.

   A. Prove that the Euclidean Algorithm to find gcd(a,b) halts, and that the value of gcd(a,b) is the last non-zero remainder generated in the process of executing the Euclidean Algorithm.

   B. Prove that for any two positive integers a, b, with gcd(a,b) = d, there exist integers x, y such that $ax + by = d$. Devise an algorithm to obtain x, y given a, b.

2. If a, b are co-prime to a positive integer n, show that (ab mod n) is also co-prime to n.

3. Given that phi(nm) = phi(n) phi(m) for co-prime integers n, m, where phi is the Euler totient function, prove that phi(n) = n (1 - 1/p_1) (1 - 1/p_2) … (1 - 1/p_k) for $n = p_1^{a1} p_2^{a2} \cdots p_k^{ak}$. Prove the same result using the principle of inclusion-exclusion.

4. Generalize the Chinese Remainder Theorem for multiple moduli m_1, m_2, …, m_k, where $k > 2$.

5. Show that the number of quadratic resides modulo p is (p-1)/2, where p is a prime.

6. Construct a complete proof (both directions) of the Euler's criterion : a in Z_p^* is a quadratic residue modulo p if and only if $a^{(p-1)/2} = 1$ modulo p.