

Cryptography Assignment 2

1. Show that Euclid's algorithm gives the GCD quickly by showing the following. Assume that Euclid's algorithm on inputs m and n give the output a .
 - (a) Show a divides both m and n .
 - (b) If d divides both m and n then d divides a .
 - (c) Show that in each step of the algorithm the largest number shrinks by at least half its value. Specifically show that if $a < b$ then $b \bmod a \leq \frac{b}{2}$.

2. Let $\phi(n)$ be the number of $m < n$ relatively prime to n .
 - (a) Show that if p is prime then $\phi(p^r) = p^{r-1}(p-1)$.
 - (b) Show that if a and b are relatively prime then $\phi(ab) = \phi(a)\phi(b)$. Hint: Use the Chinese remainder theorem.
 - (c) Conclude that if $m = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ for distinct primes p_1, \dots, p_k then
$$\phi(m) = (p_1 - 1)p_1^{r_1-1}(p_2 - 1)p_2^{r_2-1} \cdots (p_k - 1)p_k^{r_k-1}.$$

3. Let p be prime with $p \equiv 3 \pmod{4}$. Show that there are no x with $x^2 \equiv -1 \pmod{p}$. Hint: Use Fermat's little theorem.

4. The order of $a \bmod n$ is the smallest $r > 0$ such that $a^r \equiv 1 \pmod{n}$. Show that the order of a always divides $\phi(n)$.