Cryptography

Problem set 6 - 8-9 V 2013

Problem 1 Let $a \in \mathcal{Z}$, $n \in \mathcal{N}$, $n \geq 2$, and $gcd(a, n) = 1$. Show that if $(X+a)^n = X^n + a(\mathrm{mod}\, n)$ then n is prime.

Problem 2 Let $a \in \mathcal{Z}$, $n \in \mathcal{N}$, $n \geq 2$, and $gcd(a, n) = 1$. Show that if n is prime then $(X+a)^n = X^n + a(\mathrm{mod} n)$.

Problem 3 Definition 1: Let $f(X) = g(X)(\mathrm{mod} h(X), n)$ denote that $f(X) = f_h(X)h(X) + r_f(X)$ and $g(X) = g_h(X)h(X) + r_g(X)$ and corresponding coefficients of $r_f(X)$ and $r_g(X)$ are equal modulo n.

Definition 2: For a polynomial $f(X)$ and a number $m \in \mathcal{N}$ we say that m is *introspective* for $f(X)$ if:

$$[f(X)]^m = f(X^m)(\mathrm{mod} X^r - 1, n).$$

Let p, q be introspective numbers for $f(X)$, show that so is pq.

Problem 4 Let $LCM(m)$ denote the least common multiply of first m numbers. Show that for $m \geq 7$: $LCM(m) \geq 2^m$.

Problem 5 Show that if r is a prime number such that $gcd(r, n) = 1$ and if

$$(X-1)^n = X^n - 1(\mathrm{mod} X^r - 1, n)$$

then either n is prime or $n^2 = 1 \bmod r$.