HIT — Cryptography — Homework 5

September 4, 2014

Problem 1. This question concerns the Euler phi function.

1. Let p be a prime and $e \geq 1$ an integer. Show that $\phi(p^e) = p^{e-1}(p-1)$.
2. Let p, q be relatively prime. Show that $\phi(pq) = \phi(p) \cdot \phi(q)$. (You may use the Chinese remainder theorem.)
3. Prove Theorem: $N = \prod_i p_i^{e_i}$, $\{p_i\}$ are distinct primes, $\phi(N) = \prod_i p_i^{e_i - 1}(p_i - 1)$.

Problem 2. Solve the following system of congruences (find x by hand):

$$13x \equiv 4 \pmod{99}, \qquad 15x \equiv 56 \pmod{101}$$

Problem 3. Compute $[101^{4,800,000,023} \bmod 35]$ (by hand).

Problem 4. Let $N = pq$ be a product of two distinct primes. Show that if $\phi(N)$ and N are known, then it is possible to compute p and q in polynomial time.