Homework Set 9

Due: April 4, 2011

1. Prove Proposition B.2 in the textbook.

2. Let p be a prime number, and let $r \geq 1$. Prove that if $p \nmid m$, then $m^{(p-1)p^{r-1}} \equiv 1 \pmod{p^r}$. (*Hint:* Use Corollary 6.36 and induction on r.)

Problems 3–5 all have the following setup: Let p and q be two *different* prime numbers. Let $n = pq$, and let $f = (p-1)(q-1)$.

3. Prove that if $m \equiv 1 \pmod{p}$ and $m \equiv 1 \pmod{q}$, then $m \equiv 1 \pmod{n}$. Also, give a counterexample to show that this is false if $p = q$.

4. Prove that if neither p nor q divides m, then $m^f \equiv 1 \pmod{n}$. (*Hint:* This is related to Fermat's Little Theorem. You may need to use Corollary 6.36 and the previous question.)

5. Assume that $e, d \in \mathbb{N}$ are such that $ed \equiv 1 \pmod{f}$. Assume that neither p nor q divides m, and let $M = m^e \pmod{n}$. (*Note:* This unfortunate notation means "let M be the remainder when you divide m^e by n." Pay attention to the difference between $=$ and $\equiv$; they're closely related but different.) Prove that $M^d \equiv m \pmod{n}$.

How RSA works: You pick two different prime numbers, p and q. As above, let $n = pq$ and $f = (p-1)(q-1)$. You also find two numbers e and d such that $ed \equiv 1 \pmod{f}$. (See below.) You publicly announce n and e, and keep p, q, and d secret.

When someone wants to send you a secret message m, they compute $M = m^e \pmod{n}$, and they send you that number. M is the *encrypted message*. You decrypt it by computing M^d; Problem 5 above tells you that you get back m when you do that.

How do you find e and d? You pick any e such that $\gcd(e, f) = 1$, and then you compute d using a procedure called the *extended Euclidean algorithm*. The point is that you need to know p and q to carry out that procedure. Your adversaries will know n and e, but they can't compute d on their own unless they know how to factor n.

6. Pick some specific numbers and work out an example. (No proofs for this question.)

7. (Bonus) Euler's Theorem: Let $n \in \mathbb{N}$. Write its prime factorization in the form

$$n = \prod_{i=1}^{r} p_i^{k_i} = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r},$$

where $p_1, p_2, \ldots, p_k$ are *distinct* primes. Let

$$f = \prod_{i-1}^{r} (p_i - 1)p_i^{k_i - 1} = (p_1 - 1)p_1^{k_1 - 1}(p_2 - 1)p_2^{k_2 - 1} \cdots (p_r - 1)p_r^{k_r - 1}.$$

Prove that if $\gcd(m, n) = 1$, then $m^f \equiv 1 \pmod{n}$. (This statement is a generalization of Fermat's Little Theorem and Problems 2 and 4 above. To prove it, you'll need to do induction on the number of prime factors in n.)