347 PROBLEM SET 8, FALL 2006

DUE MONDAY, NOVEMBER 10

(1) (0 points) In-class practice: Go carefully through the solutions to the questions you couldn't answer in your first midterm. Especially the set-theoretic stuff will be on there again. Practice some similar things.

Remember also what the negation of $A \Rightarrow B$ is. Practice finding multiplicative inverses in $\mathbb{Z}/m\mathbb{Z}$ using the Euclidean algorithm. Practice modular arithmetic in general, remembering that it is always a good idea to take the remainder mod m as soon as you can.

(2) (10 points) State *cleanly* the statement of Fermat's little theorem. Compute (without using it or your calculator) $5^{10} \mod 11$, $7^{12} \mod 13$, and $2^{17} \mod 17$.

(3) Let p and q be prime numbers. Set $n = p \cdot q$ and

$$m = (p-1) \cdot (q-1).$$

Let e be a natural number such that e and m share no common factors. You are allowed to use the fact, discussed in class, that under these conditions, there are positive integers d and y such that

$$ed = 1 + my.$$

Let now W be a non-negative integer less then n. Let C be the remainder if W^e is divided by n.

(a) (9 points) In the example $p = 3$ and $q = 5$, compute m, and then find (by trial and error if necessary) possible values for e and d.

(b) (7 points) Stick with the values for e, d and y you chose in part (a). Starting with $W = 8$, compute C and C^d and the remainder of C^d if divided by n. Then do the same for $W = 7$.

Date: November 3, 2006.

(c) (9 points) Let a and k be a natural numbers, and let b be an integer. Prove: if r is the remainder of b modulo a then the remainder of b^k modulo a equals the remainder of r^k modulo a.

(d) (25 points) Use Fermat's little theorem to prove that for any values of p, q and e satisfying the above conditions, the remainder of C^d modulo n is W.

(4) (40 points) Explain in your own words how RSA-codes (public-key codes) work.

(a) Who sends what to whom?

(b) What is secret, what is public?

(c) Why does Problem (1) prove that this works?

(d) Why is it possible to encode and decode something reasonably quickly?

(e) Why is it so much harder to break the code?

(f) Given p and q, how would you systematically compute d and e?