Math 437/537 Homework #3

due Friday, October 10, 2008 at the beginning of class

I. Let p be an odd prime, and write $p - 1 = 2^k q$ where q is odd. Suppose a is a quadratic nonresidue modulo p. Prove that $a^{2^j q}$ has order exactly 2^{k-j} modulo p for every $0 \le j \le k$.

II. Niven, Zuckerman, and Montgomery, Section 3.2, p. 141, #15. (Hint: use problem I.)

III. Niven, Zuckerman, and Montgomery, Section 3.2, p. 141, #16. (Hint: use problem I.)

IV. Let p and q be primes, let k be a positive integer, and let a and b be reduced residues modulo p. Suppose that both a and b have order q^k modulo p. Prove that exactly $q - 2$ of the numbers ab, ab^2, $\dots$, ab^{q-1} have order q^k modulo p.

V. Niven, Zuckerman, and Montgomery, Section 3.2, p. 141, #18

VI. Let $g(x) = x^6 - 53x^4 + 680x^2 - 1156 = (x^2-2)(x^2-17)(x^2-34)$. Show that $g(x) = 0$ has solutions in the real numbers and that $g(x) \equiv 0 \pmod{m}$ has solutions for every modulus m, but that $g(x) = 0$ has no solutions in the rational numbers. (Hint: when m equals a power of 2, note that $x = 1$ is a solution modulo 8; use Theorem 2.24.)

[Context: For a polynomial equation with integer coefficients to have a rational solution (a "global" solution), it's clearly *necessary* for it to have both a real solution and a solution modulo m for every m ("local" solutions); this problem shows that existence of these local solutions isn't *sufficient* in general.]

VII. Hint: look for short solutions to these problems!
(a) Niven, Zuckerman, and Montgomery, Section 3.2, p. 141, #14
(b) Niven, Zuckerman, and Montgomery, Section 3.3, p. 148, #14

VIII. Niven, Zuckerman, and Montgomery, Section 3.2, p. 141, #19

IX. Niven, Zuckerman, and Montgomery, Section 2.4, p. 83, #19. Do not use the fact that there are infinitely many Carmichael numbers.

X. Niven, Zuckerman, and Montgomery, Section 2.5, p. 86, #2

XI. The following message was encrypted using the RSA encryption scheme using the public key $n = 99407207$, $e = 51082705$:

79033274, 43938308, 3682551, 67435692, 76389994, 79201196

Break the code to read the message. You may use a computer to do your calculations; just tell me what computations you performed.

(continued on next page)

XII. (Alice and Bob are talking on the phone and want to flip a coin so that each has a 50% chance of winning, but they're afraid that someone might cheat if they flip an actual coin.) The following protocol is often referred to as "flipping coins over the telephone":

1. Alice finds two large primes p and q that are both congruent to 3 (mod 4). She keeps them secret but tells Bob the product $n = pq$.
2. Bob chooses a random number x and computes $y \equiv x^2 \pmod{n}$. He keeps x secret and tells y to Alice.
3. Alice computes all the square roots of y modulo n. She chooses one at random, z, and tells it to Bob.
4. At this point, if Bob can tell Alice what the primes p and q are, he wins the coin flip; otherwise, he concedes the coin flip to Alice.

Discuss why this is a reasonable protocol to simulate a coin flip—that is, discuss why Alice and Bob each have about a 50% chance of winning. (Are the chances of winning exactly 50% for both players, or does one have a tiny advantage?) Explain whether or not all of the calculations involved can be done in polynomial time.