Math 432/537 Homework #3

due Friday, October 18, 2002 at the beginning of class

I. Niven, Zuckerman, and Montgomery, Section 2.4, p. 83, #19

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

III. Niven, Zuckerman, and Montgomery, Section 3.1, p. 137, #20

IV. Niven, Zuckerman, and Montgomery, Section 3.2, p. 141, #15

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

55853011, 45722978, 14492772, 72285991, 13737652

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

VI. Determine the number of solutions to the congruence $22x^2 + 10x + 35 \equiv 0 \pmod{p}$ for each of the primes $p = 103$, $p = 149$, and $p = 227$. Show your calculations for this problem.

VII. Determine whether 5 is a quadratic residue or nonresidue modulo 771. Then calculate the least nonnegative residue of $5^{(771+1)/4} \pmod{771}$. How do your results relate to the discussion in the last paragraph of Niven, Zuckerman, and Montgomery, page 110?

VIII. 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 $g(x) \equiv 0 \pmod{p}$ has solutions for every prime p, but that $g(x) = 0$ has no solutions in the rational numbers. (*Bonus question*: show that $g(x) \equiv 0 \pmod{m}$ has solutions for every positive integer m. This shows, essentially, that a polynomial can have roots in every "local field" without having solutions in the rationals.)

IX. Find a single polynomial $f(x)$ with integer coefficients such that the congruence $f(x) \equiv 0 \pmod{5}$ has exactly two solutions, the congruence $f(x) \equiv 0 \pmod{7}$ has exactly one solution, and the congruence $f(x) \equiv 0 \pmod{11}$ has no solutions.

X. Let m be a positive integer and let a and b be relatively prime to m. Suppose that the order of a modulo m is h and that the order of b modulo m is k. Determine the possible orders of ab modulo m, in terms of h, k, and (h, k). Demonstrate that your possibilities actually arise.

XI. Let n be a positive integer and let a be relatively prime to n. Suppose that $a^{n-1} \equiv 1 \pmod{n}$ and that, for every prime factor p of $n - 1$, we have $a^{(n-1)/p} \not\equiv 1 \pmod{n}$. Prove that n is prime. Does this give rise to a polynomial-time algorithm for testing whether n is prime?

XII. Suppose that p and q are twin primes, i.e., p and q are both primes and $q = p + 2$. Prove that there is an integer m such that $p \mid (m^2 - 2)$ if and only if there is an integer n such that $q \mid (n^2 + 2)$.

XIII. Prove that for any positive integer k, there exist k consecutive integers *none* of which are square-free. What is the largest integer k such that there exist k consecutive integers that *are* square-free?

XIV. (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. Are the chances of winning exactly 50% for both players or does one have a slight advantage? Can all of the calculations involved be done in polynomial time?