Math 573 Problem Set 4

1. Pick numbers so that I can send you an encoded message using the RSA system. Send me an e-mail with those numbers. You will be sent an encoded question. Decode the question, figure out the answer, then e-mail me the answer back encoded using the numbers I sent you with the e-mail. You must allow 24 hours for each response to your e-mail. In other words, don't wait until the morning this is due to send me your numbers. This problem is worth 15 points.

2. Let p be an odd prime and let $a \in \mathbb{Z}$ with $p \nmid a$. Prove that if the congruence $x^2 \equiv a \pmod{p^j}$ has a solution when $j = 1$, it has a solution for all j.

3. Let n be a positive integer with prime factorization given by

$$n = 2^a \prod_{p \equiv 1 \pmod 4} p^b \prod_{q \equiv 3 \pmod 4} q^c.$$

Prove that n can be expressed as the sum of two squares of integers if and only if all the exponents c are even. (Hint: The identity $(r^2+s^2)(t^2+u^2) = (at-su)^2 + (au-st)^2$ may be helpful.)

4. For which values of n is $\phi(n)$ odd?

5. Let m and n be positive integers and set $d = \gcd(m,n)$. Prove that

$$\phi(mn) = d\,\frac{\phi(m)\phi(n)}{\phi(d)}.$$

6. In this problem you will prove that if $f(x) = a_n x^n + \cdots + a_1 x + a_0$ with $p \nmid a_n$ for p a prime, then congruence $f(x) \equiv 0 \pmod p$ has at most n solutions by induction on n.

(a) State and prove the base cases of $n = 0$ and $n = 1$.

(b) State your inductive hypothesis for $0 \le n \le N-1$. Let $f(x) = a_N x^N + \cdots + a_1 x + a_0$ be such that $p \nmid a_N$ and $f(x) \equiv 0 \pmod p$ has solutions $\alpha_1, \ldots, a_{N+1}$ with $\alpha_i \not\equiv \alpha_j \pmod p$ if $i \neq j$. Consider the polynomial $g(x) = f(x) - a_N(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_N)$. Observe that $g(x) \equiv 0 \pmod p$ has at least N solutions. What are they?

(c) We now break into 2 cases. Case 1: Suppose every coefficient of $g(x)$ is divisible by p. Use this to reach a contradiction.

(d) Case 2: Suppose there is at least one coefficient of $g(x)$ that is not divisible by p. Use this to reach a contradiction.

(e) State the conclusion of your induction.

7. Let Y be the coded form of a message that was encoded by using the RSA alogrithm. Suppose that you discover that Y and the encoding modulus n are not relatively prime. Explain how you could factor n and thus find the decoding algorithm. (Note that the probability of such a Y occurring is less then 10^{-99} for prime factors p, q of n having more then 100 digits.)

8. For m odd, prove that the sum of the elements of any complete residue system modulo m is congruent to 0 modulo m. Prove that if $m > 2$, the sum of the elements of any reduced residue system is congruent to 0 modulo m.

9. Prove that the positive integer n has as many representations as a sum of two squares as does the integer $2n$.

10. Prove that a positive integer is representable as the difference of two squares if and only if it is the product of two factors that are both even or both odd.