Exam 1, Math 401
Tuesday, September 25

Problem 1. a) State Fermat's Little Theorem and Euler's Theorem.

b) Let m, n be relatively prime positive integers. Prove that

$$m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn} .$$

Problem 2. a) State Chinese Remainder Theorem.

b) Find all positive integers smaller than 200 which leave remainder $1, 3, 4$ upon division by $3, 5, 7$ respectively.

Problem 3. a) Define $\gcd(a, b)$. Using Euclid's algorithm compute $\gcd(889, 168)$ and find $x, y \in \mathbb{Z}$ such that $\gcd(889, 168) = x \cdot 889 + y \cdot 168$ (check your answer).

b) Let a be an integer. Prove that $\gcd(3a + 5, 7a + 12) = 1$. **Hint:** If $d|u$ and $d|w$ then $d|su + tw$ for any integers s, t.

Problem 4. a) Define prime numbers. State the Fundamental Theorem of Arithmetic. Explain the notation: $p^k||m$.

b) Let $n = p_1^{a_1} p_2^{a_2} ... p_s^{a_s}$, where $p_1 < p_2 < ... < p_s$ are prime numbers. Prove that n is a perfect square (i.e. $n = m^2$ for some integer m) iff $a_1, a_2, ..., a_s$ are all even.

c) Suppose that $k \cdot l$ is a perfect square and $\gcd(k, l) = 1$. Prove that both k and l are perfect squares.

Problem 5. a) Define quadratic residues and non-residues modulo a prime p. Find all quadratic residues modulo 11.

b) Suppose that $n = a^2 + b^2$ for some integers a, b. Prove that $n \not\equiv 3 \pmod{4}$.

****

****

The following problems are optional. You may earn extra points, but work on these problems only after you are done with the other problems

Problem 6. Prove that $n^{21} \equiv n \pmod{30}$ for every integer n.

Problem 7. Let $a > 1$, $n > 1$ be integers.

a) What is the order of a modulo $a^n + 1$?

b) Prove that $2n | \phi(a^n + 1)$.