Math 437/537 Homework #4

due Monday, October 27, 2008 at the beginning of class

I. Find all solutions of the equation $x^2 + y^4 = z^2$ in positive integers x, y, z that satisfy $(x, y, z) = 1$.

II. Let $g(x, y) = x + 2x^2 + 3x^3 + 3y + y^3$.

(a) Two points such that $g(x, y) = 10$ are $(1, 1)$ and $(-3, 4)$. Find a third point (u, v) with rational coordinates such that $g(u, v) = 10$ by considering the line passing through the first two points.

(b) Find two points (u, v) with rational coordinates such that $g(u, v) = 0$. One such point should be obvious; find the second by considering the tangent line to the curve $g(x, y) = 0$ passing through the first point.

III. (a) Niven, Zuckerman, and Montgomery, Section 5.4, p. 240, #10

(b) Niven, Zuckerman, and Montgomery, Section 5.6, p. 260, #5. In addition, find two nonzero rational numbers x, y such that $y^2 = x^3 + 2x^2$ and both $|x|$ and $|y|$ are less than $\frac{1}{100}$.

IV. (a) Find the smallest number n such that there are exactly 48 ordered pairs (a, b) of integers with $a^2 + b^2 = n$.

(b) Find all numbers n such that $\phi(n) = 120$.

V. Both parts of this problem have very short solutions, although they can be tricky to find.

(a) Prove that for every number n, there is a number x such that $\tau(nx) = n$.

(b) Let n_0 be a positive composite number, and for each $j \geq 1$ let $n_j = \tau(n_{j-1})$. Prove that some n_j is a perfect square.

VI. Show that $\sigma(n) = \sum_{d|n} \phi(d)\tau(n/d)$ for every positive integer n.

VII. Suppose that m and n are positive, squarefree integers that satisfy $n\phi(m) = m\phi(n)$. Prove that $m = n$.

VIII. Define $f(n) = \sum_{d|n} \phi\big((d, n/d)\big)$ for all numbers n. (That's the Euler phi-function applied to a gcd.)

(a) Prove carefully that f is a multiplicative function.

(b) Prove that there exist multiplicative functions g and h such that $f(n) = \sum_{d|n} g(d)$ and $g(n) = \sum_{d|n} h(d)$. Furthermore, prove that for this function h, we have $h(n) \neq 0$ if and only if n is a perfect square such that $2^2 \nmid n$.

IX. The largest perfect number known today is $N = 2^{p-1}(2^p - 1)$, where $p = 43{,}112{,}609$. Determine how many digits N has, and find the first three digits (on the left) and the last three digits (on the right). You may use a calculator to do arithmetic; just indicate what calculations you did. Do not evaluate N directly.

(continued on next page)

X. Consider the following four quadratic forms of discriminant -120:

$$e(x,y) = x^2 + 30y^2 \qquad f(x,y) = 2x^2 + 15y^2$$
$$g(x,y) = 3x^2 + 10y^2 \qquad h(x,y) = 5x^2 + 6y^2$$

It turns out that a product of any two of them can be written as a value of one of the four forms: for example,

$$e(a,b)e(c,d) = e(ac - 30bd, bc + ad). \tag{1}$$

(a) Find similar product formulas for $e(a,b)f(c,d)$ and $g(a,b)g(c,d)$ and $g(a,b)h(c,d)$.

(b) Write out a "multiplication table" for the four forms e, f, g, h. You don't have to work out all the exact formulas like you did in part (a); just record which forms arise from which products. For example, the entry for $e \times e$ will be "e" because of the identity (1).

DEFINITIONS AND BACKGROUND. When n is a positive integer, a *primitive nth root of unity* is a complex number of the form $e^{2\pi ik/n}$ where $(k,n) = 1$. Equivalently, a primitive nth root of unity is a complex number z such that $z^n = 1$ but $z^m \neq 1$ for any $0 < m < n$ (in other words, an "element of order n" in the field of complex numbers). Define the *nth cyclotomic polynomial* $\Phi_n(x)$ to be the polynomial whose roots are precisely the $\phi(n)$ primitive nth roots of unity. For example, $\Phi_6(x) = (x - e^{\pi i/3})(x - e^{5\pi i/3}) = x^2 - x + 1$.

It turns out that Φ_n has integer coefficients and is irreducible over the integers. (You don't have to prove either of these assertions, although you should be able to verify the first assertion using your knowledge of graduate-level algebra. The proof of the second assertion isn't that hard, but it does require a little cleverness as well as some knowledge of algebraic number theory, so you might want to look up a proof for your own edification.) Because it has integer coefficients, we can just as well consider $\Phi_n(x)$ as a polynomial (mod m) for any positive integer m (although it may or may not remain irreducible when considered modulo m).

XI. (a) Prove that

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}.$$

For example, $\Phi_6(x) = (x-1)^1(x^2-1)^{-1}(x^3-1)^{-1}(x^6-1)^1 = x^2 - x + 1$.

(b) Define the *von Mangoldt Lambda-function*

$$\Lambda(n) = \begin{cases} \ln p, & \text{if } n = p^r \text{ with } p \text{ prime and } r \geq 1, \\ 0, & \text{otherwise.} \end{cases}$$

So for example, $\Lambda(125) = \ln 5$. Prove the two identites

$$\sum_{d|n} \mu(n/d) \ln d = \Lambda(n) \quad \text{and} \quad \sum_{d|n} \mu(d) \ln d = -\Lambda(n).$$

(Hint: $\ln d = \ln n - \ln(n/d)$.)

(c) Evaluate $\Phi_n(1)$ for every $n \geq 1$. (Hint: cancel factors of $x - 1$.)

XII. Suppose that p is a prime not dividing n. If $n \mid (p-1)$, prove that the roots of Φ_n (mod p) are precisely the $\phi(n)$ elements of order n modulo p. If $n \nmid (p-1)$, prove that Φ_n has no roots (mod p).