MATH 4400/6400
TAKE-HOME MIDTERM
DUE 4/3/08

Instructions: Math 6400 students should do all the problems. Math 4400 students should do four of the five problems.

Problem 1: Let p be an odd prime.

(a) Let g be a primitive root in $\mathbb{F}_p$. Show that g is not a square in $\mathbb{F}_p$.

Now assume that p is a prime equal to $2^{2^n} + 1$ for some n.

(b) Let g be an element of $\mathbb{F}_p^*$ that is not a square. Show that g is a primitive root in $\mathbb{F}_p^*$.

(c) Show that 7 is a primitive root in $\mathbb{F}_p^*$.

Problem 2: Define the *von Mangoldt function* $\Lambda(n)$ by the formula

$$\Lambda(n) = \begin{cases} \ln p & \text{if } n = p^e \text{ for some positive } e \\ 0 & \text{otherwise} \end{cases}$$

(a) Let $\ell(n)$ denote the least common multiple of the first n positive integers. Show that

$$e^{\Lambda(n)} = \frac{\ell(n)}{\ell(n-1)}.$$

(b) Show that $\sum_{d|n} \Lambda(d) = \ln n$. (WARNING: $\Lambda(n)$ is NOT multiplicative!)

(c) Show that $\Lambda(n) = -\sum_{d|n} \mu(d) \ln d$. (Hint: remember that $\ln(n/d) = \ln(n) - \ln(d)$.)

Problem 3: Find *all* primitive solutions in positive integers to the equation $3x^2 + 5y^2 = 23z^2$. To start, you might notice that $(1, 2, 1)$ is a solution.

Problem 4: Let q be a prime power.

(a) Let ℓ be a prime number. Give a formula for the number of ℓth powers in $\mathbb{F}_q^*$. (You will have to take cases on q and ℓ. The original midterm problem was the case $\ell = 3$.)

(b) Now generalize: let ℓ be any positive integer. Give a formula for the number of ℓth powers in $\mathbb{F}_q^*$.

Problem 5: Let $\omega = \dfrac{-1 + \sqrt{-3}}{2}$.

(a) Show that $\mathbb{Z}[\omega]$ is a principal ideal domain.

(b) Let p be an integer prime not equal to 2 or 3. Show that the following are equivalent:

(1) p is reducible in $\mathbb{Z}[\omega]$
(2) p can be written as $x^2 - xy + y^2$ for some integers x and y
(3) -3 is a square mod p
(4) $p \equiv 1 \bmod 3$

(c) Use the identities

$$x^2 - xy + y^2 = \left(x - \frac{y}{2}\right)^2 + 3(y/2)^2 = \left(\frac{x}{2} - y\right)^2 + 3(x/2)^2 = \left(\frac{x+y}{2}\right)^2 + 3\left(\frac{x-y}{2}\right)^2$$

to show that we can add a fifth condition:

(5) p can be written as $a^2 + 3b^2$ for some integers a and b

to the list of equivalent conditions in part (b). (Remember to show that it is *equivalent* to the other four!)