Name:_____

Math 4400

Third Midterm Examination Answer Key

November 30, 2012

Please indicate your reasoning and show all work on this exam paper.

Relax and good luck!

Problem	Points	Score
1	20	20
2	20	20
3	20	20
4	20	20
5	20	20
Total	100	100

1. Give precise definitions of each of the following (5 points each)

(a) The Legendre symbol.

The symbol:

$$\left(\frac{a}{p}\right)$$

is defined when p is a prime and a is an integer relatively prime to p. It is 1 if a is square (mod p) and -1 otherwise.

(b) A Gaussian integer.

A Gaussian integer is a complex number of the form $a + bi$ where a, b are (ordinary) integers.

(c) An indecomposable Gaussian integer.

A Gaussian integer $a + bi$ is indecomposable if $a + bi$ is not a unit, and its only factors are units or the product of $a + bi$ with units.

(d) Pell's Equation.

Pell's equation is any equation of the form:

$$x^2 - Dy^2 = 1$$

where D is a natural number which is not a perfect square.

2.

(a) (10 points) State and prove Euler's criterion for computing the Legendre symbol.

Euler's Criterion states that the Legendre symbol satisfies:

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod{p}$$

whenever p is an odd prime.

Proof. Let $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ be a primitive element. Then the squares mod p are the **even** powers of g and (because there are an equal number of squares and non-squares), the non-squares are the **odd** powers of g.

Let a be a square. Then for some k,

$$a \equiv g^{2k} \pmod{p}, \text{ so } a^{\frac{p-1}{2}} \equiv g^{k(p-1)} \equiv 1 \pmod{p}$$

by Fermat's Little Theorem.

On the other hand, it follows from the fact that g is primitive (and Fermat's Little Theorem) that $g^{\frac{p-1}{2}} \equiv -1 (\text{mod } p)$, so if a is **not** a square, then there is some k such that:

$$a \equiv g^{2k+1} \pmod{p}, \text{ so } a^{\frac{p-1}{2}} \equiv g^{k(p-1)+\frac{p-1}{2}} \equiv -1 \pmod{p}$$

which proves Euler's criterion.

(b) (10 points) For an odd prime p, prove that:

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 \text{ if } p \equiv 1 \pmod{4} \\ \\ -1 \text{ if } p \equiv 3 \pmod{4} \end{cases}$$

By Euler's criterion:

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} = \begin{cases} 1 \text{ if } p \equiv 1 \pmod{4} \\ -1 \text{ if } p \equiv 3 \pmod{4} \end{cases}$$

3. In the ring of Gaussian integers, find the following:

(a) (10 points) A factorization of:

$$12 + 12i$$

as a product of indecomposable Gaussian integers.

First of all,

$$12 + 12i = 12(1 + i)$$

and $1 + i$ is indecomposable. Next, we factor 12:

$$12 = 2^2 \cdot 3$$

and 3 is indecomposable. Finally, we factor 2:

$$2 = (-i)(1 + i)^2$$

so putting it all together, we have:

$$12 + 12i = (-i)^2 \cdot 3 \cdot (1 + i)^5 = -3(1 + i)^5$$

(b) (10 points)

$$\gcd(8 + i, 7 + 4i)$$

We begin by computing norms:

$$N(8 + i) = 64 + 1 = 65, \qquad N(7 + 4i) = 49 + 16 = 65$$

and since $65 = 5 \cdot 13$, it follows that any indecomposable common factor must have norm 5 or norm 13. These are:

$$1 + 2i,\ 1 - 2i,\ 2 + 3i,\ 2 - 3i$$

We start by *trying* to divide each by $1 + 2i$:

$$\frac{8 + i}{1 + 2i} = \frac{(8 + i)(1 - 2i)}{5} = \frac{10 - 15i}{5} = 2 - 3i$$

It works! Thus the factorization of $8 + i$ is $8 + i = (1 + 2i)(2 - 3i)$.

Similarly,

$$\frac{7 + 4ii}{1 + 2i} = \frac{(7 + 4i)(1 - 2i)}{5} = \frac{15 - 10i}{5} = 3 - 2i$$

which also works! The factorization of $7+4i$ is $7+4i = (1+2i)(3-2i)$.

Since $1 + 2i$ is a common factor, and $2 - 3i$ and $3 - 2i$ are **not** associated indecomposables (one is not a unit times the other), it follows that the gcd is:

$$1 + 2i$$

4. (a) (5 points) Fill in the blanks. If p is an odd prime, then:

$$\left(\frac{2}{p}\right) = \begin{cases} 1 \text{ if } p \equiv 1 \text{ or } 7 \pmod 8 \\ -1 \text{ if } p \equiv 3 \text{ or } 5 \pmod 8 \end{cases}$$

(b) (5 points) Carefully state the Quadratic Reciprocity Theorem.

If p and q are two different odd primes, then:

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \textbf{ unless } p \equiv q \equiv 3 \pmod 4$$

in which case:

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$$

(c) (10 points) Compute the following two Legendre symbols (show your work!).

$$\left(\frac{50}{101}\right) \qquad\qquad \left(\frac{51}{101}\right)$$

Using (a) above:

$$\left(\frac{50}{101}\right) = \left(\frac{2}{101}\right) \cdot \left(\frac{25}{101}\right) = \left(\frac{2}{101}\right) = -1$$

because $101 \equiv 5 \pmod 8$.

Using (b) above:

$$\left(\frac{51}{101}\right) = \left(\frac{3}{101}\right)\left(\frac{17}{101}\right) = \left(\frac{101}{3}\right)\left(\frac{101}{17}\right) = \left(\frac{2}{3}\right)\left(\frac{-1}{17}\right) = -1 \cdot 1 = -1$$

We conclude that neither 50 nor 51 is a square mod 101.

5. Let p be an odd prime.

(a) (10 points) Prove that if p is a sum of two perfect squares, then

$$p \equiv 1 \pmod 4.$$

If $p = a^2 + b^2$, then:

$$a^2 \equiv -b^2 \pmod p \quad \Rightarrow \quad (ab^{-1})^2 \equiv 1 \pmod p$$

where b^{-1} is the multiplicative inverse of b in $(\mathbb{Z}/p\mathbb{Z})^\times$, so:

$$\left(\frac{-1}{p}\right) = 1 \Rightarrow p \equiv 1 \pmod 4$$

(b) (10 points) Sketch the proof of the converse to (a). If

$$p \equiv 1 \pmod 4,$$

then p is the sum of two perfect squares.

From $p \equiv 1 (\text{mod } 4)$, we conclude that -1 is a square mod p, so:

$$a^2 \equiv -1 \text{ (mod) p)}$$

for some a, which then solves the equation:

$$a^2 + 1 = mp$$

for some $m \geq 1$. If $m = 1$, we are done. Otherwise, Fermat's method of infinite descent allows us to find a pair of integers (u, v), such that:

$$u^2 + v^2 = rp$$

where $r < m/2$, which we can invoke until we arrive at $r = 1$.