Name:_____

Math 4400
Second Midterm Examination
Answer Key
October 26, 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) Field.

A field is a set F with two binary operations $+, \cdot$, such that:

$(F, +)$ is a commutative group with additive identity 0.

$(F - \{0\} = F^\times, \cdot)$ is a commutative group with multiplicative id 1.

Addition and multiplication satisfy the distributive law.

(b) Perfect number.

A perfect number is a natural number n that is the sum of all its proper divisors, i.e. n is perfect if:

$$n = \sum_{d|n, d<n} d$$

(c) Mersenne prime.

An integer of the form:

$$M_l = 2^l - 1$$

is a Mersenne number. If it is prime, it is a Mersenne prime. It is true, but not needed for the definition, that a necessary (but not sufficient) condition for M_l to be prime is that l itself be prime.

(d) Primitive element in $(\mathbb{Z}/p\mathbb{Z})^\times$.

A primitive dth root of 1 in a field is an element $a \in F^\times$ with the property that $a^d = 1$ but $a^e \neq 1$ for any $e < d$. In this case, a primitive element in $(\mathbb{Z}/p\mathbb{Z})^\times$ is a primitive $p-1$st root of 1. It can also be defined as an element $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ with the property that every element of $(\mathbb{Z}/p\mathbb{Z})^\times$ is a (unique) power of a.

2. Solve the following two equations:

(a) (10 points)

$$5x \equiv 7 \pmod{22}$$

From Euclid's algorithm applied to $(5, 22)$, we obtain:

$$22 = 4 \cdot 5 + 2, \quad 5 = 2 \cdot 2 + 1$$

and

$$2 = 22 - 4 \cdot 5, \quad 1 = 5 - 2 \cdot 2 = 5 - 2(22 - 4 \cdot 5)$$

giving the equation:

$$9 \cdot 5 - 2 \cdot 22 = 1$$

so $9 \equiv 5^{-1} \pmod{22}$. Thus we solve the equation by:

$$x \equiv 9(5x) \equiv 9 \cdot 7 \equiv 19 \pmod{22}$$

(b) (10 points)

$$x^5 \equiv 7 \pmod{23}$$

From the previous problem(!) we have $9 \equiv 5^{-1} \pmod{22}$. Thus:

$$x \equiv (x^5)^9 \equiv 7^9 \pmod{23}$$

and we compute 7^9 by successive squaring:

$$7^1 = 7, \quad 7^2 \equiv 3, \quad 7^4 \equiv 9, \quad 7^8 \equiv 81 \equiv 12$$

and then:

$$7^9 \equiv 12 \cdot 7 \equiv 15 \pmod{23}$$

3. State the following theorems precisely (10 points each):

(a) Dirichlet's Theorem on Primes in Arithmetic Progressions.

If a and d are natural numbers, and $\gcd(a, d) = 1$, then there are infinitely many primes in the arithmetic progression:

$$a, a + d, a + 2d, a + 3d, \cdots$$

(b) The Lucas-Lehmer Test for Primeness of $M_l = 2^l - 1$.

Let l be an odd prime number. Define a sequence of integers by:

$$s_1 = 4, \quad s_{n+1} = s_n^2 - 2 \text{ for } n \geq 1$$

Then $M_l = 2^l - 1$ is prime if and only if $M_l | s_{l-1}$.

4. (a) (5 points) How many primitive elements are there in $(\mathbb{Z}/19\mathbb{Z})^\times$?

There are:

$$\phi(18) = \phi(2) \cdot \phi(9) = 6$$

primitive elements in $(\mathbb{Z}/19\mathbb{Z})^\times$.

(b) (15 points) Find **all** of the primitive elements in $(\mathbb{Z}/19\mathbb{Z})^\times$.

(Hint: To get you started, 2 is a primitive element.)

We use the known primitive element 2 to make a table:

I	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2^I	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1

The primitive elements are the powers 2^I with $\gcd(I, 18) = 1$, i.e.

$$2^1 = 2,\ 2^5 \equiv 13,\ 2^7 \equiv 14,\ 2^{11} \equiv 15,\ 2^{13} \equiv 3,\ 2^{17} \equiv 10$$

Checking against (a), we see that there are indeed six of these.

5. (a) (10 points) Verify that:

$$28 = \sum_{d|28} \phi(d)$$

The divisors of 28 are $1, 2, 4, 7, 14, 28$. We compute:

$\phi(1) = 1,\ \phi(2) = 1,\ \phi(4) = 2,\ \phi(7) = 6,\ \phi(14) = 6$ and $\phi(28) = 12$

Summing them up, we get:

$$1 + 1 + 2 + 6 + 6 + 12 = 28$$

This verifies the equation.

(b) (10 points) The first three even perfect numbers are:

$$6, 28 \text{ and } 496$$

What is the next one? (You may write it as a product of two numbers.)

The formula for even perfect numbers is:

$$n = 2^{l-1}(2^l - 1)$$

where $M_l = 2^l - 1$ is a Mersenne prime. The first few are:

$l = 2. \quad n = 2 \cdot 3 = 6.$

$l = 3. \quad n = 4 \cdot 7 = 28.$

$l = 5. \quad n = 16 \cdot 31 = 496$

The next one is:

$l = 7. \quad n = 64 \cdot 127 = 8128.$