North Carolina State University is a land-grant university and a constituent institution of The University of North Carolina

Department of Mathematics

NC STATE UNIVERSITY

MA 410 Theory of Numbers, final examination, May 6, 2011

Prof. Erich Kaltofen <kaltofen@math.ncsu.edu>
www.math.ncsu.edu/~kaltofen/courses/NumberTheory/Spring10/ (URL)

919.515.8785 (phone)
919.515.3798 (fax)

Your Name: _____

For purpose of anonymous grading, please do **not** write your name on the subsequent pages.

This examination consists of 6 problems, which are subdivided into 12 questions, where each question counts for the explicitly given number of points, adding to a total of **50 points**. Please write your answers in the spaces indicated, or below the questions, using the **back of the sheets** for completing the answers and **for all scratch work,** if necessary. You are allowed to consult **three** 8.5in $\times$ 11in sheets with notes, but **not** your book or your class notes. If you get stuck on a problem, it may be advisable to go to another problem and come back to that one later.

You will have **120 minutes** to do this test.

Good luck!

Problem 1 _____

2 _____

3 _____

4 _____

5 _____

6 _____

Total _____

Problem 1 (16 points)

(a, 4pts) Please compute 2^{100} mod 10. Please show your work.

(b, 4pts) True of false: For all integers $x, y, z \in \mathbb{Z}_{>0}$ with $x^2 + y^2 = z^2$ one has $xyz \geq 60$. Please explain your answer.

(c, 4pts) Let $p = 11$ and $\boldsymbol{i} = \sqrt{-1}$, which does not exist in $\mathbb{Z}_{11}$. Please simplify the fraction $\dfrac{2+7\boldsymbol{i}}{1+\boldsymbol{i}}$ to form $a + \boldsymbol{i}\,b$, where $a, b \in \mathbb{Z}_{11}$. Please show your work.

(d, 4pts) Please give a modulus $m \in \mathbb{Z}_{\geq 2}$ and a quadratic equation $ax^2 + bx + c \equiv 0 \pmod{m}$, where $a, b, c \in \mathbb{Z}_m$, that has 3 or more solutions in the unknown residue $x \in \mathbb{Z}_m$.

Problem 2 (5 points): **Using the quadratic reciprocity law**, please compute the value of the Jacobi symbol $\left(\frac{168}{179}\right)$. Please show all your work.

Problem 3 (8 points): We know for all prime numbers $p \geq 3$ that $\left(\frac{2}{p}\right) = +1 \Longleftrightarrow p \equiv \pm 1 \pmod 8$. Please prove that

(a, 4pts) if $p \equiv 1 \pmod 8$, c is a quadratic non-residue modulo p, and $b = c^{(p-1)/8} + c^{7(p-1)/8}$, then we have $b^2 \equiv 2 \pmod p$. Note that $(p-1)/8 \in \mathbb{Z}$.

(b, 4pts) if $p \equiv 7 \pmod 8$ and $b = 2^{(p+1)/4}$, then we have $b^2 \equiv 2 \pmod p$. Note that $(p+1)/4 \in \mathbb{Z}$.

Problem 4 (10 points): Consider the following table of indices (discrete logarithms) for the prime number 23 with respect to the primitive root $g = 5$:

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
$\text{ind}_5(a)$	0	2	16	4	1	18	19	6	10	3	9	20	14	21	17	8	7	12	15	5	13	11

(a, 4pts) From the above index table, compute the multiplicative order modulo 23 of the following residues (the exponent that belongs to the following residues module 23):

$$1, \quad 2, \quad 10, \quad 22 \quad \in \mathbb{Z}_{23}.$$

(b, 6pts) Using the above table, please solve for $x \in \mathbb{Z}_{23}$, $y \in \mathbb{Z}_{23}$, and $z \in \mathbb{Z}_{23}$ the three congruences

$$10x^8 \equiv 22 \pmod{23}, \quad y^{13} \equiv 2 \pmod{23}, \quad 4^z \equiv z^4 \pmod{23}.$$

Please give **all** solutions and show your work.

Problem 5 (6 points): Taher El Gamal's 1984 public key cryptosystem realizes probabilistic cryptography. Please explain how Bob chooses his public key, how Alice encrypts her messages to him, and how Bob decrypts them with his secret private key. In particular, explain why randomization is necessary for the system's security.

Problem 5 (5 points): Please find three positive integers $x, y, z \in \mathbb{Z}_{>0}$ such that $x^2 + 5y^4 = z^2$. Please show your work.