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 5, 2010

Prof. Erich Kaltofen <kaltofen@math.ncsu.edu>
919.515.8785 (phone)
919.515.3798 (fax)
www.math.ncsu.edu/~kaltofen/courses/NumberTheory/Spring10/ (URL)

Your Name: ______________________

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

This examination consists of 5 problems, which are subdivided into 10 questions, where each question counts for the explicitly given number of points, adding to a total of **46 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	_____
Total	_____

Problem 1 (16 points)

(a, 4pts) Please compute $2^{1000000} \bmod 55$. Hint: use Chinese remaindering and Euler's generalization of the little Fermat theorem.

(b, 4pts) True of false: For all integers x, y, z with $xyz \neq 0$ we have $x^4 + 4y^4 \neq z^4$. Please explain your answer.

(c, 4pts) True or false: if p is a prime number with $p \equiv 3 \pmod 4$ then for all $a \in \mathbb{Z}_p$, $a \neq 0$ exactly one of a and $p - a$ are quadratic residues.

(d, 4pts) The Riemann zeta function

$$\zeta(z) = \frac{1}{1^z} + \frac{1}{2^z} + \cdots + \frac{1}{i^z} + \cdots$$

is defined for complex values $z \in \mathbb{C}$ (but not everywhere, e.g., not for $z = 1$). The Riemann hypothesis conjectures a property for all complex zeros $w \in \mathbb{C}$ of ζ, i.e., $\zeta(w) = 0$. Which property?

Problem 2 (5 points): **Using the quadratic reciprocity law**, please compute the value of the Jacobi symbol $\left(\frac{70}{151}\right)$. Please show all your work.

Problem 3 (5 points): Using Newton iteration discussed in class compute consecutively residues $b_0 \in \mathbb{Z}_3$, then $b_1 \in \mathbb{Z}_3$ and finally $b_2 \in \mathbb{Z}_3$ such that $b_0 + 3b_1 + 9b_2 = b \in \mathbb{Z}_{27}$ satisfies $b^2 \equiv 7 \pmod{27}$.

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

(a, 4pts) By inspecting the above table, please list all primitive roots modulo 23.

(b, 6pts) Using the above table, please solve for $x \in \mathbb{Z}_{23}$, $y \in \mathbb{Z}_{23}$, and $z \in \mathbb{Z}_{22}$ the three congruences

$$10x^9 \equiv 22 \pmod{23}, \quad y^4 \equiv 2 \pmod{23}, \quad 7^z \equiv 10 \pmod{23}.$$

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

(c, 5pts) Suppose Bob has set up a public key $p = 23$, $g = 5$, and $h = 19 = g^s \pmod{23}$ for Taher ElGamal's cryptosystem. Alice has chose her random $r = 15$ and encrypts a message $M = 15$. What cipertext is Alice sending to Bob? You can use the table above part (a) for modular exponentiation (instead of repeated squaring) but not for computing Bob's secret s.

Problem 5 (5 points): Please find three integers $x, y, z \in \mathbb{Z}_{>0}$ such that $\mathrm{GCD}(x, y) = 1$ and $x^2 + y^5 = z^2$. Please show your work.