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 7, 2012

Prof. Erich Kaltofen <kaltofen@math.ncsu.edu>
www.math.ncsu.edu/~kaltofen/courses/NumberTheory/Spring12/ (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 11 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 100. Please show your work.

(b, 4pts) True or false: If p is a prime number then $\sigma(p^2 - p) = (p+1)\sigma(p-1)$. Please explain.

(c, 4pts) Please construct a primitive Pythagorean triple $(x, 7, z) \in \mathbb{Z}^3_{>0}$ such that $x^2 + 7^2 = z^2$.

(d, 4pts) Please state a conjecture in number theory, which is yet to be proven.

Problem 2 (5 points): **Using the quadratic reciprocity law**, please compute the value of the Jacobi symbol $\left(\frac{610}{987}\right)$. Please show all your work.

Problem 3 (8 points):

(a, 4pts) Show that $a = 13$ is a quadratic residue and $c = 14$ is a quadratic non-residue, both modulo 29.

(b, 4pts) Using the algorithm from class, compute $b \in \mathbb{Z}_{29}$ such that $b^2 \equiv 13 \pmod{29}$. If you need a quadratic non-residue, please use 14.

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) By inspecting the above table, for the multiplicative orders $k = 1, 2, 11, 22$ please list one residue $a_k \in \mathbb{Z}_{23} \setminus \{0\}$ each that has order k (belongs to the exponent k modulo 23).

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

$$18x^6 \equiv 9 \pmod{23}, \quad y^{21} \equiv 22 \pmod{23}, \quad 5^{3z} \equiv z \pmod{23}.$$

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

Problem 5 (6 points): Taher El Gamal's 1984 public key cryptosystem in its original form is still malleable. Alice sends Bob a ciphertext

$$E(M_A) = \Big(\underbrace{g^{r_A} \bmod p}_{x_A}, \quad \underbrace{M_A h_B^{r_A} \bmod p}_{y_A}\Big), \quad r_A \text{ random and hidden,}$$

of her message M_A with his public key $h_B = (g^{s_B} \bmod p)$, s_B secret. Charlie, knowing the cipher x_A, y_A, can encrypt $\lambda_C M_A$ with his λ_C without knowing M_A. A problem is that Charlie needs to send his own x_C, and does so by using $x_C = (x_A g^{r_C} \bmod p)$ for his own random r_C. Please give Charlie's y_C for $E(\lambda_C M_A)$, and justify that Bob's decryption produces $\lambda_C M_A$.

Problem 6 (5 points): Please find three positive integers $x, y, z \in \mathbb{Z}_{>0}$ such that $\mathrm{GCD}(x, y) = 1$ and $x^2 + y^2 = z^4$.