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 2, 2007

Prof. Erich Kaltofen <kaltofen@math.ncsu.edu>
www.math.ncsu.edu/~kaltofen/courses/NumberTheory/Spring07/ (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 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	____
6	____
Total	____

Problem 1 (16 points)

(a, 4pts) Please state Fermat's little theorem and Euler's generalization to composite moduli.

(b, 4pts) Let p be a positive prime integer and let ϕ be Euler's ϕ function. True or false: there are $\phi(\phi(p))$ primitve roots modulo p. Please explain your answer.

(c, 4pts) True or false: If p is a positive prime integer and a is a quadratic non-residue modulo p, then $(a^3 \bmod p)$ must be a quadratic non-residue modulo p. Please explain.

(d, 4pts) Please explain the Diffie-Hellman private key exchange protocol.

Problem 2 (4 points): Please give the value of the sum $\sum_{d|300,\, d>0} \phi(d)$.

Problem 3 (5 points): **Using the quadratic reciprocity law**, please compute the value of the Jacobi symbol $\left(\frac{232}{123}\right)$. Please show all your work.

Problem 4 (11 points): Consider the following table of indices (discrete logarithms) for the prime number 17 with respect to the primitive root $g = 3$:

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\text{ind}_3(a)$	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

(a, 5pts) Using the above table, please solve in $x \in \mathbb{Z}_{17}$ and $y \in \mathbb{Z}_{17}$ the two congruences

$$x^3 \equiv 2 \pmod{17}, \quad y^5 \equiv 2 \pmod{17}$$

Please give all solutions.

(b, 6pts) Suppose a residue $M \in \mathbb{Z}_{17}$ has been encrypted by the el-Gamal public key system with public keys $p = 17$, $g = 3$ and $h \equiv 3^s \equiv 7 \bmod 17$. The ciphertext is

$$N = (g^r \bmod 17,\ M \cdot h^r \bmod 17) = (14, 14).$$

Please compute from N the encryption N' of $M' = M/3$, with $r' = (r + 1 \bmod 16)$, that **without** computing r or s. Please show your derivation.

Problem 5 (5 points): Let $p > 2$ be a prime integer with $p \equiv 3 \pmod 4$ and let $a \in \mathbb{Z}_p$ be a quadratic non-residue modulo p. Show that for $x = (a^{\frac{p+1}{4}} \bmod p)$ one has $x^2 \equiv -a \pmod p$.

Problem 6 (5 points): Please find integers $x, y, z \in \mathbb{Z}_{>0}$ such that $x^4 + y^2 = z^2$. Please show your work.