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, April 30, 2008
Prof. Erich Kaltofen <kaltofen@math.ncsu.edu>
www.math.ncsu.edu/~kaltofen/courses/NumberTheory/Spring08/ (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 **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) Fermat's last theorem is a famous impossibility theorem of mathematics. Please state another impossibility theorem of mathematics.

(b, 4pts) True of false: For all integers x, y, z with $xyz \neq 0$ we have $x^4 + y^4 \neq z^2$. Please explain your answer.

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

(d, 4pts) Let $p > 1$ be a prime integer. How many residues in $\mathbb{Z}_p$ are primitive roots?

Problem 2 (5 points): **Using the quadratic reciprocity law**, please compute the value of the Jacobi symbol $\left(\frac{58}{101}\right)$. Please show all your work.

Problem 3 (5 points): The El Gamal public key cryptosystem is a *probabilistic* cryptosystem because clear text is encrypted using a different random residue for each cyphertext. Show that if instead a single fixed residue is used for all encryptions, the resulting *non*-probabilistic system can be broken by the *chosen ciphertext attack*.

Problem 4 (10 points): Consider the following table of indices (discrete logarithms) for the prime number 19 with respect to the primitive root $g = 2$:

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\mathrm{ind}_2(a)$	18	1	13	2	16	14	6	3	8	17	12	15	5	7	11	4	10	9

(a, 5pts) There are $\phi(9)$ residues in $\mathbb{Z}_{19} \setminus \{0\}$ that have (multiplicative) order 9 modulo 19 (belong to the exponent 9 modulo 19). By inspecting the above table, please list all those residues.

(b, 5pts) Using the above table, please solve $x \in \mathbb{Z}_{19}$ and all $y \in \mathbb{Z}_{19}$ the two congruences

$$x^3 \equiv 7 \pmod{19}, \quad 5y^5 \equiv 12 \pmod{19}$$

Please give all solutions and show your work.

Problem 5 (6 points): Let $p > 2$ be a prime integer with $p \equiv 5 \pmod 8$, i.e., 8 divides $p+3$ and 4 divides $p-1$, and let $a \in \mathbb{Z}_p$ be a quadratic residue modulo p.
Since $a^{\frac{p-1}{2}} \pmod p = \left(\frac{a}{p}\right) = 1$ we must have $a^{\frac{p-1}{4}} \equiv \pm 1 \pmod p$.

(a, 3pts) Case $a^{\frac{p-1}{4}} \equiv 1 \pmod p$: Show that for $x = (a^{\frac{p+3}{8}} \bmod p)$ one has $x^2 \equiv a \pmod p$.

(b, 3pts) Case $a^{\frac{p-1}{4}} \equiv -1 \pmod p$: Let c be an arbitrary quadratic non-residue.
Show that for $x = (a^{\frac{p+3}{8}} c^{\frac{p-1}{4}} \bmod p)$ one has $x^2 \equiv a \pmod p$.

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