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 4, 2005

919.515.8785 (phone)
919.515.3798 (fax)
kaltofen@math.ncsu.edu (email)
www.math.ncsu.edu/~kaltofen/courses/NumberTheory/Spring05/ (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 **47 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) Let p be a positive prime integer. Please define under which conditions a residue $g \in \mathbb{Z}_p$ is a *primitive root*.

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

(c, 4pts) The RSA public key cryptosystem is *malleable*. Please explain what that means.

(d, 4pts) Please state Fermat's last theorem, which was proved by Andrew Wiles in 1994.

Problem 2 (5 points): Please compute the sum

$$\sum_{d|300,\, d>0} (\mu(d) \cdot d)\,,$$

where μ is the Möbius function. Please show your derivation. [Hint: note that $300 = 2^2 \cdot 3 \cdot 5^2$ and that the function $\mu(m) \cdot m$ is multiplicative.]

Problem 3 (5 points): **Using the quadratic reciprocity law**, please compute the value of the Legendre symbol $\left(\frac{11}{1019}\right)$ (Burton's book writes $(11/1019)$ instead). Note that $1019 = 92 \cdot 11 + 7$. Please show all your work.

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

(a, 5pts) There are $\phi(16)$ residues in $\mathbb{Z}_{17} \setminus \{0\}$ that are primitive roots (including 3). By inspecting the above table, please list all those residues.

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

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

Please give all solutions.

(c, 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 M, showing your derivation. [Hint: you can use the table on the previous page for deriving the private key s, and for powering, multiplication, and reciprocal modulo 17.]

Problem 5 (5 points): Please compute all primitive Pythagorean triples (x, y, z) such that $x = 12$, $y > 0$ and $z > 0$.