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 1, 2009

Prof. Erich Kaltofen <kaltofen@math.ncsu.edu>
www.math.ncsu.edu/~kaltofen/courses/NumberTheory/Spring09/ (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	____
Total	____

Problem 1 (16 points)

(a, 4pts) What makes a public key cryptosystem public? Please explain by example of the RSA.

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

(c, 4pts) Please prove: let $p > 2$ be a prime number such that $p \equiv 3 \pmod 4$, i.e., $p - 1$ is a quadratic non-residue. Then for all $x, y \in \mathbb{Z}_p$ with $x > 0, y > 0$ one has $x^2 + y^2 \not\equiv 0 \pmod p$.

(d, 4pts) True of false: there does **not** exist an algorithm that for a system of polynomial equations with integer coefficients determines if the system has a solution where the values of the variables are integers.

Problem 2 (5 points): **Using the quadratic reciprocity law**, please compute the value of the Jacobi symbol $\left(\frac{110}{199}\right)$. Please show all your work.

Problem 3 (5 points): Let $p > 2$ be a prime integer with $p \equiv 5 \pmod 8$, and let $a \in \mathbb{Z}_p$ be a quadratic residue modulo p with $a^{(p-1)/4} \equiv -1 \pmod p$. Please explain how you can compute a residue b with $b^2 \equiv a \pmod p$.

Problem 4 (15 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) By inspecting the above table, for the multiplicative orders $k = 1,2,3,6,9,18$ please list one residue $a_k \in \mathbb{Z}_{19}$ each that has order k (belongs to the exponent k modulo 19).

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

$$x^4 \equiv 5 \pmod{19}, \quad 7y^7 \equiv 8 \pmod{19}$$

Please give all solutions and show your work.

(c, 5pts) Suppose Alice has digitally signed her signature $F_A \in \mathbb{Z}_{19}$ by the el-Gamal public key system. The shared modulus is $p = 19$ and the shared primitive root is $g = 2$. Her public key is $h_A = 15 \equiv 2^{s_A} \bmod 19$. Her digital signature using Bob's $x_B = 9 \equiv 2^{r_B} \bmod 19$ is $G_A = 10 \in \mathbb{Z}_{19}$. Please show how Bob computes F_A. You can use the table in part (a) to determine Bob's secret random exponent r_B, but not Alice's private key, namely exponent s_A.

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