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 5, 2016

Prof. Erich Kaltofen <kaltofen@math.ncsu.edu>
www.math.ncsu.edu/~kaltofen/courses/NumberTheory/Spring16/ (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 **49 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) In public key cryptography, Alice encodes her clear text using no secret. Please explain why such a cipher text can be secure, in particular what assumption guarantees the security of an RSA cipher.

(b, 4pts) True or false: if n is a **composite** integer ≥ 4 then $\phi(n) \leq \frac{n}{2}$, where ϕ is Euler's function. Please explain.

(c, 4pts) True or false: for all non-negative integers $n \in \mathbb{Z}_{\geq 0}$ there exist four non-negative integers $x, y, z, w \in \mathbb{Z}_{\geq 0}$ such that $n = x^2 + y^2 + z^2 + w^2$. Please explain.

(d, 4pts) True or false: there exist positive integers $x, y, z, w \in \mathbb{Z}_{>0}$ such that $x^4 + y^4 + z^4 = w^4$. Please explain.

Problem 2 (5 points): The following is a trace of the computation of the Legendre symbol $\left(\frac{-142}{239}\right)$ using Jacobi's reciprocity law. Please fill in the blanks.

$$\left(\frac{-142}{239}\right) = \left(\frac{-1}{239}\right)\left(\frac{142}{239}\right); \quad \left(\frac{-1}{239}\right) = \underline{\hspace{4cm}}$$

$$\left(\frac{142}{239}\right) = \left(\frac{2}{239}\right)\left(\frac{71}{239}\right); \quad \left(\frac{2}{239}\right) = \underline{\hspace{4cm}}$$

$$\left(\frac{71}{239}\right)\left(\frac{239}{71}\right) = \underline{\hspace{4cm}}; \quad 239 \bmod 71 = 26;$$

$$\left(\frac{26}{71}\right) = \left(\frac{2}{71}\right)\left(\frac{13}{71}\right); \quad \left(\frac{2}{71}\right) = \underline{\hspace{4cm}}$$

$$\left(\frac{13}{71}\right)\left(\frac{71}{13}\right) = \underline{\hspace{4cm}}; \quad 71 \bmod 13 = 6$$

$$\left(\frac{6}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{3}{13}\right); \quad \left(\frac{2}{13}\right) = \underline{\hspace{4cm}};$$

$$\left(\frac{3}{13}\right)\left(\frac{13}{3}\right) = \underline{\hspace{4cm}}; \quad \left(\frac{13}{3}\right) = \underline{\hspace{1cm}}; \quad \left(\frac{-142}{239}\right) = \underline{\hspace{1cm}}$$

Problem 3 (8 points):

(a, 4pts) Please show that $a = p - 2 \equiv -2 \pmod{p}$ is a quadratic residue modulo a prime $p \geq 3$ if and only if $p \equiv 1 \pmod{8}$ or $p \equiv 3 \pmod{8}$. [Hint: Legendre symbol.]

(b, 4pts) Suppose that $p \equiv 1 \pmod{8}$. Let c be a quadratic non-residue modulo p, and let $b = c^{(p-1)/8} - c^{7(p-1)/8}$; note that $(p-1)/8 \in \mathbb{Z}$. Please show that $b^2 \equiv -2 \pmod{p}$.

Problem 4 (10 points): Consider the following table of indices (discrete logarithms) for the prime number 23 with respect to the primitive root $g = 10$:

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
$\mathrm{ind}_{10}(a)$	0	8	20	16	15	6	21	2	18	1	3	14	12	7	13	10	17	4	5	9	19	11

(a, 4pts) For the primitive root $g' = 5$ there is a constant residue $k \in \mathbb{Z}_{22}$ such that for all residues $a \in \mathbb{Z}_{23} \setminus \{0\}$ one has $\mathrm{ind}_5(a) \equiv k \cdot \mathrm{ind}_{10}(a) \pmod{22}$. Please compute k (using the above table) and show your work.

(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

$$15x^{15} \equiv 16 \pmod{23}, \quad 18y^{16} \equiv 13 \pmod{23}, \quad 10^{-2z} \equiv 2z^2 \pmod{23}.$$

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

Problem 5 (5 points): Suppose Alice requests a digital signature from Bob using Taher El-Gamal's public key system with $p = 23$ and $g = 10$ by sending $h_A = (10^{r_A} \bmod 23) = 15$. Here r_A is a one-time random choice. Bob replies with his digital signature $\tau = (\sigma \cdot (h_A^{s_B})^{-1} \bmod 23) = 19$, where $h_B = (10^{s_B} \bmod 23) = 20$ is Bob's public key and s_B is Bob's secret private key. Please show how Alice can retrieve σ from her r_A and h_B. You may use the previous page for deriving Alice's r_A, and for powering, multiplication, and reciprocal modulo 23.

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