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, second mid-semester examination, March 26, 2012

Prof. Erich Kaltofen <kaltofen@math.ncsu.edu>
www.math.ncsu.edu/~kaltofen/courses/NumberTheory/Spring12/ (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 9 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 **two** 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 **75 minutes** to do this test.

Good luck!

Problem 1	____
2	____
3	____
4	____
5	____
6	____
Total	____

If you are taking the exam later, please sign the following statement:

I, ______________________*, affirm that I have no knowledge of the contents of this exam.*

____

Signature

Problem 1 (16 points)

(a, 4pts) True of false:

$$\forall p, p \text{ prime} \geq 2 \colon \forall a \in \mathbb{Z}_p \colon a^2 \equiv 1 \pmod{p} \Longrightarrow a \equiv 1 \pmod{p} \quad \text{or} \quad a \equiv p-1 \pmod{p}.$$

Please explain.

(b, 4pts) Please show that $2821 = 7 \cdot 13 \cdot 31$ is a Carmichael number.

(c, 4pts) Please show that 3^{400} ends with 001 when written as a number with decimal digits. [Hint: prove that $3^{400} \equiv 1 \pmod{1000}$.]

(d, 4pts) Please prove that the system of linear congruences

$$\begin{aligned} 7x + 2y &\equiv 4 \pmod{n}, \\ 3x + y &\equiv 5 \pmod{n} \end{aligned}$$

is solvable for $x, y \in \mathbb{Z}_n$ for all $n \in \mathbb{Z}_{\geq 2}$.

Problem 2 (6 points): For which $n \in \mathbb{Z}$ is $6^n + 2 \cdot 4^{2n+2} \equiv 0 \pmod{11}$? Please explain.

Problem 3 (6 points): By completing the entries in the following table, please verify the Möbius's inversion formula for $f =$ identity function and $F = \sigma$ (sum of all positive divisors) at $n = 36 = 2^2\, 3^2$:

d	$\sigma(d)$	$\mu(\frac{36}{d})$	$\mu(\frac{36}{d}) \cdot \sigma(d)$
$1 = 2^0 \cdot 3^0$			
$2 = 2^1 \cdot 3^0$			
$4 = 2^2 \cdot 3^0$			
$3 = 2^0 \cdot 3^1$			
$6 = 2^1 \cdot 3^1$			
$12 = 2^2 \cdot 3^1$			
$9 = 2^0 \cdot 3^2$			
$18 = 2^1 \cdot 3^2$			
$36 = 2^2 \cdot 3^2$			
	$\sum_{d \mid 36 \text{ and } d \geq 1} \mu(\frac{36}{d}) \cdot \sigma(d)$	$=$	

Problem 4 (8 points): Consider $2310 = 14 \cdot 11 \cdot 15$ and let $a \in \mathbb{Z}_{2310}$ with

$$\begin{aligned} a &\equiv 13 \pmod{14}, \\ a &\equiv \ 4 \pmod{11}, \\ a &\equiv \ 1 \pmod{15}. \end{aligned}$$

Please compute $y_0 \in \mathbb{Z}_{14}$, $y_1 \in \mathbb{Z}_{11}$ and $y_2 \in \mathbb{Z}_{15}$ such that

$$a = y_0 + y_1 \cdot 14 + y_2 \cdot 14 \cdot 11.$$

Please show all your work.

Problem 5 (5 points): The Miller-Rabin algorithm is a *randomized algorithm of the Las Vegas kind* for the proving compositeness of an integer. Please explain what that means.

Problem 6 (5 points): Please consider the following instance of the RSA: the public modulus is $n = 91$ $(= 7 \cdot 13)$ and the public (enciphering) exponent is $k = 17$. Please compute the private deciphering exponent j such that $(M^{17})^j \equiv M \pmod{91}$ (at least for all $M \in U_{91}$). Please show your work.