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 28, 2011

Prof. Erich Kaltofen <kaltofen@math.ncsu.edu>
www.math.ncsu.edu/~kaltofen/courses/NumberTheory/Spring11/ (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 (12 points)

(a, 4pts) True of false:

$$\forall p, p \text{ prime} \geq 5\colon \forall a \in \mathbb{Z}_p\colon a^3 \equiv 1 \pmod{p} \Longrightarrow a \equiv 1 \pmod{p}.$$

Please explain.

(b, 4pts) Please compute residues $x, y \in \mathbb{Z}_{10}$, or prove that none exist, such that $3x + 4y \equiv 5 \pmod{13}$ and $6x + 7y \equiv 8 \pmod{13}$. Please show all your work.

(c, 4pts) Please compute $7^{10^{10}}$ mod 10. Please show your work. [Hint: use Euler's theorem.]

Problem 2 (6 points): For which $n \in \mathbb{Z}$ is $2 \cdot 3^{n+1} + 4^n \equiv 0 \pmod 7$? Please explain.

Problem 3 (6 points): By completing the entries in the following table, please verify Gauss's theorem for Euler's totient function ϕ and its associated Möbius's inversion formula for $n = 72$:

d	$\phi(d)$	$\mu(d)$	$\mu(d) \cdot \frac{72}{d}$
$1 = 2^0 \cdot 3^0$			
$2 = 2^1 \cdot 3^0$			
$4 = 2^2 \cdot 3^0$			
$8 = 2^3 \cdot 3^0$			
$3 = 2^0 \cdot 3^1$			
$6 = 2^1 \cdot 3^1$			
$12 = 2^2 \cdot 3^1$			
$24 = 2^3 \cdot 3^1$			
$9 = 2^0 \cdot 3^2$			
$18 = 2^1 \cdot 3^2$			
$36 = 2^2 \cdot 3^2$			
$72 = 2^3 \cdot 3^2$			
$\sum_{d \mid 72 \text{ and } d \geq 1}$			

Problem 4 (8 points): Consider $1716 = 13 \cdot 12 \cdot 11$ and let $a \in \mathbb{Z}_{1716}$ with

$$\begin{aligned} a &\equiv 9 \pmod{13}, \\ a &\equiv 7 \pmod{12}, \\ a &\equiv 3 \pmod{11}. \end{aligned}$$

Please compute $y_0 \in \mathbb{Z}_{13}$, $y_1 \in \mathbb{Z}_{12}$ and $y_2 \in \mathbb{Z}_{11}$ such that

$$a = y_0 + y_1 \cdot 13 + y_2 \cdot 13 \cdot 12.$$

Please show all your work.

Problem 5 (9 points): This problem shows an instance of the Miller-Rabin Monte Carlo primality test. Let $n = 1105$ and $a = 511 \in \mathbb{Z}_{1105}$. Note that $n - 1 = 1104 = 2^4 \cdot 69$. The following has been computed by repeated squaring modulo n:

$$a^{69} \equiv 511^{69} \equiv 766 \pmod{1105} \quad \text{and} \quad 766^2 \equiv 1 \pmod{1105}. \tag{1}$$

(a, 4pts) Please explain why (1) already proves that $n = 1105$ is a composite integer.

(b, 5pts) Using (1), please compute a non-trivial factor of 1105. Please show all your work.

Problem 6 (5 points): Please prove: if for an integer $N \geq 2$ the integer $2^N + 1$ is a prime number, then N must be a pure power of 2, i.e., there exists an integer $n \geq 1$ such that $N = 2^n$ (N has no odd factor > 1).