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 25, 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 5 problems, which are subdivided into 9 questions, where each question counts for the explicitly given number of points, adding to a total of **44 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 **60 minutes** to do this test.

Good luck!

Problem 1 _____

2 _____

3 _____

4 _____

5 _____

Total _____

Problem 1 (12 points)

(a, 4pts) True of false:

$$\forall n \in \mathbb{Z}_{\geq 2}, a \in \mathbb{Z}_n \colon a^2 \equiv 1 \pmod{n} \Longrightarrow a = 1 \text{ or } a = n-1.$$

Please explain.

(b, 4pts) Applying Möbius's inversion formula to $F(n) = n$, namely, $f(n) = \sum_{d|n, d\geq 1} \mu(d) \frac{n}{d}$ yields what number theoretic function for f? Please explain.

(c, 4pts) Please show that $1105 = 5 \cdot 13 \cdot 17$ is a Carmichael number.

Problem 2 (6 points): For which integers $n \in \mathbb{Z}_{\geq 0}$ is $2^n - 4$ divisible by 7. Please justify your answer.

Problem 3 (6 points): Please compute residues $x, y \in \mathbb{Z}_{11}$ such that $3x + 4y \equiv 0 \pmod{11}$ and $4x + 3y \equiv 1 \pmod{11}$. Please show all your work.

Problem 4 (8 points): Consider $315 = 5 \cdot 7 \cdot 9$ and let $a \in \mathbb{Z}_{315}$ with

$$\begin{aligned} a &\equiv 3 \pmod 5, \\ a &\equiv 5 \pmod 7, \\ a &\equiv 7 \pmod 9. \end{aligned}$$

Please compute $y_0 \in \mathbb{Z}_5$, $y_1 \in \mathbb{Z}_7$ and $y_2 \in \mathbb{Z}_9$ such that

$$a = y_0 + y_1 \cdot 5 + y_2 \cdot 5 \cdot 7.$$

Please show all your work. After seeing the answer, could you have determined y_1 and y_2 without any computation?

Problem 5 (12 points): Consider the following instance of the RSA: the public key $K = P \cdot Q$ where P and Q are primes with $P \not\equiv 1 \pmod 5$, $Q \not\equiv 1 \pmod 5$; the public (enciphering) exponent is $Y = 5$, i.e., the ciphertext of a message M is $N = E_K(M) = (M^5 \bmod K)$. Please prove the following.

(a, 5pts) $\lambda = ((P-1)(Q-1) \bmod 5) \neq 0$
and $X = \dfrac{\mu(P-1)(Q-1)+1}{5}$ is an integer for $\mu = (4\lambda^{-1} \bmod 5)$.

(b, 5pts) The integer X as defined in (a) is the private (recovery) exponent, that is for all residues $M \in \mathbb{Z}_K$ with $\mathrm{GCD}(M,K) = 1$ one has $(M^5)^X \equiv M \pmod K$.

(c, 2pts) What is X in this case (namely, $Y = 5$) for $P = 3$ and $Q = 5$?