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 24, 2015

Prof. Erich Kaltofen <kaltofen@math.ncsu.edu>
www.math.ncsu.edu/~kaltofen/courses/NumberTheory/Spring15/ (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	_____

Problem 1 (16 points)

(a, 4pts) True of false:

$$\forall p, p \text{ prime} \geq 2\colon \forall a \in \mathbb{Z}_p\colon \exists x \in \mathbb{Z}_p\colon x^3 \equiv a \pmod{p}.$$

Please explain.

(b, 4pts) True or false: $1729 = 7 \cdot 13 \cdot 19$ is a Carmichael number. Please explain.

(c, 4pts) Please compute $2^{1000} \bmod 7$, showing your work.

(d, 4pts) Please compute the solution $(x, y) \in \mathbb{Z}_{11} \times \mathbb{Z}_{11}$ of the system of linear congruences

$$\begin{aligned} x + y &\equiv 10 \pmod{11}, \\ 10x + y &\equiv \ \ 2 \pmod{11}. \end{aligned}$$

Problem 2 (6 points): Please prove that there are infinitely many prime numbers that are $\equiv 2 \pmod 3$. [Hint: consider $3\times$ product of all odd such primes $+2$].

Problem 3 (6 points): By completing the $3 \cdot 13$ entries in the following table, please verify Gauss's theorem for Euler's totient function ϕ and its associated Möbius's inversion formula for $n = 140$:

d	$\phi(d)$	$\mu(d)$	$\mu(d) \cdot \frac{140}{d}$
$1 = 2^0 \cdot 5^0 \cdot 7^0$			
$2 = 2^1 \cdot 5^0 \cdot 7^0$			
$4 = 2^2 \cdot 5^0 \cdot 7^0$			
$5 = 2^0 \cdot 5^1 \cdot 7^0$			
$10 = 2^1 \cdot 5^1 \cdot 7^0$			
$20 = 2^2 \cdot 5^1 \cdot 7^0$			
$7 = 2^0 \cdot 5^0 \cdot 7^1$			
$14 = 2^1 \cdot 5^0 \cdot 7^1$			
$28 = 2^2 \cdot 5^0 \cdot 7^1$			
$35 = 2^0 \cdot 5^1 \cdot 7^1$			
$70 = 2^1 \cdot 5^1 \cdot 7^1$			
$140 = 2^2 \cdot 5^1 \cdot 7^1$			
$\sum_{d \text{ divides } 140 \text{ and } d \geq 1}$			

Problem 4 (8 points): Consider $2145 = 15 \cdot 13 \cdot 11$ and let $a \in \mathbb{Z}_{2145}$ with

$$\begin{aligned} a &\equiv 13 \pmod{15}, \\ a &\equiv 3 \pmod{13}, \\ a &\equiv 7 \pmod{11}. \end{aligned}$$

Please compute $y_0 \in \mathbb{Z}_{15}$, $y_1 \in \mathbb{Z}_{13}$ and $y_2 \in \mathbb{Z}_{11}$ such that

$$a = y_0 + y_1 \cdot 15 + y_2 \cdot 15 \cdot 13.$$

Then compute a. Please show all your work.

Problem 5 (5 points): The first pseudo-prime (for base 2) is 341: $2^{340} \equiv 1 \pmod{341}$, but 341 is a composite number. In fact, $2^{170} \equiv 1 \pmod{341}$ and $2^{85} \equiv 32 \pmod{341}$. Using the latter two congruences, please factor 341. Please show your work.

Problem 6 (5 points): Bob receives RSA-encrypted messages from Alice, for which he has provided Alice with a public modulus n and a public exponent k. However, Bob by mistake has chosen n to be a prime number. On the (toy) example $n = 101$, $k = 67$, and the ciphertext $E = (M^{67} \bmod 101) = 5$, please show how Charlie can compute M from the public key (n,k) and E. Your method should also work on larger keys where n is prime.