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 21, 2019

Prof. Erich Kaltofen <kaltofen@math.ncsu.edu>
919.515.8785 (phone)
919.515.3798 (fax)
www.math.ncsu.edu/~kaltofen/courses/NumberTheory/Spring19/ (URL)

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 **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 **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 or false: $\forall n \in \mathbb{Z}_{\geq 2}, a, b, c \in \mathbb{Z}_n, b \neq 0$: $ab \equiv cb \pmod{n} \implies a \equiv c \pmod{\frac{n}{\gcd(b,n)}}$. Please explain.

(b, 4pts) True or false: $101101 = 7 \cdot 11 \cdot 13 \cdot 101$ is a pseudo-prime. Please explain.

(c, 4pts) Please compute $4444^{4444} \bmod 7$, showing your work.

(d, 4pts) Please show how to compute $a^{15} \bmod n$ for $a \in \mathbb{Z}_n$ with 5 multiplications modulo n.

Problem 2 (5 points): Please compute residues $x, y \in \mathbb{Z}_{11}$, or prove that none exist, such that

$$\begin{array}{rrcrcrl} & 6x & + & 5y & \equiv & 1 & \pmod{11} \\ \text{and} & 9x & + & 2y & \equiv & 6 & \pmod{11}. \end{array}$$

Problem 3 (5 points) Let p, q be two prime numbers ≥ 2, $p \neq q$. Please verify that

$$\sum_{d \text{ divides } p^3 q \text{ and } d \geq 1} \phi(d) = p^3 q.$$

Problem 4 (8 points): Consider $2730 = 13 \cdot 14 \cdot 15$ and let $a \in \mathbb{Z}_{2730}$ with

$$\begin{aligned} a &\equiv 3 \pmod{13}, \\ a &\equiv 4 \pmod{14}, \\ a &\equiv 5 \pmod{15}. \end{aligned}$$

Please compute $y_0 \in \mathbb{Z}_{13}$, $y_1 \in \mathbb{Z}_{14}$ and $y_2 \in \mathbb{Z}_{15}$ such that

$$a = y_0 + y_1 \cdot 13 + y_2 \cdot 13 \cdot 14.$$

Then compute a. Please show all your work. Is there a direct explanation for a?

Problem 5 (5 points): Please consider the following (toy) instance of the RSA: the public modulus is $n = 51$ and the private (deciphering) exponent is $j = 13$. Please compute the public enciphering exponent k such that $(m^k)^{13} \equiv m \pmod{51}$ for all messages m with $\mathrm{GCD}(m, 51) = 1$. Please decipher the message m from the cipher text $c = (m^k \bmod 51) = 2$ that was encoded with the computed k. Please show your work.

Problem 6 (5 points): For k in Problem 5, please prove that $m^{13k} \equiv m \pmod{51}$ **for all** $m \in \mathbb{Z}_{51}$. [Hint: consider the congruence modulo each factor of 51.]