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 29, 2010
Prof. Erich Kaltofen <`kaltofen@math.ncsu.edu`>
`www.math.ncsu.edu/~kaltofen/courses/NumberTheory/Spring10/` (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 × 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 _____

Total _____

Problem 1 (12 points)

(a, 4pts) True of false: for all $a \in \mathbb{Z}_{17}$ the cubic equation

$$x^3 \equiv a \pmod{17}$$

has a solution $x \in \mathbb{Z}_{17}$. Please explain.

(b, 4pts) Please compute residues $x, y \in \mathbb{Z}_{10}$, or prove that none exist, such that $3x + 4y \equiv 0 \pmod{10}$ and $x + 2y \equiv 1 \pmod{10}$. Please show all your work.

(c, 4pts) True or false: Let $n \in \mathbb{Z}_{\geq 2}$. If $\forall a \in \mathbb{Z}_n \colon a^n \equiv a \pmod{n}$ then n must be a prime number. Please explain.

Problem 2 (6 points): Please prove for all prime and composite Fermat numbers $F_n = 2^{2^n} + 1$ that

$$2^{F_n - 1} \equiv 1 \pmod{F_n} \quad \text{for all} \quad n \geq 0.$$

Hint: for $M = 2^n$ first prove that $2^{2M} \equiv 1 \pmod{2^M + 1}$.

Problem 3 (6 points): Please verify the following identity, where ϕ is Euler's totient function and μ is Möbius's function:

$$\phi(60) = \sum_{d|n \text{ and } d \geq 1} \mu(d) \frac{60}{d}$$

Please show your work.

Problem 4 (8 points): Consider $630 = 7 \cdot 9 \cdot 10$ and let $a \in \mathbb{Z}_{630}$ with

$$\begin{aligned} a &\equiv 6 \pmod{7}, \\ a &\equiv 8 \pmod{9}, \\ a &\equiv 6 \pmod{10}. \end{aligned}$$

Please compute $y_0 \in \mathbb{Z}_7$, $y_1 \in \mathbb{Z}_9$ and $y_2 \in \mathbb{Z}_{10}$ such that

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

Please show all your work.

Problem 5 (12 points):

(a, 4pts) Please describe the difference between a private key cryptosystem and a public key cryptosystem. How old is public key cryptography and who has invented it?

(b, 4pts) Please consider the following instance of the RSA: the public modulus is $n = 77$ and the public (enciphering) exponent is $k = 11$. Please compute the private deciphering exponent j such that $(M^{11})^j \equiv M \pmod{77}$ (at least for all $M \in U_{77}$).

(c, 4pts) Suppose Alice has encrypted M as $2 = (M^{11} \bmod 77)$. What is M? Please show all of Bob's computations using j from Part b.