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 30, 2005
kaltofen@math.ncsu.edu (email)
www.math.ncsu.edu/~kaltofen/courses/NumberTheory/Spring05/ (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 **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 **60 minutes** to do this test.

Good luck!

Problem 1	_____
2	_____
3	_____
4	_____
5	_____
Total	_____

Problem 1 (16 points)

(a, 4pts) Suppose a pair $(a,b) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ represents the equivalence class of a rational number $\frac{a}{b}$ and $\chi((a,b))$ is the canonical representative of that equivalence class, as I defined it in my lecture. Please compute $\chi((49,-35))$.

(b, 4pts) True or false: $\forall p$ prime, $\forall a \in \mathbb{Z}_p$: $a^4 \equiv 1 \pmod{p} \implies a^2 \equiv 1 \pmod{p}$. Please explain.

(c, 4pts) True or false: $F_5 = 2^{2^5} + 1$ is a pseudo-prime. Please explain.

(d, 4pts) True or false: $F_5 = 2^{2^5} + 1$ is a Carmichael number. Please explain.

Problem 2 (6 points): For $n \geq 0$, please use congruence theory to prove the following divisibility statement: $27 \mid 2^{5n+1} + 5^{n+2}$.

Problem 3 (6 points): Please make a table of all positive divisors d of 45 and the corresponding $\phi(d)$ values. Also, please verify Gauss's theorem: $45 = \sum_{d>0 \text{ and } d|45} \phi(d)$.

Problem 4 (8 points): Consider $280 = 5 \cdot 7 \cdot 8$ and let $a \in \mathbb{Z}_{280}$ with

$$\begin{aligned} a &\equiv 2 \pmod{5}, \\ a &\equiv 1 \pmod{7}, \\ a &\equiv 0 \pmod{8}. \end{aligned}$$

Please compute $y_0 \in \mathbb{Z}_5$, $y_1 \in \mathbb{Z}_7$ and $y_2 \in \mathbb{Z}_8$ such that

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

Please show all your work.

Problem 5 (10 points): Consider the following instance of the RSA: $n = p \cdot q$ where p and q are primes with $p \equiv q \equiv 2 \pmod{3}$; the public (enciphering) exponent is $k = 3$. Please prove the following.

(a, 4pts) $j = \dfrac{2(p-1)(q-1)+1}{3}$ is an integer.

(b, 6pts) The integer j as defined in (a) is the private (recovery) exponent, that is for all residues $M \in \mathbb{Z}_n$ with $\mathrm{GCD}(M, n) = 1$ one has $(M^3)^j \equiv M \pmod{n}$.