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

919.515.8785 (phone)
919.515.3798 (fax)
kaltofen@math.ncsu.edu (email)
www.math.ncsu.edu/~kaltofen/courses/NumberTheory/Spring05/ (URL)

Your Name: SOLUTION

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 $\chi((49,-35))$.

$(-7,5)$

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

False for $p = 5, a = 2$: $a^4 = 16 \equiv 1 \pmod{5}$,
but $a^2 \equiv 4 \not\equiv 1 \pmod{5}$.

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

True: $641 \mid F_5$*, so* F_5 *is a composite number (see also d).*
But $F_5 \mid 2^{F_5} - 2$ *as shown in Homework 3.*

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

False: $F_5 = 2^{2^5} + 1 \equiv 4^{31} + 1 \equiv 2 \pmod{3}$, *so* $\gcd(3, F_5) = 1$.
But $3^{F_5 - 1} \not\equiv 1 \pmod{F_5} \Longleftrightarrow 3^{F_5} \not\equiv 3 \pmod{F_5}$*, as shown in Homework 3.*

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

$$\begin{aligned} 2^{5n+1} + 5^{n+2} &= 2 \cdot (2^5)^n + 5^2 \cdot 5^n \\ &\equiv 2 \cdot 5^n + 25 \cdot 5^n \pmod{27} \\ &= 27 \cdot 5^n \equiv 0 \pmod{27}. \end{aligned}$$

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: $45 = \sum_{d>0 \text{ and } d|45} \phi(d)$.

Note: $45 = 3^2 \cdot 5$

d	$\phi(d)$
$3^0 \cdot 5^0 = 1$:	1
$3^1 \cdot 5^0 = 3$:	2
$3^2 \cdot 5^0 = 9$:	$9 \cdot (1 - \frac{1}{3}) = 6$
$3^0 \cdot 5^1 = 5$:	4
$3^1 \cdot 5^1 = 15$:	$15 \cdot (1 - \frac{1}{3})(1 - \frac{1}{5}) = 8$
$3^2 \cdot 5^1 = 45$:	$45 \cdot (1 - \frac{1}{3})(1 - \frac{1}{5}) = 24$

Gauss's theorem for $n = 45$: $1 + 2 + 6 + 4 + 8 + 24 = 45$.

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.

$y_0 = 2$
$2 + y_1 \cdot 5 \equiv 1 \pmod 7$
$y_1 \equiv 5^{-1} \cdot 6 \equiv 3 \cdot 6 \equiv 4 \pmod 7$ *(extended Euclidean scheme for* $(7,5)$ *not shown)*
Check: $2 + 4 \cdot 5 = 22 \equiv 1 \pmod 7$

$2 + 4 \cdot 5 + y_2 \cdot 5 \cdot 7 \equiv 0 \pmod 8$
$2 + 4 + 3 \cdot y_2 \equiv 0 \pmod 8$
$y_2 \equiv 3^{-1} \cdot 2 \equiv 3 \cdot 2 \equiv 6 \pmod 8$ *(extended Euclidean scheme for* $(8,3)$ *not shown)*
$a = 2 + 4 \cdot 6 + 6 \cdot 5 \cdot 7 = 232$
Check $232 = 29 \cdot 8 + 0$.

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.

We show that $3 \mid 2(p-1)(q-1)+1$:
$2(p-1)(q-1)+1 \equiv 2(2-1)(2-1)+1 \equiv 2+1 \equiv 0 \pmod 3$.

(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 $(M^3)^j \equiv M \pmod n$.

Since $\phi(n) = (p-1)(q-1)$ *we have*

$$(M^3)^{\frac{2(p-1)(q-1)+1}{3}} = M^{2(p-1)(q-1)+1} = M \cdot (M^{\phi(n)})^2 \equiv M \cdot 1^2 \pmod n,$$

the latter by Euler's theorem.