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, final examination, May 4, 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: 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 10 questions, where each question counts for the explicitly given number of points, adding to a total of **47 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 **three** 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 **120 minutes** to do this test.

Good luck!

Problem 1	____
2	____
3	____
4	____
5	____
Total	____

Problem 1 (16 points)

(a, 4pts) Let p be a positive prime integer. Please define under which conditions a residue $g \in \mathbb{Z}_p$ is a *primitive root*.

1. $g \neq 0$,
2. $\forall i, 1 \leq i \leq p-2 \colon g^i \not\equiv 1 \pmod{p}$.

(b, 4pts) True or false: If p is a positive prime integer and both a and b are quadratic non-residues modulo p, then $c = (a \cdot b) \bmod p$ must be a quadratic residue modulo p. Please explain.

True:
If $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = -1$*, then* $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = +1$*, so* ab *is a Q.R.*

(c, 4pts) The RSA public key cryptosystem is *malleable*. Please explain what that means.

Given a ciphertext $N = E_K(M)$*, one can, without knowledge of* M*, produce the ciphertext for a modified* M*, say* $N' = E_K(2 \cdot M)$.

(d, 4pts) Please state Fermat's last theorem, which was proved by Andrew Wiles in 1994.

$\forall n, x, y, z \in \mathbb{Z}, n \geq 3, x, y, z > 0 \colon x^n + y^n \neq z^n$.

Problem 2 (5 points): Please compute the sum

$$\sum_{d|300,\, d>0} (\mu(d) \cdot d)\,,$$

where μ is the Möbius function. Please show your derivation. [Hint: note that $300 = 2^2 \cdot 3 \cdot 5^2$ and that the function $\mu(m) \cdot m$ is multiplicative.]

$\mu(d) \cdot d$ is multiplicative, so
$F(2^2 \cdot 3 \cdot 5^2) = \sum_{d|300,\, d>0} (\mu(d) \cdot d)$
$= F(2^2) \cdot F(3) \cdot F(5)$
$= (\mu(1) \cdot 1 + \mu(2) \cdot 2 + \mu(2^2) \cdot 4) \cdot (\mu(1) \cdot 1 + \mu(3) \cdot 3) \cdot (\mu(1) \cdot 1 + \mu(5) \cdot 5 + \mu(5^2) \cdot 25)$
$= (1-2) \cdot (1-3) \cdot (1-5) = -8.$

Problem 3 (5 points): **Using the quadratic reciprocity law**, please compute the value of the Legendre symbol $\left(\frac{11}{1019}\right)$ (Burton's book writes $(11/1019)$ instead). Note that $1019 = 92 \cdot 11 + 7$. Please show all your work.

$\left(\frac{11}{1019}\right) \cdot \left(\frac{1019}{11}\right) = (-1)^{\frac{11-1}{2} \cdot \frac{1019-1}{2}} = -1$
$\left(\frac{7}{11}\right) \cdot \left(\frac{11}{7}\right) = (-1)^{\frac{11-1}{2} \cdot \frac{7-1}{2}} = -1$
$\left(\frac{4}{7}\right) = \left(\frac{2}{7}\right)^2 = +1$
$\Longrightarrow \left(\frac{11}{1019}\right) = +1.$

Problem 4 (16 points): Consider the following table of indices (discrete logarithms) for the prime number 17 with respect to the primitive root $g = 3$:

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\mathrm{ind}_3(a)$	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

(a, 5pts) There are $\phi(16)$ residues in $\mathbb{Z}_{17} \setminus \{0\}$ that are primitive roots (including 3). By inspecting the above table, please list all those residues.

a is a prim. root $\iff a = g^i$ with $\gcd(i, 16) = 1$.
So $a = 3^1 = 3, 3^3 \equiv 10, 3^5 \equiv 5, 3^7 \equiv 11, 3^9 \equiv 14, 3^{11} \equiv 7, 3^{13} \equiv 12, 3^{15} \equiv 6$ *are the prim. roots.*
In numeric order: $3, 5, 6, 7, 10, 11, 12, 14$.

(b, 5pts) Using the above table, please solve in $x \in \mathbb{Z}_{17}$ and $y \in \mathbb{Z}_{17}$ the two congruences

$$x^2 \equiv 2 \pmod{17}, \quad y^3 \equiv 2 \pmod{17}$$

Please give all solutions.

$2 \equiv 3^{14} \equiv 3^{14+16} \pmod{17}$
$x_1 \equiv 3^7 \equiv 11$, $x_2 \equiv 3^{15} \equiv 6 \pmod{17}$.

$2 \equiv 3^{14} \equiv 3^{3k} \pmod{17}$,
$3k \equiv 14 \pmod{16}$, $3^{-1} \equiv 11 \pmod{16}$ *(by extended Euclidean algorithm not shown),*
$k \equiv 11 \cdot 14 \equiv -22 \equiv 10 \pmod{16}$,
$y \equiv 3^{10} \equiv 8 \pmod{17}$.
Check: $8^3 \equiv 2^9 \equiv 2^4 \cdot 2^4 \equiv 2 \equiv (-1) \cdot (-1) \cdot 2 \equiv 2 \pmod{17}$.

(c, 6pts) Suppose a residue $M \in \mathbb{Z}_{17}$ has been encrypted by the el-Gamal public key system with public keys $p = 17$, $g = 3$ and $h \equiv 3^s \equiv 7 \bmod 17$. The ciphertext is

$$N = (g^r \bmod 17,\ M \cdot h^r \bmod 17) = (14, 14).$$

Please compute M, showing your derivation. [Hint: you can use the table on the previous page for deriving the private key s, and for powering, multiplication, and reciprocal modulo 17.]

$3^{11} \equiv 7 \pmod{17}$, *so* $s = 11$.
$h^r \equiv (3^s)^r \equiv (3^r)^s \equiv 14^{11} \equiv 3^{9\cdot 11} \equiv 3^{9\cdot 11 \bmod 16} \equiv 3^3 \pmod{17}$.
$M \equiv 14 \cdot 3^{-3} \equiv 14 \cdot 3^{13} \equiv 14 \cdot 12 \equiv (-3)\cdot(-5) \equiv 15 \pmod{17}$.

Problem 5 (5 points): Please compute all primitive Pythagorean triples (x, y, z) such that $x = 12$, $y > 0$ and $z > 0$.

$x = 2st = 12, s > t, y = s^2 - t^2, z = s^2 + t^2$.
$6 = st = 3 \cdot 2 = 6 \cdot 1$
$y_1 = 3^2 - 2^2 = 5, z_1 = 3^2 + 2^2 = 13$
$y_2 = 6^2 - 1^2 = 35, z_1 = 6^2 + 1^2 = 37$