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 5, 2015

Prof. Erich Kaltofen <kaltofen@math.ncsu.edu>

www.math.ncsu.edu/~kaltofen/courses/NumberTheory/Spring15/ (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 6 problems, which are subdivided into 11 questions, where each question counts for the explicitly given number of points, adding to a total of **50 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	_____
6	_____
Total	_____

Problem 1 (16 points)

(a, 4pts) Please describe how Bob, using his private keys of a public key crypto system, can provide a digital signature that Alice can verify using Bob's public keys.

(b, 4pts) True or false: $6^{\phi(1000)} = 6^{400} \equiv 1 \pmod{1000}$. Please explain.

(c, 4pts) Please construct a primitive Pythagorean triple $(8, y, z) \in \mathbb{Z}^3_{>0}$ such that $8^2 + y^2 = z^2$.

(d, 4pts) Please state the recent progress (by Yitang Zhang and followed-up by others) towards proving that there are infinitely prime twins.

Problem 2 (5 points): The following is a trace of the computation of the Legendre symbol $\left(\frac{-146}{233}\right)$ using Jacobi's reciprocity law. Please fill in the blanks.

$\left(\frac{-146}{233}\right) = \left(\frac{-1}{233}\right)\left(\frac{146}{233}\right)$; $\quad \left(\frac{-1}{233}\right) =$ ____________________

$\left(\frac{146}{233}\right) = \left(\frac{2}{233}\right)\left(\frac{73}{233}\right)$; $\quad \left(\frac{2}{233}\right) =$ ____________________

$\left(\frac{73}{233}\right)\left(\frac{233}{73}\right) =$ ____________________; $\quad 233 \bmod 73 = 14$;

$\left(\frac{14}{73}\right) = \left(\frac{2}{73}\right)\left(\frac{7}{73}\right)$; $\quad \left(\frac{2}{73}\right) =$ ____________________

$\left(\frac{7}{73}\right)\left(\frac{73}{7}\right) =$ ____________________; $\quad 73 \bmod 7 = 3$

$\left(\frac{3}{7}\right)\left(\frac{7}{3}\right) =$ ____________________; $\quad 7 \bmod 3 = 1$; $\quad \left(\frac{-146}{233}\right) =$ ____________________

Problem 3 (8 points): Let p be a prime integer with $p \equiv 5 \pmod 8$, that is, $p-1 \equiv 0 \pmod 4$, $p+3 \equiv 0 \equiv 3p+1 \pmod 8$. Let a be a quadratic residue and c a quadratic non-residue modulo p. Please prove that $b^2 \equiv a \pmod p$ for

$$b \equiv 2^{-1}\left((1+c^{\frac{p-1}{4}})a^{\frac{3p+1}{8}} + (1-c^{\frac{p-1}{4}})a^{\frac{p+3}{8}}\right) \pmod p.$$

Problem 4 (10 points): Consider the following table of indices (discrete logarithms) for the prime number 23 with respect to the primitive root $g = 7$:

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
$\mathrm{ind}_7(a)$	0	14	2	6	7	16	1	20	4	21	19	8	10	15	9	12	5	18	17	13	3	11

(a, 4pts) From the above index table, please compute the multiplicative order modulo 23 of the following residues (the exponent that belongs to the following residues module 23), showing your work:

$$2, \quad 3, \quad 4, \quad 5 \quad \in \mathbb{Z}_{23}.$$

(b, 6pts) Using the above table, please solve for $x \in \mathbb{Z}_{23}$, $y \in \mathbb{Z}_{23}$, and $z \in \mathbb{Z}_{23}$ the three congruences

$$x^{19} \equiv 19 \pmod{23}, \quad 19y^{12} \equiv 14 \pmod{23}, \quad 7^{2z} \equiv z^2 \pmod{23}.$$

Please give **all** solutions and show your work.

Problem 5 (6 points): Suppose Alice has encrypted a residue $M \in \mathbb{Z}_{23}$ by the Taher El-Gamal's public key system with public keys $p = 23$, $g = 7$ and $h \equiv 7^s \equiv 16 \bmod 23$. Alice's ciphertext is

$$E = (g^r \bmod 23,\ M \cdot h^r \bmod 23) = (13, 11).$$

Please show how Bob computes M. [Hint: you can use the table on the previous page for deriving Bob's private key s, and for powering, multiplication, and reciprocal modulo 23.]

Problem 6 (5 points): Please find three positive integers $x, y, z \in \mathbb{Z}_{>0}$, $x \neq y$, but not necessarily relatively prime, such that $x^2 + y^2 = z^3$.