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 2, 2017

Prof. Erich Kaltofen <kaltofen@math.ncsu.edu>
www.math.ncsu.edu/~kaltofen/courses/NumberTheory/Spring17/ (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 (17 points)

(a, 4pts) Please consider the multiplication table for non-zero residues modulo 14, that is a 13×13 matrix A with entries $a_{i,j} = (i\,j \bmod 14)$ for $1 \leq i, j \leq 13$.
True or false: A is a Latin square. Please explain.

(b, 4pts) True of false: $2^{2016} \equiv 2018 \pmod{4034}$. Please explain. [Hint: $4034 = 2 \cdot 2017$ with 2017 a prime number.]

(c, 4pts) True or false: $\forall s, t$ such that $s \not\equiv t \pmod 2$ and $\mathrm{GCD}(s,t) = 1$: $(2st, s^2 - t^2, s^2 + t^2)$ form a **primitive** Pythagorean triple. Please explain.

(d, 5pts) True or false: there exist positive integers $x, y, z \in \mathbb{Z}_{>0}$ such that $x^4 + y^4 = z^3$. Please explain.

Problem 2 (5 points): The following is a trace of the computation of the Legendre symbol $\left(\frac{-122}{211}\right)$ using Jacobi's reciprocity law. Please fill in the blanks.

$$\left(\frac{-122}{211}\right) = \left(\frac{-1}{211}\right)\left(\frac{122}{211}\right); \quad \left(\frac{-1}{211}\right) = \underline{\hspace{4cm}}$$

$$\left(\frac{122}{211}\right) = \left(\frac{2}{211}\right)\left(\frac{61}{211}\right); \quad \left(\frac{2}{211}\right) = \underline{\hspace{4cm}}$$

$$\left(\frac{61}{211}\right)\left(\frac{211}{61}\right) = \underline{\hspace{4cm}}; \quad 211 \bmod 61 = 28;$$

$$\left(\frac{28}{61}\right) = \left(\frac{2^2}{61}\right)\left(\frac{7}{61}\right); \quad \left(\frac{2^2}{61}\right) = \underline{\hspace{4cm}}$$

$$\left(\frac{7}{61}\right)\left(\frac{61}{7}\right) = \underline{\hspace{4cm}}; \quad 61 \bmod 7 = 5$$

$$\left(\frac{5}{7}\right) = \left(\frac{-2}{7}\right) = \left(\frac{-1}{7}\right)\left(\frac{2}{7}\right); \quad \left(\frac{-1}{7}\right) = \underline{\hspace{4cm}};$$

$$\left(\frac{2}{7}\right) = \underline{\hspace{4cm}}; \quad \left(\frac{-122}{211}\right) = \underline{\hspace{1cm}}$$

Problem 3 (8 points): Let p be a prime with $p \equiv 5 \pmod 8$ and let $a \in \mathbb{Z}_p$ be a quadratic residue modulo p. Please prove:

(a, 3pts) If $a^{(p-1)/4} \equiv 1 \pmod p$ then for $b = (a^{(p+3)/8} \bmod p)$ one has $b^2 \equiv a \pmod p$.

(b, 5pts) If $a^{(p-1)/4} \equiv -1 \pmod p$ then for $b = (a^{(p+3)/8}\, 2^{(p-1)/4} \bmod p)$ one has $b^2 \equiv a \pmod p$.

Problem 4 (10 points): Consider the following table of indices (discrete logarithms) for the prime number 23 with respect to the primitive root $g = 11$:

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

(a, 4pts) Please compute the average multiplicative order of the non-zero residues modulo 23, namely

$$\frac{1}{22} \sum_{d \text{ divides } 22} (\text{number of non-zero residues of order } d) \cdot d.$$

(b, 6pts) Using the above table, please solve for $x \in \mathbb{Z}_{23}$, $y \in \mathbb{Z}_{23}$, and $z \in \mathbb{Z}_{2\underline{\mathbf{3}}}$ the three congruences

$$20x^{21} \equiv 21 \pmod{23}, \quad 13y^{10} \equiv 16 \pmod{23}, \quad 11^{-3z} \equiv 4z^3 \pmod{23}.$$

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

Problem 5 (5 points): Suppose Alice has encrypted a residue $M \in \mathbb{Z}_{23}$ by the Taher El-Gamal's public key system with public keys $p = 23$, $g = 11$ and $h \equiv 11^s \equiv 17 \bmod 23$. Alice's ciphertext is

$$E = (g^r \bmod 23,\ M \cdot h^r \bmod 23) = (19, 1).$$

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 $x, y, z \in \mathbb{Z}_{>0}$ such that $\mathrm{GCD}(x, y, z) = 1$, x is even, $x \geq 4$ and $x^4 + y^2 = z^2$.