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 22, 2018

Prof. Erich Kaltofen <kaltofen@math.ncsu.edu>
www.math.ncsu.edu/~kaltofen/courses/NumberTheory/Spring18/ (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 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 **75 minutes** to do this test.

Good luck!

Problem 1 _____

2 _____

3 _____

4 _____

5 _____

6 _____

Total _____

If you are taking the exam later, please sign the following statement:

I, _____*, affirm that I have no knowledge of the contents of this exam.*

_____

Signature

Problem 1 (16 points)

(a, 4pts) True or false: $\forall a \in \mathbb{Z}_{16}, a$ an odd integer: $a^4 \equiv 1 \pmod{16}$.

(b, 4pts) True or false: $63973 = 7 \cdot 13 \cdot 19 \cdot 37$ is a Carmichael number. Please explain.

(c, 4pts) Please compute 2^{100} mod 100, showing your work. Hint: $100 = 4 \cdot 25$, use Euler's theorem modulo 25.

(d, 4pts) Please show how to compute a^{23} mod n for $a \in \mathbb{Z}_n$ with 6 multiplications modulo n.

Problem 2 (6 points): Please prove for all prime numbers $p \geq 2$ and for all integers k with $1 \leq k \leq p-1$ that the binomial coefficient $\binom{p}{k}$ satisfies $\binom{p}{k} \equiv 0 \pmod{p}$.

Problem 3 (6 points): Please determine **two** integers $n_1 \geq 1, n_2 \geq 1, n_1 \neq n_2$ such that $\phi(n_1) = \phi(n_2) = 20$, where ϕ is Euler's phi-function.

Problem 4 (8 points): Consider $2015 = 31 \cdot 13 \cdot 5$ and let $a \in \mathbb{Z}_{2015}$ with

$$\begin{aligned} a &\equiv 18 \pmod{31}, \\ a &\equiv 1 \pmod{13}, \\ a &\equiv 4 \pmod{5}. \end{aligned}$$

Please compute $y_0 \in \mathbb{Z}_{31}$, $y_1 \in \mathbb{Z}_{13}$ and $y_2 \in \mathbb{Z}_5$ such that

$$a = y_0 + y_1 \cdot 31 + y_2 \cdot 31 \cdot 13.$$

Then compute a. Please show all your work.

Problem 5 (5 points): The Miller-Rabin algorithm is a *randomized algorithm of the Monte Carlo kind* for the establishing the **primality** of an integer input. Please explain what that means.

Problem 6 (5 points): Please consider the following (toy) instance of the RSA: the public modulus is $n = 55$ and the public (enciphering) exponent is $k = 27$. Please compute the private deciphering exponent j such that $(M^{27})^j \equiv M \pmod{55}$ (at least for all $M \in U_{55}$). With the computed j, please decipher the message M from the cipher text $C = (M^{27} \bmod 55) = 49$. Please show your work.