Be sure that this examination has 8 pages, including this cover.

The University of British Columbia
Final Examinations – December 2013
Mathematics 312
Instructor: V. Vatsal
Time: 2.5 hours

Name:
Student Number:

Signature:

Special instructions:

1. No calculators, books, notes, or other aids allowed.
2. Answer all 6 questions. Each question is worth 10 points, for a total of 60 points.
3. Give your answer in the space provided. If you need extra space, use the back of the page.
4. Show enough of your work to justify your answer. Show ALL steps.

Rules governing examinations:

1. Each candidate should be prepared to produce his/her library/AMS card upon request.
2. No candidate shall be permitted to enter the examination room after the expiration of one half hour, or to leave during the first half hour of the examination. Candidates are not permitted to ask questions of the invigilators, except in cases of supposed errors or ambiguities in the examination questions.
3. Candidates guilty of any of the following or similar practices shall be immediately dismissed from the examination, and and shall be liable to disciplinary action:

   a) Making use of any books, papers or memoranda, other than those authorized by the examiners.

   b) Speaking or communicating with other candidates.

   c) Purposely exposing written papers to the view of other candidates. The plea of accident or forgetfulness will not be received.

Problem 1:

a) Suppose $m > 1$ is a positive integer and $(a, m) = 1$. State the definition of the inverse $\overline{a}$ of a modulo m.

b) Find the inverse of 16 modulo 19 and solve the congruence $16X \equiv 2 \pmod{19}$.

Problem 2:

a) Find all solutions to the congruence $X^2 \equiv 1 \pmod{55}$.

b) Find the last three decimal digits of the number 7^{999}.

Problem 3:

a) State the definition of the Euler ϕ function.

b) Determine if $2821 = 7 \times 13 \times 31$ is a Carmichael number. Explain your answer. (Recall that a Carmichael number is a compositive integer n such that $a^{n-1} \equiv 1 \pmod{n}$ whenever $(a, n) = 1$.

Problem 4:

a) Decrypt OAPB, which was encrypted by the affine transformation $C \equiv 7P + 11 \bmod 26$.

b) Find $9^{23} \bmod 71$.

Problem 5:

a) Suppose a, b, m are integers with $(a, m) = (b, m) = 1$. Let $s = \mathrm{ord}_m(a)$ and $t = \mathrm{ord}_m(b)$ and suppose that $(s, t) = 1$. Then show that $\mathrm{ord}_m(ab) = st$. (This was a homework problem.)

b) Suppose that p is a prime with $p \equiv 3 \bmod 4$. Show that there is no solution to the congruence $X^2 \equiv= -1 \bmod p$. (This problem was on the midterm.)

Problem 6:

a) Find all integers n such that $n!$ is divisible by 7^9 but NOT divisible by 7^{10}.

b) Let a and b denote positive integers. Let m denote the least common multiple of a and b, and let d denote the greatest common divisor of a and b. Then show that $ab = md$. (Hint: use the prime factorization of a and b.)

Problem 6:

a) Suppose that p is an odd prime and let a be a primitive root mod p. Then show that $a^{(p-1)/2} \equiv -1 \bmod p$.

b) Suppose p is an odd prime and let a be a primitive root mod p. Show that $-a$ is a primitive root mod p if and only if $p \equiv 1 \pmod 4$.