

UNIVERSITY OF MANITOBA

DATE: December 7, 2012

COURSE NO: MATH 2500
EXAMINATION:
Introduction to Number Theory

FINAL EXAMINATION
TITLE PAGE
TIME: 3 hours
EXAMINER: M. Davidson

FAMILY NAME: (Print in ink) _____

GIVEN NAME(S): (Print in ink) _____

STUDENT NUMBER: _____

SEAT NUMBER: _____

SIGNATURE: (in ink) _____
(I understand that cheating is a serious offense)

INSTRUCTIONS TO STUDENTS:

This is a 3 hour exam. **Please show your work clearly.**

A single line display, simple calculator is permitted. No texts, notes, or other aids are permitted. There are no cellphones or electronic translators, or other electronic devices permitted.

This exam has a title page and 13 pages of questions, which includes one page with a table of primes. Please check that you have all the pages. You may remove the table if you wish, but be careful not to loosen the staples.

The value of each question is indicated in the lefthand margin beside the statement of the question. The total value of all questions is 110 points.

Answer all questions on the exam paper in the space provided beneath the question. If you need more room, you may continue your work on the reverse side of the page, but **CLEARLY INDICATE** that your work is continued.

Question	Points	Score
1	10	
2	10	
3	8	
4	12	
5	8	
6	10	
7	18	
8	6	
9	12	
10	8	
11	8	
Total:	110	

UNIVERSITY OF MANITOBA

DATE: December 7, 2012

FINAL EXAMINATION

COURSE NO: MATH 2500

PAGE: 1 of 13

EXAMINATION:

TIME: 3 hours

Introduction to Number Theory

EXAMINER: M. Davidson

[10] 1. (a) Find $(2002, 897)$.

(b) Find all integer solutions to $2002x + 897y = (2002, 897)$.

UNIVERSITY OF MANITOBA

DATE: December 7, 2012

FINAL EXAMINATION

COURSE NO: MATH 2500

PAGE: 2 of 13

EXAMINATION:

TIME: 3 hours

Introduction to Number Theory

EXAMINER: M. Davidson

- [10] 2. For each of the following linear congruences, find out how many solutions there are. If solutions exist, you need *NOT* find them, but you should state a reason for your answer.

(a) $3388x \equiv 42 \pmod{7413}$

(b) $2500x \equiv 42 \pmod{2012}$

UNIVERSITY OF MANITOBA

DATE: December 7, 2012

FINAL EXAMINATION

COURSE NO: MATH 2500

PAGE: 3 of 13

EXAMINATION:

TIME: 3 hours

Introduction to Number Theory

EXAMINER: M. Davidson

- [8] 3. Given the public information of an RSA encryption is $(n, e) = (2599, 107)$, find the decrypt key d .
[Hint: One of the two prime factors of n is less than 30.]

UNIVERSITY OF MANITOBA

DATE: December 7, 2012

FINAL EXAMINATION

COURSE NO: MATH 2500

PAGE: 4 of 13

EXAMINATION:

TIME: 3 hours

Introduction to Number Theory

EXAMINER: M. Davidson

- [12] 4. Recall $d(n)$ is the number of divisors of n , $\sigma(n)$ is the sum of the divisors of n and $\phi(n)$ is the Euler phi function. ($229320 = 2^3 \cdot 3^2 \cdot 5 \cdot 7^2 \cdot 13$)

(a) What is $d(229320)$? $\sigma(229320)$? $\phi(229320)$?

(b) Show that if n is a square then $d(n)$ is odd.

(c) Under what conditions is $\phi(2n) = \phi(n)$? (Justify your answer.)

UNIVERSITY OF MANITOBA

DATE: December 7, 2012

FINAL EXAMINATION

COURSE NO: MATH 2500

PAGE: 5 of 13

EXAMINATION:

TIME: 3 hours

Introduction to Number Theory

EXAMINER: M. Davidson

[8] 5. (a) Define what is meant for a number n to be *abundant*.

(b) Define what is meant for a number n to be *deficient*.

(c) For what values of a is $2^a \cdot 11$ abundant?

(d) Show that there are infinitely many deficient numbers.

UNIVERSITY OF MANITOBA

DATE: December 7, 2012

FINAL EXAMINATION

COURSE NO: MATH 2500

PAGE: 6 of 13

EXAMINATION:

TIME: 3 hours

Introduction to Number Theory

EXAMINER: M. Davidson

[10] 6. (a) Use Wilson's Theorem to find the least residue of $235! \pmod{239}$.

(b) Use Gauss's Lemma to decide if 3 is a quadratic residue or quadratic non-residue modulo 31.
(No credit will be given for any other method.)

UNIVERSITY OF MANITOBA

DATE: December 7, 2012

FINAL EXAMINATION

COURSE NO: MATH 2500

PAGE: 7 of 13

EXAMINATION:

TIME: 3 hours

Introduction to Number Theory

EXAMINER: M. Davidson

[18] 7. (a) How many primitive roots does the prime 71 have?

(b) What are the possible orders a modulo 71 when $(a, 71) = 1$?

(c) Show that 7 is a primitive root of 71.

Continued on next page. \Rightarrow

UNIVERSITY OF MANITOBA

DATE: December 7, 2012

FINAL EXAMINATION

COURSE NO: MATH 2500

PAGE: 8 of 13

EXAMINATION:

TIME: 3 hours

Introduction to Number Theory

EXAMINER: M. Davidson

- (d) List two other primitive roots. (How do you know they are primitive roots?)
These should be in least residue.

- (e) Given that $7^6 = 117649 = 71(1657) + 2$, what is the order of 2 modulo 71?
What is the order of 14 mod 71?

UNIVERSITY OF MANITOBA

DATE: December 7, 2012

FINAL EXAMINATION

COURSE NO: MATH 2500

PAGE: 9 of 13

EXAMINATION:

TIME: 3 hours

Introduction to Number Theory

EXAMINER: M. Davidson

- [6] 8. Suppose that a has order $t \pmod{m}$. What is the order of a^2 if:
- (a) t is odd? (Justify your answer.)

(b) t is even? (Justify your answer.)

UNIVERSITY OF MANITOBA

DATE: December 7, 2012

FINAL EXAMINATION

COURSE NO: MATH 2500

PAGE: 10 of 13

EXAMINATION:

TIME: 3 hours

Introduction to Number Theory

EXAMINER: M. Davidson

- [12] 9. Calculate the following Legendre Symbols:
Note: 1723 is prime.

(a) $\left(\frac{499}{1723}\right)$

(b) $\left(\frac{113616}{997}\right)$

UNIVERSITY OF MANITOBA

DATE: December 7, 2012

FINAL EXAMINATION

COURSE NO: MATH 2500

PAGE: 11 of 13

EXAMINATION:

TIME: 3 hours

Introduction to Number Theory

EXAMINER: M. Davidson

- [8] 10. We note that for the prime number $p = 2819$, that $2p + 1 = 5639$ is also prime. Use Euler's Criterion for quadratic residues (together with calculation of Legendre symbols) to decide which, if any, of 2, 3, 5, or 7 are primitive roots of 5639.

UNIVERSITY OF MANITOBA

DATE: December 7, 2012

FINAL EXAMINATION

COURSE NO: MATH 2500

PAGE: 12 of 13

EXAMINATION:

TIME: 3 hours

Introduction to Number Theory

EXAMINER: M. Davidson

[8] 11. (a) Give a formula for finding integer solutions to $x^2 + y^2 = z^2$.

(b) Under what conditions is this solution fundamental?

(c) Find a Pythagorean triple where one of the values is:

i. 11.

ii. 14.

UNIVERSITY OF MANITOBA

DATE: December 7, 2012

COURSE NO: MATH 2500

EXAMINATION:

Introduction to Number Theory

FINAL EXAMINATION

PAGE: 13 of 13

TIME: 3 hours

EXAMINER: M. Davidson

NAME: (Print in ink) _____

FILL IN THE ABOVE IF YOU WISH TO REMOVE THIS SHEET FROM THE EXAM PAPER

The following is a list of all primes less than 1000

2	3	5	7	11	13	17	19
23	29	31	37	41	43	47	53
59	61	67	71	73	79	83	89
97	101	103	107	109	113	127	131
137	139	149	151	157	163	167	173
179	181	191	193	197	199	211	223
227	229	233	239	241	251	257	263
269	271	277	281	283	293	307	311
313	317	331	337	347	349	353	359
367	373	379	383	389	397	401	409
419	421	431	433	439	443	449	457
461	463	467	479	487	491	499	503
509	521	523	541	547	557	563	569
571	577	587	593	599	601	607	613
617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719
727	733	739	743	751	757	761	769
773	787	797	809	811	821	823	827
829	839	853	857	859	863	877	881
883	887	907	911	919	929	937	941
947	953	967	971	977	983	991	997