UNIVERSITY OF MANITOBA

DATE: December 7, 2012

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

COURSE NO: MATH 2500
EXAMINATION:
Introduction to Number Theory

ANSWER KEY

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
PAGE: 1 of 13
TIME: 3 hours
EXAMINER: M. Davidson

COURSE NO: MATH 2500
EXAMINATION:
Introduction to Number Theory

---

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

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

a) $2002 = 897(2) + 208$

$897 = 208(4) + 65$

$208 = 65(3) + 13$

$65 = 13(5) + 0$

Hence $(2002, 897) = 13$

b) $13 = 208 + 65(-3)$

$= 208 + [897 + 208(-4)](-3)$

$= 897(-3) + 208(13)$

$= 897(-3) + [2002 + 897(-2)](13)$

$= 2002(13) + 897(-29)$

So $2002(13) + 897(-29) = 13$

So all solutions are:

$x = 13 + \frac{897}{13}t = 13 + 69t$

$y = -29 - \frac{2002}{13}t = -29 - 154t$

---

[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) $3388x \equiv 42 \pmod{7413}$

$7413 = 3388(2) + 637$

$3388 = 637(5) + 203$

$637 = 203(3) + 28$

$203 = 28(7) + 7$

$28 = 7(4) + 0$

Since $(3388, 7413) = 7$ and $7 \mid 42$

there are 7 solutions

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

$2500 = 2012(1) + 488$

$2012 = 488(4) + 60$

$488 = 60(8) + 8$

$60 = 8(7) + 4$

$8 = 4(2) + 0$

Since $(2500, 2012) = 4$ and $4 \nmid 42$

there are no solutions

---

[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.]

$2599 = 23 \cdot 113$

and so $\phi(2599) = \phi(23)\,\phi(113)$

$= 22 \cdot 112$

$= 2464$

Now we know $de \equiv 1 \bmod n$ so we must solve

$107d \equiv 1 \bmod 2464$

$2464 = 107(23) + 3$
$107 = 3(35) + 2$
$3 = 2(1) + 1$
$2 = 1(2) + 0$

$1 = 3 + 2(-1)$
$= 3 + [107 + 3(-35)](-1)$
$= 107(-1) + 3(36)$
$= 107(-1) + [2464 + 107(-23)](36)$
$= 2464(36) + 107(-829)$

Now $(107)(-829) \equiv 1 \bmod 2464$

So $d \equiv -829 \equiv 1635 \bmod 2464$

The decrypt key is 1635.

---

[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 $d(229320)$? $\sigma(229320)$? $\phi(229320)$?

$d(229320) = d(2^3)d(3^2)d(5)d(7^2)d(13) = 4 \cdot 3 \cdot 2 \cdot 3 \cdot 2 = 144$

$\sigma(229320) = (2^4-1)\left(\frac{3^3-1}{3-1}\right)(6)\left(\frac{7^3-1}{7-1}\right)(14)$

$= 15 \cdot 13 \cdot 6 \cdot 57 \cdot 14 = 933660$

$\phi(229320) = 2^2(2-1)\,3(3-1)(5-1)\,7(7-1)(13-1)$

$= 4 \cdot 3 \cdot 2 \cdot 4 \cdot 7 \cdot 6 \cdot 12 = 48384$

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

Suppose n is a square, so $n = m^2$. If the prime power decomposition of m is $p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ then the prime power decomposition of $n = p_1^{2e_1} p_2^{2e_2} \cdots p_r^{2e_r}$.

Now $d(n) = d(p_1^{2e_1})\,d(p_2^{2e_2}) \cdots d(p_r^{2e_r})$

$= (2e_1+1)(2e_2+1) \cdots (2e_r+1)$

So every term in this product, $(2e_i+1)$, is odd, so $d(n)$ is odd.

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

If n is odd then $(n,2) = 1$ and so

$\phi(2n) = \phi(2)\,\phi(n)$

$= \phi(n)$.

[(Further:)

Also, if n is even, then $n = 2^e m$ where m is odd, so

$\phi(2n) = \phi(2^{e+1}m) = 2^e \cdot \phi(m)$

$= 2(2^{e-1}\phi(m))$

$= 2\,\phi(n)$.

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

n is abundant if

$$\sigma(n) - n > n$$

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

n is deficient if

$$\sigma(n) - n < n$$

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

$$\sigma(2^a \cdot 11) - 2^a \cdot 11 > 2^a \cdot 11$$

$$\sigma(2^a)\sigma(11) > 2^{a+1} \cdot 11$$

$$(2^{a+1} - 1)(12) > 2^{a+1} \cdot 11$$

$$12 \cdot 2^{a+1} - 12 > 2^{a+1} \cdot 11$$

$$2^{a+1} > 12$$

$$\therefore a + 1 \geq 4$$

$$\boxed{a \geq 3}$$

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

If p is prime then

$$\sigma(p) - p = (p+1) - p = 1 < p$$

all primes are deficient

[10] 6. (a) Use Wilson's Theorem to find the least residue of 235! (mod 239).

$238! \equiv -1 \mod 239$

$(238)(237)(236)235! \equiv -1 \mod 239$

$(-1)(-2)(-3)\,235! \equiv -1 \mod 239$

$-6\,(235!) \equiv -1 \mod 239$

$6\,(235!) \equiv 1 \mod 239$

$235! \equiv 40 \mod 239$

$239 = 6(39) + 5$

$6 = 5(1) + 1$

$1 = 6 + 5(-1)$

$= 6 + [239 + 6(-39)](-1)$

$= 239(-1) + 6(40)$

The least residue, modulo 239, of 235! is 40.

(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.)

$\frac{p-1}{2} : \frac{31-1}{2} = \frac{30}{2} = 15$

So

(mult 3) 3 6 9 12 15 18 21 24 27 30 33 36 39 42 45

(least residue mod 31) 3 6 9 12 15 18 21 24 27 30 2 5 8 11 14

Larger than $\frac{p-1}{2}$: (18, 21, 24, 27 & 30) so $g = 5$

so $\left(\frac{3}{31}\right) = (-1)^5 = -1$

Hence 3 is a quadratic nonresidue

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

$p-1 = 71-1 = 70 = 2 \cdot 5 \cdot 7$

$\phi(70) = \phi(2)\phi(5)\phi(7)$
$= 1 \cdot 4 \cdot 6 = 24$

So 71 has 24 primitive roots.

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

(all divisors of 70)

1, 2, 5, 7, 10, 14, 35, 70

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

[Check all orders < 70]

$7^1 \equiv 7 \mod 71$

$7^2 \equiv 49 \mod 71$

$7^5 \equiv 16807 \equiv 51 \mod 71$

$7^7 \equiv 49 \cdot 51 \equiv 2499 \equiv 14 \mod 71$

$7^{10} \equiv (7^5)^2 \equiv 51^2 \equiv 2601 \equiv 45 \mod 71$

$7^{14} \equiv (7^7)^2 \equiv 14^2 \equiv 196 \equiv 54 \mod 71$

$7^{35} \equiv \left(\frac{7}{71}\right) \equiv -\left(\frac{71}{7}\right) \equiv -\left(\frac{1}{7}\right) \equiv -1 \mod 71$

[note: If $7^{35} \equiv -1 \mod 71$, the only other orders that need be checked are 2, 10 & 14]

Since 7 does not have order 1, 2, 5, 7, 10, 14 or 35, it must have order 70, and is hence a primitive root.

Continued on next page. ⇒

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

7^k is a primitive root iff $(k, 70) = 1$

[The 24 numbers relatively prime to 70 are:
1, 3, 9, 11, 13, 17, 19, 23, 27, 29, 31, 33, 37, 39, 41, 43, 47, 51,
53, 57, 59, 61, 67, 69]

Some other primitive roots:

$7^3 \equiv 343 \equiv 59 \mod 71$ — 59 is a prim. root.

$7^9 \equiv 49 \cdot 7^7 \equiv 49 \cdot 14 \equiv 686 \equiv 47 \mod 71$ — 47 is a prim. root

$7^{11} \equiv 7^{10} \cdot 7 \equiv 45 \cdot 7 \equiv 315 \equiv 31 \mod 71$ — 31 is a prim. root

$7^{13} \equiv 7^{11} \cdot 49 \equiv 31 \cdot 49 \equiv 1519 \equiv 28 \mod 71$ — 28 is a prim. root.

(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?

{using order of g^k is $\frac{p-1}{(p-1,k)}$}

Since $2 \equiv 7^6 \mod 71$, the order of 2

is $\frac{70}{(70,6)} = \frac{70}{2} = 35$

Since $14 \equiv 7^7 \mod 71$, the order of 14

is $\frac{70}{(70,7)} = \frac{70}{7} = 10$

[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.)

Since $(2,t)=1$, the order of a^2 is the same as the order of a.

So a^2 has order t.

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

Since $(2,t)=2$, the order of a^2 CANNOT be t.

Suppose the order of a^2 were s. Then

$(a^2)^s \equiv a^{2s} \equiv 1 \mod m$, so $t \mid 2s \Rightarrow t/2 \mid s$

and

$(a^2)^{t/2} \equiv a^t \equiv 1 \mod m$ so $s \mid t/2$.

so we get $s = t/2$.

So the order of a^2 is $t/2$.

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

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

$499 \equiv 3 \bmod 4$

$1723 \equiv 3 \bmod 4$

$= -1\left(\frac{1723}{499}\right) = -1\left(\frac{226}{499}\right)$

$1723 \equiv 226 \bmod 499$

$= -1\left(\frac{2}{499}\right)\left(\frac{113}{499}\right)$

$499 \equiv 3 \bmod 8$

$113 \equiv 1 \bmod 4$

$= (-1)(-1)\left(\frac{499}{113}\right) = \left(\frac{47}{113}\right)$

$499 \equiv 47 \bmod 113)$

$= \left(\frac{113}{47}\right) = \left(\frac{19}{47}\right) = (-1)\left(\frac{47}{19}\right)$

$113 \equiv 19 \bmod 47$

$19 \equiv 47 \equiv 3 \bmod 4$

$47 \equiv 9 \bmod 19$

$= (-1)\left(\frac{9}{19}\right) = -1$

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

$113616 = 2^4 \cdot 3^3 \cdot 263$

$= \left(\frac{2^4}{997}\right)\left(\frac{3^3}{997}\right)\left(\frac{263}{997}\right) = \left(\frac{3}{997}\right)\left(\frac{263}{997}\right)$

$997 \equiv 1 \bmod 4$

$= \left(\frac{997}{3}\right)\left(\frac{997}{263}\right) = \left(\frac{1}{3}\right)\left(\frac{208}{263}\right) = \left(\frac{2^4}{263}\right)\left(\frac{13}{263}\right)$

$997 \equiv 1 \bmod 3$

$997 \equiv 208 \bmod 263$

$= \left(\frac{13}{263}\right) = \left(\frac{263}{13}\right) = \left(\frac{3}{13}\right) = \left(\frac{13}{3}\right) = \left(\frac{1}{3}\right)$

$13 \equiv 1 \bmod 4$

$263 \equiv 3 \bmod 13$

$13 \equiv 1 \bmod 3$

$= 1$

[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.

We know that any element mod 5639 will have order 1, 2, 2819 or 5638.

(obviously) the orders of 2, 3, 5 & 7 are not 1 or 2.

If they are primitive roots, then they will not have order 2819.

Using Euler's Criterion, $a^{2819} \equiv \left(\frac{a}{5639}\right) \mod 5639$

and so

$\left(\frac{2}{5639}\right) = 1$ since $5639 \equiv 7 \mod 8$

$\left(\frac{3}{5639}\right) = -1\left(\frac{5639}{3}\right) = -1\left(\frac{2}{3}\right) = (-1)(-1) = 1$ since $5639 \equiv 3 \mod 4$

$\left(\frac{5}{5639}\right) = \left(\frac{5639}{5}\right) = \left(\frac{4}{5}\right) = 1$ since $5 \equiv 1 \mod 4$, $5639 \equiv 4 \mod 5$

$\left(\frac{7}{5639}\right) = -1\left(\frac{5639}{7}\right) = -1\left(\frac{4}{7}\right) = -1$ $5639 \equiv 7 \equiv 3 \mod 4$, $5639 \equiv \mod 7$

Hence 7 does not have order 2819, so it must have order 5638, and is hence a primitive root.

[The orders of 2, 3 & 5 are all 2819]

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

a solution $x=a$ $y=b$ $z=c$ is

$a = 2mn$

$b = m^2 - n^2$

$c = m^2 + n^2$

(b) Under what conditions is this solution fundamental?

It is fundamental if:
m, n are positive integers,

$(m,n) = 1$,

$m > n$,

$m \not\equiv n \mod 2$

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

i. 11.

$36 - 25 = 11$
$6^2 - 5^2 = 11$

$a = 2 \cdot 5 \cdot 6 = 60$

$b = 11$

$c = 36 + 25 = 61$

So

$(60, 11, 61)$ is a triple including 11.

ii. 14.

$14 = 2 \cdot 7 \cdot 1$

$a = 14$

$b = 49 - 1 = 48$

$c = 50$

So

$(14, 48, 50)$ is a triple including 14.

UNIVERSITY OF MANITOBA

DATE: December 7, 2012

FINAL EXAMINATION
PAGE: 13 of 13
TIME: 3 hours
EXAMINER: M. Davidson

COURSE NO: MATH 2500
EXAMINATION:
Introduction to Number Theory

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