UNIVERSITY OF MANITOBA

DATE: April 22, 2010

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

COURSE NO: MATH 2500
EXAMINATION:
Introduction to Number Theory

FAMILY NAME: (Print in ink) _____

GIVEN NAME(S): (Print in ink) Answer Key

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, 14 pages of questions, which includes 1 blank pages for rough work and one page with a table of primes. Please check that you have all the pages. You may remove the blank page and table if you want, 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 150 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	14	
2	12	
3	10	
4	12	
5	20	
6	18	
7	20	
8	14	
9	10	
10	20	
Total:	150	

UNIVERSITY OF MANITOBA

DATE: April 22, 2010

FINAL EXAMINATION
PAGE: 1 of 14
TIME: 3 hours
EXAMINER: M. Davidson

COURSE NO: MATH 2500
EXAMINATION:
Introduction to Number Theory

---

[14] 1. 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. ($169884 = 2^2 \cdot 3^3 \cdot 11^2 \cdot 13$)

(a) What is $d(169884)$? $\sigma(169884)$? $\phi(169884)$?

$d(169884) = d(2^2)\,d(3^3)\,d(11^2)\,d(13) = 3 \cdot 4 \cdot 3 \cdot 2 = 72$

$\sigma(169884) = \sigma(2^2)\sigma(3^3)\sigma(11^2)\sigma(13) = \left[\left(\frac{2^3-1}{2-1}\right)\left(\frac{3^4-1}{3-1}\right)\left(\frac{11^3-1}{11-1}\right)\left(\frac{13^2-1}{13-1}\right)\right]$

$= (1+2+4)(1+3+9+27)(1+11+121)(1+13) = 7 \cdot 40 \cdot 133 \cdot 14$

$= 521\,360$

$\phi(169884) = \phi(2^2)\,\phi(3^3)\,\phi(11^2)\,\phi(13)$

$= 2(2-1)\,3^2(3-1)\,11(11-1)(13-1) = 47520$

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

Let $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ be the prime power decomposition of n. Then $d(n) = (e_1+1)(e_2+1)\cdots(e_k+1)$.

Since $d(n)$ is odd, each factor of $d(n)$ must be odd. So for $1 \le j \le k$, e_j+1 is odd, hence e_j is even. So for some integer f_j; $e_j = 2f_j$.

So $n = p_1^{2f_1} p_2^{2f_2} \cdots p_k^{2f_k} = \left(p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}\right)^2$;

n is a square.

(c) Prove that if $c \mid ab$ and $(c, a) = d$ then $c \mid db$.

Since $(c,a) = d$, there are integers s and t such that $cs + at = d$. Multiplying by b we get

$cbs + abt = bd$.

Since $c \mid c$ and $c \mid ab$ then $c \mid c(bs) + ab(t)$,

and so $c \mid bd$.

[12] 2. Find all solutions to the following Diophantine equations:

(a) $2743\ x + 663\ y = 42$

(b) $2166\ x + 678\ y = 42$

a) $2743 = 663(4) + 91$

$663 = 91(7) + 26$

$91 = 26(3) + 13$

$26 = 13(2) + 0$

Since $(2743, 663) = 13$ and $13 \nmid 42$, the equation $2743x + 663y = 42$ has no solutions.

b) $2166 = 678(3) + 132$

$678 = 132(5) + 18$

$132 = 18(7) + 6$

$18 = 6(3) + 0$

(Since $(2166, 678) = 6$ and $42 = 6 \cdot 7$, solutions exist)

$6 = 132 + 18(-7)$

$= 132 + [678 + 132(-5)](-7)$

$= 678(-7) + 132(36)$

$= 678(-7) + [2166 + 678(-3)](36)$

$= 2166(36) + 678(-115)$

$2166(36) + 678(-115) = 6$

$2166(252) + 678(-805) = 42$

all solutions are

$x = 252 + \frac{678}{6}t = 252 + 113t$

$y = -805 - \frac{2166}{6}t = -805 - 361t$

[10] 3. Prove the following is true for $n \geq 1$ using induction:

$$1+4+7+10+\ldots+(6n-2) = n(6n-1).$$

Let $P(n)$ be the statement

$$1+4+7+10+\cdots+(6n-2) = n(6n-1).$$

If $n=1$

(Since $6(1)-2=4$) $\quad 1+4=5$

and $\quad (1)(6(1)-1)=5$

$P(1)$ is true.

Suppose $P(k)$ is true;

$$1+4+7+10+\cdots+(6k-2) = k(6k-1)$$

Then

$$\begin{aligned}
&1+4+7+10+\cdots+(6(k+1)-2) \\
&= 1+4+7+10+\cdots+(6k-2)+(6k+1)+(6k+4) \\
&= k(6k-1)+(6k+1)+(6k+4) \\
&= 6k^2-k+12k+5 \\
&= 6k^2+11k+5 \\
&= (k+1)(6k+5) \\
&= (k+1)(6(k+1)-1)
\end{aligned}$$

Hence $P(k+1)$ is also true.

Since $P(1)$ is true and $P(k)$ implies $P(k+1)$ then by PMI, $P(n)$ is true for all $n \geq 1$.

[12] 4. Write as a single congruence (if possible):

$x \equiv 3 \mod 43$
$x \equiv 5 \mod 47$
$x \equiv 27 \mod 107$

$x = 3 + 43k_1$

$3 + 43k_1 \equiv 5 \mod 47$

$43k_1 \equiv 2 \mod 47$

$(-12)43k_1 \equiv (-12)2 \mod 47$

$k_1 \equiv -24 \equiv 23 \mod 47$

$47 = 43(1) + 4$
$43 = 4(10) + 3$
$4 = 3(1) + 1$

$1 = 4 + 3(-1)$
$= 4 + [43 + 4(-10)](-1)$
$= 43(-1) + 4(11)$
$= 43(-1) + [47 + 43(-1)](11)$
$= 47(11) + 43(-12)$

$k_1 = 23 + 47k_2$

$x = 3 + 43(23 + 47k_2)$
$= 992 + 2021k_2$

$992 + 2021k_2 \equiv 27 \mod 107$

$2021k_2 \equiv -965 \mod 107$

$95k_2 \equiv 105 \mod 107$

$(-9)95k_2 \equiv (-9)105 \mod 107$

$k_2 \equiv -945 \equiv 18 \mod 107$

$107 = 95(1) + 12$
$95 = 12(7) + 11$
$12 = 11(1) + 1$

$1 = 12 + 11(-1)$
$= 12 + [95 + 12(-7)](-1)$
$= 95(-1) + 12(8)$
$= 95(-1) + [107 + 95(-1)](8)$
$= 107(8) + 95(-9)$

$k_2 = 18 + 107k_3$

$x = 992 + 2021(18 + 107k_3)$

$= 37\,370 + 216\,247k_3$

As a single congruence:

$x \equiv 37\,370 \mod 216\,247$

[20] 5. (a) i. State Fermat's Theorem.

For p a prime, $(a,p)=1$

$$a^{p-1} \equiv 1 \bmod p$$

ii. Find the least residue of 187^{2312} (mod) 463.

Since 463 is prime $187^{462} \equiv 1 \bmod 463$

So $187^{2312} \equiv (187)^{462(5)+2} \bmod 463$

$\equiv (187^{462})^5 \cdot 187^2 \bmod 463$

$\equiv 1^5 \cdot 34969 \bmod 463$

$\equiv 244 \bmod 463$

(b) i. State Eulers's Theorem.

If $(a,m)=1$ then $a^{\phi(m)} \equiv 1 \bmod m$

ii. Find the least residue of 187^{2312} (mod) 468.

$468 = 2^2 \cdot 117 = 2^2 \cdot 3^2 \cdot 13$

So $\phi(468) = 2 \cdot 3(3-1)(13-1) = 144$

$187^{2312} \equiv (187^{144})^{16} \cdot 187^8 \bmod 468$

$\equiv 1^{16} (187^2)^4 \bmod 468$

$\equiv (337^2)^2 \bmod 468$

$\equiv 313^2 \bmod 468$

$\equiv 157 \bmod 468$

(c) i. State Wilson's Theorem.

p is prime iff $(p-1)! \equiv -1 \bmod p$

ii. Find the least residue of 453! (mod) 457.

Since 457 is prime $456! \equiv -1 \bmod 457$

So $(456)(455)(454)\,453! \equiv -1 \bmod 457$

$(-1)(-2)(-3)\,453! \equiv -1 \bmod 457$

$6(453!) \equiv 1 \bmod 457$

$457 = 6(76) + 1$

$1 = 457 + 6(-76)$

$(-76)(6)(453!) \equiv (-76)1 \bmod 457$

$453! \equiv -76 \equiv 381 \bmod 457$

(d) i. State Gauss's Lemma.

If among the least residues of $a, 2a, 3a, \ldots, \frac{p-1}{2}a \pmod p$ there are g greater than $\frac{p-1}{2}$ then $\left(\frac{a}{p}\right) = (-1)^g$

ii. Use Gauss's Lemma to find if 7 is a quadratic residue or nonresidue modulo 19.

$\frac{19-1}{2} = 9$

na	7	14	21	28	35	42	49	56	63
mod 19	7	14	2	9	16	4	11	18	6
		*			*		*	*	

Since there are 4 least residues greater than 9,

$\left(\frac{7}{19}\right) = (-1)^4 = 1$, hence 7 is a quadratic residue of 19.

[18] 6. Calculate the following Legendre Symbols:

(a) $\left(\frac{169884}{751}\right)$ (Recall $169884 = 2^2 \cdot 3^3 \cdot 11^2 \cdot 13$)

$\left(\frac{169884}{751}\right) = \left(\frac{2^2}{751}\right)\left(\frac{3^2}{751}\right)\left(\frac{3}{751}\right)\left(\frac{11^2}{751}\right)\left(\frac{13}{751}\right)$

$13 \equiv 1 \bmod 4$
$751 \equiv 3 \bmod 4$
$13 \equiv 5 \bmod 8$
$5 \equiv 1 \bmod 4$

$= (-1)\left(\frac{751}{3}\right)\left(\frac{751}{13}\right) = (-1)\left(\frac{1}{3}\right)\left(\frac{10}{13}\right)$

$= (-1)\left(\frac{2}{13}\right)\left(\frac{5}{13}\right) = (-1)(-1)\left(\frac{13}{5}\right) = \left(\frac{3}{5}\right)$

$= \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1$

(b) $\left(\frac{733}{787}\right)$

$\left(\frac{733}{787}\right) = \left(\frac{787}{733}\right) = \left(\frac{54}{733}\right) = \left(\frac{3^3 \cdot 2}{733}\right)$

$733 \equiv 1 \bmod 4$
$733 \equiv 5 \bmod 8$

$= \left(\frac{3^2}{733}\right)\left(\frac{3}{733}\right)\left(\frac{2}{733}\right) = \left(\frac{733}{3}\right)(-1)$

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

(c) $\left(\frac{579}{727}\right)$

$\left(\frac{579}{727}\right) = \left(\frac{3 \cdot 193}{727}\right) = \left(\frac{3}{727}\right)\left(\frac{193}{727}\right)$

$727 \equiv 3 \bmod 4$
$193 \equiv 1 \bmod 4$

$= (-1)\left(\frac{727}{3}\right)\left(\frac{727}{193}\right) = (-1)\left(\frac{1}{3}\right)\left(\frac{148}{193}\right) = (-1)\left(\frac{2^2 \cdot 37}{193}\right)$

$= (-1)\left(\frac{2^2}{193}\right)\left(\frac{37}{193}\right) = (-1)\left(\frac{193}{37}\right) = (-1)\left(\frac{8}{37}\right) = (-1)\left(\frac{2^3}{37}\right)$

$37 \equiv 5 \bmod 8$

$= (-1)\left(\frac{2^2}{37}\right)\left(\frac{2}{37}\right) = (-1)(-1) = 1$

[20] 7. (a) How many primitive roots does the prime 79 have?

$p-1 = 78 = 2 \cdot 3 \cdot 13$

$\phi(78) = (2-1)(3-1)(13-1) = 2 \cdot 12 = 24$

79 has 24 primitive roots.

(b) Show that 3 is a primitive root of 79.

The possible orders of an element modulo 79 are:
1, 2, 3, 6, 13, 26, 39 and 78 (divisors of $\phi(79)$)

$3^2 \equiv 9 \mod 79$

$3^3 \equiv 27 \mod 79$

$3^6 \equiv 18 \mod 79$

$3^{13} \equiv 24 \mod 79$

$3^{26} \equiv 23 \mod 79$

$3^{39} \equiv 78 \ (\equiv -1) \mod 79$

Since the order of 3 is not 1, 2, 3, 6, 13, 26 or 39, it must be 78; 3 is a primitive root.

(c) List two other primitive roots. (How do you know they are primitive roots?)

Since $(78,5)=1$ and $(78,7)=1$, the least residues of 3^5 and 3^7 are primitive roots.

$3^5 \equiv 243 \equiv 6 \mod 79$ $\quad 3^7 \equiv 2187 \equiv 54 \mod 79$

6 and 54 are primitive roots. (There are others)

(d) Given that $3^9 = 19683 = 79(229) + 12$, what is the order of 12 mod 79? What is the order of 36 mod 79?

Since $12 \equiv 3^9 \mod 79$, its order is $\frac{78}{(78,9)} = \frac{78}{3} = 26$.

Since $36 \equiv 3^{10} \mod 79$, its order is $\frac{78}{(78,9)} = \frac{78}{2} = 39$.

[14] 8. (a) Are any of the following numbers k-perfect? If so, for what value of k? (Hint: the primes in the prime power decomposition of the following are all less than 50) .

i. 32760

$32760 = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$

$\sigma(32760) = 15 \cdot 13 \cdot 6 \cdot 8 \cdot 14$

$= 131040 = 4(32760)$

Hence 32760 is 4 perfect.

ii. 27720

$27720 = 2 \cdot 3 \cdot$

$\sigma(27720) = 15 \cdot 13 \cdot 6 \cdot 8 \cdot 12$

$= 112\,320$

Since $27720 \nmid 112\,320$, 27720 is not k-perfect.

iii. $523776 = 2^9 \cdot 3 \cdot 11 \cdot 31$

$\sigma(523776) = 1023 \cdot 4 \cdot 12 \cdot 32$

$= 1571328$

$= 3(523776)$

Hence 523776 is 3 perfect

(b) If n is odd and 4-perfect, is $4n$ k-perfect? If so, for what value of k? (Justify your steps carefully!)

Since n is odd $(n, 4) = 1$.

Therefore $\sigma(4n) = \sigma(4)\,\sigma(n)$ (σ is multiplicative)

$= (1+2+4)(4n)$

$= 7(4n)$

So $4n$ is 7 perfect.

[10] 9. (a) For an RSA encryption scheme, the publicly listed (N,e) pair is (2257, 997). Find the secret decrypt key.

$2257 = 37 \cdot 61$

$\phi(2257) = \phi(37)\phi(61) = 36 \cdot 60 = 2160$

If d is the decrypt key then

$997d \equiv 1 \mod 2160$

$2160 = 997(2) + 166$

$997 = 166(6) + 1$

So $1 = 997 + 166(-6)$

$= 997 + [2160 + 997(-2)](-6)$

$= 2160(-6) + 997(13)$

The decrypt key is 13

(b) You have intercepted the coded message 1761, decode it.

If M is the original message then

$M \equiv (1761)^{13} \mod 2257$

$\equiv (1761^2)^6 \cdot 1761 \mod 2257$

$\equiv 3^6 \cdot 1761 \mod 2257$

$\equiv 1283769 \equiv 1793 \mod 2257$

The message decodes to 1793.

[20] 10. (a) Use Euler's Criterion to show:
If p is an odd prime, then

$$\left(\frac{-1}{p}\right) = 1 \quad \text{if} \quad p \equiv 1 \pmod 4$$

and

$$\left(\frac{-1}{p}\right) = -1 \quad \text{if} \quad p \equiv 3 \pmod 4$$

From Euler's criterion we know that

$$\left(\frac{a}{p}\right) = (a)^{\frac{p-1}{2}} \mod p$$

If $p \equiv 1 \mod 4$ then $p = 4k+1$, so $\frac{p-1}{2} = 2k$

$$\left(\frac{-1}{p}\right) \equiv (-1)^{2k} \equiv 1 \mod p, \text{ so } \left(\frac{-1}{p}\right) = 1.$$

If $p \equiv 3 \mod 4$ then $p = 4k+3$, so $\frac{p-1}{2} = 2k+1$

$$\left(\frac{-1}{p}\right) \equiv (-1)^{2k+1} \equiv -1 \mod p \quad \text{so} \quad \left(\frac{-1}{p}\right) = -1.$$

Question continued on next page.

(b) Find a similar formula for deciding if -2 is a quadratic residue or nonresidue modulo p where p is an odd prime.
(Hint: this should be in terms of modulo 8.)

Since $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$

If $p \equiv 1 \bmod 8$ then $p \equiv 1 \bmod 4$ so $\left(\frac{2}{p}\right) = 1$ and $\left(\frac{-1}{p}\right) = 1$

so $\left(\frac{-2}{p}\right) = (1)(1) = 1$.

If $p \equiv 3 \bmod 8$ then $p \equiv 3 \bmod 4$ so $\left(\frac{2}{p}\right) = -1$ and $\left(\frac{-1}{p}\right) = -1$

so $\left(\frac{-2}{p}\right) = (-1)(-1) = 1$.

If $p \equiv 5 \bmod 8$ then $p \equiv 1 \bmod 4$ so $\left(\frac{2}{p}\right) = -1$ and $\left(\frac{-1}{p}\right) = 1$

so $\left(\frac{-2}{p}\right) = (-1)(1) = -1$.

If $p \equiv 7 \bmod 8$ then $p \equiv 3 \bmod 4$ so $\left(\frac{2}{p}\right) = 1$ and $\left(\frac{-1}{p}\right) = -1$

So $\left(\frac{-2}{p}\right) = (1)(-1) = -1$

(c) For what values of p (modulo 8) is it possible for both 2 and $p-2$ to be primitive roots of p?

If g is a primitive root of p then $\left(\frac{g}{p}\right) = -1$.

$\left(\frac{2}{p}\right) = -1$ if $p \equiv 3$ or $5 \bmod 8$

$\left(\frac{p-2}{p}\right) = \left(\frac{-2}{p}\right) = -1$ if $p \equiv 5$ or $7 \bmod 8$

The only possible values of p are $p \equiv 5 \bmod 8$.

UNIVERSITY OF MANITOBA

DATE: February 5, 2010

MIDTERM I
TITLE PAGE
TIME: 50 minutes
EXAMINER: M. Davidson

COURSE NO: MATH 2500
EXAMINATION:
Introduction to Number Theory

FAMILY NAME: (Print in ink) ANSWER KEY

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

STUDENT NUMBER: _____

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

INSTRUCTIONS TO STUDENTS:

This is a 50 minute 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, 4 pages of questions and also 2 blank pages for rough work. Please check that you have all the pages. You may remove the blank pages if you want, 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 40 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	7	
3	3	
4	10	
5	10	
Total:	40	

UNIVERSITY OF MANITOBA

DATE: February 5, 2010

MIDTERM I
PAGE: 1 of 4
TIME: 50 minutes
EXAMINER: M. Davidson

COURSE NO: MATH 2500
EXAMINATION:
Introduction to Number Theory

---

[10] 1. Use **mathematical induction** to show that $2+5+8+\ldots+(6n-1)=n(6n+1)$.

Let $P(n)$ be the statement

$$2+5+8+\cdots+(6n-1)=n(6n+1)$$

If $n=1$ Then $2+5=7$

and $1(6+1)=7$

Hence $P(1)$ is true.

Assume $P(k)$ is true:

$$2+5+8+\cdots+(6k-1)=k(6k+1).$$

Then $2+5+8+\cdots+(6(k+1)-1)$

$=2+5+8+\cdots+(6k-1)+(6k+2)+(6k+5)$

$=k(6k+1)+6k+2+6k+5$

$=6k^2+k+12k+7$

$=6k^2+13k+7$

$=(k+1)(6k+7)$

$=(k+1)(6(k+1)+1)$

So $2+5+8+\cdots+(6(k+1)-1)=(k+1)(6(k+1)+1)$; ie $P(k+1)$ is true.

Since $P(1)$ is true and $P(k)$ implies $P(k+1)$, by PMI

$P(n)$ is true for all $n\geq 1$.

[7] 2. (a) Show: If $a \equiv b \pmod{m}$ and $d \mid m$, then $a \equiv b \pmod{d}$. Justify each step.

Since $a \equiv b \bmod m$, we have $m \mid a-b$.

since $m \mid a-b$, there is an integer r such that

$a-b = rm$.

Since $d \mid m$, there is an integer s such that

$ds = m$.

From above we get $a-b = dsr$; since sr is an integer, $d \mid a-b$, hence $a \equiv b \bmod d$.

(b) Using the above, show that the following system has no solution.

$x \equiv 47 \pmod{77}$
$x \equiv 14 \pmod{43}$
$x \equiv 74 \pmod{121}$

$x \equiv 47 \bmod 77$ and $11 \mid 77$ so $x \equiv 47 \bmod 11$ or $x \equiv 3 \bmod 11$

$x \equiv 74 \bmod 121$ and $11 \mid 121$ so $x \equiv 74 \bmod 11$ or $x \equiv 8 \bmod 11$

So there is no x that satisfies the above

[3] 3. For what primes m is the following congruence true :
$1815 \equiv 1542 \pmod{m}$

$m \mid 1815 - 1542$

so $m \mid 273$

The prime power decomposition of 273 is $3 \cdot 7 \cdot 13$

Hence m could be 3 or 7 or 13

---

[10] 4. (a) Use the Euclidean algorithm to find $(7364, 553)$.

(b) Find all solutions to $7364x + 553y = 91$.

(c) Find all solutions to $553x \equiv 91 \pmod{7364}$

a) $7364 = 553(13) + 175$

$553 = 175(3) + 28$

$175 = 28(6) + 7$

$28 = 7(4) + 0$

Hence $(7364, 553) = 7$

b) $7 = 175 + 28(-6)$

$= 175 + [553 + 175(-3)](-6)$

$= 553(-6) + 175(19)$

$= 553(-6) + [7364 + 553(-13)](19)$

$= 7364(19) + 553(-253)$

So $7364(19) + 553(-253) = 7$

$7364(247) + 553(-3289) = 91$

all solutions to $7364x + 553y = 91$ are

$x = 247 + \frac{553}{7}t = 247 + 79t$

$y = -3289 - \frac{7364}{7}t = -3289 - 1052t$

c) The 7 solutions are

919, 1971, 3023, 4075, 5127, 6179, 7231

---

[10] 5. Write the following as a single congruence, if possible. If it is not possible, explain why not.

$x \equiv 2 \pmod 9$
$x \equiv 7 \pmod{13}$
$x \equiv 13 \pmod{380}$

$x \equiv 2 \bmod 9$

So $x = 2 + 9k_1$

$2 + 9k_1 \equiv 7 \bmod 13$

$9k_1 \equiv 5 \bmod 13$

$9k_1 \equiv 18 \bmod 13$

$k_1 \equiv 2 \bmod 13$

$k_1 = 2 + 13k_2$

$x = 2 + 9(2 + 13k_2)$

$= 20 + 117k_2$

Alternately:

$13 = 9(1) + 4$
$9 = 4(2) + 1$
$1 = 9 + 4(-2)$
$= 9 + [13 + 9(-1)](-2)$
$= 13(-2) + 9(3)$

$9k_1 \equiv 5 \bmod 13$
$3 \cdot 9k_1 \equiv 3 \cdot 5 \bmod 13$
$k_1 \equiv 15 \bmod 13$
$k_1 \equiv 2 \bmod 13$

$20 + 117k_2 \equiv 13 \bmod 380$

$117k_2 \equiv -7 \bmod 380$

$k_2 \equiv -91 \bmod 380$

$k_2 \equiv 289 \bmod 380$

$k_2 = 289 + 380k_3$

$x = 20 + 117(289 + 380k_3)$

$= 33833 + 44460k_3$

$380 = 117(3) + 29$
$117 = 29(4) + 1$

$1 = 117 + 29(-4)$
$= 117 + [380 + 117(-3)](-4)$
$= 380(-4) + 117(13)$

The single congruence:

$x \equiv 33833 \pmod{44460}$

UNIVERSITY OF MANITOBA

DATE: March 10, 2010

MIDTERM II
TITLE PAGE
TIME: 50 minutes
EXAMINER: M. Davidson

COURSE NO: MATH 2500
EXAMINATION:
Introduction to Number Theory

FAMILY NAME: (Print in ink) ANSWER KEY

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

STUDENT NUMBER: _____

SIGNATURE: (in ink) _____

(I understand that cheating is a serious offense)

INSTRUCTIONS TO STUDENTS:

This is a 50 minute 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, 5 pages of questions and also 2 blank pages for rough work. Please check that you have all the pages. You may remove the blank pages if you want, 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 50 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	15	
2	10	
3	8	
4	10	
5	7	
Total:	50	

UNIVERSITY OF MANITOBA

DATE: March 10, 2010

MIDTERM II
PAGE: 1 of 5
TIME: 50 minutes
EXAMINER: M. Davidson

COURSE NO: MATH 2500
EXAMINATION:
Introduction to Number Theory

---

[15] 1. (a) Given the prime factorization of $n = 45\,864$ is $2^3 \cdot 3^2 \cdot 7^2 \cdot 13$, find $d(45\,864)$, $\sigma(45\,864)$ and $\phi(45\,864)$.

$d(45864) = 4 \cdot 3 \cdot 3 \cdot 2 = 72$

$\sigma(45864) = (1+2+4+8)(1+3+9)(1+7+49)(1+13)$

$= (2^4-1)\left(\frac{3^3-1}{2}\right)\left(\frac{7^3-1}{6}\right)(1+13) = 15 \cdot 13 \cdot 57 \cdot 14$

$= 155\,610$

$\phi(45864) = 2^2(2-1) \cdot 3(3-1) \cdot 7(7-1)(13-1)$

$= 4 \cdot 3 \cdot 2 \cdot 7 \cdot 6 \cdot 12 = 12096$

(b) If p and q are distinct primes, what is $d(p^2q)$, $\sigma(p^2q)$ and $\phi(p^2q)$?

$d(p^2q) = 3 \cdot 2 = 6$

$\sigma(p^2q) = (1+p+p^2)(1+q) = \left(\frac{p^3-1}{p-1}\right)(1+q)$

$\phi(p^2q) = p(p-1)(q-1)$

(c) Prove that if n is odd then $\phi(2n) = \phi(n)$ and if n is even then $\phi(2n) = 2\phi(n)$. [Hint: recall that if n is even then it can be express as $n = 2^e m$ where $e \geq 1$ and m is odd.]

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

Since ϕ is multiplicative

$\phi(2n) = \phi(2)\phi(n) = (2-1)\phi(n) = \phi(n)$

If n is even then $n = 2^e m$ where $e \geq 1$ and m is odd

So $\phi(2n) = \phi(2^{e+1} m)$ since $(2^{e+1}, m) = 1$

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

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

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

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

UNIVERSITY OF MANITOBA

DATE: March 10, 2010

COURSE NO: MATH 2500
EXAMINATION:
Introduction to Number Theory

MIDTERM II
PAGE: 2 of 5
TIME: 50 minutes
EXAMINER: M. Davidson

---

[10] 2. Find the least residue of $x \pmod m$ for the following. State any theorem that you use.

(a) $x = 107^{2\,163}$ and $m = 433$ [Note: 433 is prime]

Using Fermat's Theorem: $107^{432} \equiv 1 \mod 433$

So $x = 107^{2163} \equiv (107^{432})^5 \cdot 107^3 \mod 433$

$\equiv 107^3 \mod 433$

$\equiv 1\,225\,043 \mod 433$

$\equiv 86 \mod 433$

(b) $x = 107^{2\,163}$ and $m = 432$ [Note: 432 is obviously not prime]

Using Euler's Theorem: $432 = 2^4 \cdot 3^3$ $\quad \phi(432) = 2^3 3^2 (3-1) = 144$

So $107^{144} \equiv 1 \mod 432$

$107^{2163} \equiv (107^{144})^{15} 107^3 \mod 432$

$\equiv 1225043 \mod 432$

$\equiv 323 \mod 432$

(c) $x = (432)(431)\cdots(44)(43)(41)(40)\cdots(3)(2)(1)$ and $m = 433$
[Note: 433 is still prime. Here, x is the product of all numbers less than or equal to 432 EXCEPT 42.]

Wilsons Theorem: $432! \equiv -1 \mod 433$

So $42x \equiv 432! \equiv -1 \mod 433$

$433 = 42(10) + 13$
$42 = 13(3) + 3$
$13 = 3(4) + 1$

$1 = 13 + 3(-4)$
$= 13 + [42 + 13(-3)](-4)$
$= 42(-4) + 13(13)$
$= 42(-4) + [433 + 42(-10)](13)$
$= 433(13) + 42(-134)$

$(-134)42x \equiv (-134)(-1) \mod 433$

$x \equiv 134 \mod 433$

---

[8] 3. (a) Define what if means for a number n to be perfect.

A number is perfect if

$\sigma(n) - n = n$

(b) Define what if means for a number n to be abundant.

A number is abundant if

$\sigma(n) - n > n$

(c) If n is an even perfect number, what is known about the prime factorization of n?

If n is an even perfect number then

$n = 2^{p-1}(2^p - 1)$

where $2^p - 1$ (and hence p) is prime.

(d) Show that if n is an even perfect number then $5n$ is abundant.

If n is an even perfect number then $n = 2^{p-1}(2^p - 1)$. Since $2^p - 1$ is prime, $5 \nmid 2^p - 1$

Hence $(n, 5) = 1$

So $\sigma(5n) = \sigma(5)\sigma(n)$

$= (5+1)(2n)$

$= 12n$

$12n - 5n = 7n > 5n$

So $5n$ is abundant.

[10] 4. (a) Define amicable and show that if m and n are amicable then $\sigma(m) = \sigma(n)$.

The numbers m & n are amicable

if $\sigma(m) - m = n$ and $\sigma(n) - n = m$.

$\sigma(m) - m = n \Rightarrow \sigma(m) = m + n$

$\sigma(n) - n = m \Rightarrow \sigma(n) = m + n$

So $\sigma(m) = \sigma(n)$

(b) Show that 6 232 and 6 368 are an amicable pair.
[Hint: 199 is prime and 779 is divisible by 19.]

$6232 = 2^3 \cdot 19 \cdot 41$

$6368 = 2^5 \cdot 199$

$\sigma(6232) - 6232 = 15 \cdot 20 \cdot 42 - 6232$

$= 12600 - 6232 = 6368$

$\sigma(6368) - 6368 = 63 \cdot 200 - 6368$

$= 12600 - 6368 = 6232$

(c) Use 168 and 297 to show that is possible to have $\sigma(m) = \sigma(n)$ without m and n being amicable.

$168 = 2^3 \cdot 3 \cdot 7$ $\qquad$ $297 = 3^3 \cdot 11$

$\sigma(168) = 15 \cdot 4 \cdot 8$ $\qquad$ $\sigma(297) = 40 \cdot 12$

$= 480$ $\qquad$ $= 486$

But $\sigma(168) - 168 = 480 - 168 = 312 \neq 297$

UNIVERSITY OF MANITOBA

DATE: March 10, 2010

COURSE NO: MATH 2500
EXAMINATION:
Introduction to Number Theory

MIDTERM II
PAGE: 5 of 5
TIME: 50 minutes
EXAMINER: M. Davidson

---

[7] 5. Given the public information of an RSA encryption key of $(n, e) = (2599, 73)$, find the decrypt key d. [Hint: One of the two prime factors of n is less than 30.]

$2599 = 23 \cdot 113$

$\phi\, 2599 = 22 \cdot 112 = 2464$

(want to solve $73x \equiv 1 \bmod 2464$)

$2464 = 73(33) + 55$

$73 = 55(1) + 18$

$55 = 18(3) + 1$

So $1 = 55 + 18(-3)$

$= 55 + [73 + 55(-1)](-3)$

$= 73(-3) + 55(4)$

$= 73(-3) + [2464 + 73(-33)](4)$

$= 2464(4) + 73(-135)$

The decrypt key is 2329.

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 $2002\,x + 897\,y = (2002, 897)$.

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

UNIVERSITY OF MANITOBA

DATE: December 7, 2012

FINAL EXAMINATION
PAGE: 6 of 13
TIME: 3 hours
EXAMINER: M. Davidson

COURSE NO: MATH 2500
EXAMINATION:
Introduction to Number Theory

---

[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's 3) 3 6 9 12 15 18 21 24 27 30 33 36 39 42 45

(least residues 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.

$7^9 \equiv 49 \cdot 7^2 \equiv 49 \cdot 14 \equiv 686 \equiv 47 \mod 71$ — 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

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

and

$(a^2)^{t/2} = a^t \equiv 1 \mod m$ 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) $\left(\frac{113616}{997}\right)$

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

$997 \equiv 1 \bmod 4$

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

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

$997 \equiv 1 \bmod 3$

$997 \equiv 208 \bmod 263$

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

$13 \equiv 1 \bmod 4$

$263 \equiv 3 \bmod 13$

$13 \equiv 1 \bmod 3$

$= 1$

[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 $5 \equiv 1 \mod 4$, $5639 \equiv 4 \mod 5$

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

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