UNIVERSITY OF MANITOBA

DATE: March 7, 2013

MIDTERM
TITLE PAGE
TIME: 90 minutes
EXAMINER: M. Davidson

COURSE NO: MATH 2500
EXAMINATION:
Introduction to Number Theory

FAMILY NAME: (Print in ink) _____

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

STUDENT NUMBER: _____

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

INSTRUCTIONS TO STUDENTS:

This is a 90 minute exam. **Please show your work clearly.**

A 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, 8 pages of questions with the last page containing a list of 'small' primes. Please check that you have all the pages.

The value of each question is indicated in the lefthand margin beside the statement of the question. The total value of all questions is 70 points.

Answer all questions on the exam paper in the space provided beneath the question. For some questions, you may have more room than needed. 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	8	
3	10	
4	12	
5	8	
6	5	
7	8	
8	9	
Total:	70	

UNIVERSITY OF MANITOBA

DATE: March 7, 2013

MIDTERM
PAGE: 1 of 8
TIME: 90 minutes
EXAMINER: M. Davidson

COURSE NO: MATH 2500
EXAMINATION:
Introduction to Number Theory

---

[10] 1. (a) Use the Euclidean Algorithm to find $(285, 609)$.

(b) Find all integer solutions to $285x + 609y = 21$.

(c) Find all solutions to $285x \equiv 21 \pmod{609}$.

a) $609 = 285(2) + 39$

$285 = 39(7) + 12$

$39 = 12(3) + 3$

$12 = 3(4) + 0$

So $(609, 285) = 3$

b) $3 = 39 + 12(-3)$

$= 39 + [285 + 39(-7)](-3)$

$= 285(-3) + 39(22)$

$= 285(-3) + [609 + 285(-2)](22)$

$= 609(22) + 285(-47)$

So $285(-47) + 609(22) = 3$

$285(-329) + 609(154) = 21$

$x = -329 + \frac{609}{3}t = -329 + 203t$

$y = 154 + \frac{285}{3}t = 154 - 95t$

c) from the solution above (part b)) we see that

$$x \equiv -329 \mod 203$$

So the three solutions are

77, 280, 483.

[8] 2. Find a solution to the following system of congruences:

$$x \equiv 3 \pmod 6$$
$$x \equiv 14 \pmod{35}$$
$$x \equiv 18 \pmod{47}$$

This solution is unique in which modulus?

From $x \equiv 3 \bmod 6$, we get

$x = 3 + 6k_1$

Substituting into $x \equiv 4 \bmod 35$, we get

$3 + 6k_1 \equiv 14 \bmod 35$

$6k_1 \equiv 11 \bmod 35$

$6(6k_1) \equiv 6(11) \bmod 35$

$k_1 \equiv 66 \equiv 31 \bmod 35$

$35 = 6(5) + 5$

$6 = 5(1) + 1$

$1 = 6 + 5(-1)$

$= 35(-1) + 6(6)$

$k_1 = 31 + 35k_2$

$x = 3 + 6(31 + 35k_2) = 189 + 210k_2$

We now substitute this expression for x into $x \equiv 18 \bmod 47$

$189 + 210k_2 \equiv 18 \bmod 47$

$210k_2 \equiv -171 \bmod 47$

$22k_2 \equiv 17 \bmod 47$

$(15)22k_2 \equiv \overset{15}{\cancel{22}}\overset{17}{\cancel{(15)}} \bmod 47$

$k_2 \equiv 255 \equiv 20 \bmod 47$

$47 = 22(2) + 3$

$22 = 3(7) + 1$

$1 = 22 + 3(-7)$

$= 47(-7) + 22(15)$

$k_2 = 20 + 47k_3$

$x = 189 + 210(20 + 47k_3)$

$= 4389 + 9870k_3$

The solution is 4389, and it is unique modulo 9870.

[10] 3. (a) Find the prime power decompostion of:
   i. 163350,
   ii. 154836.
   (b) Use the above to find (163350, 154836).
   (c) Find $d(163350), \sigma(163350)$ and $\phi(163350)$.
   (d) Is 163350 abundant or deficient?

(a) i) $163350 = 2 \cdot 3^3 \cdot 5^2 \cdot 11^2$

ii) $154836 = 2^2 \cdot 3^2 \cdot 11 \cdot 17 \cdot 23$

(b) $(163350, 154836) = 2^1 \cdot 3^2 \cdot 5^0 \cdot 11^1 \cdot 17^0 \cdot 23^0$

$= 198$

(c) $d(163350) = 2 \cdot 4 \cdot 3 \cdot 3 = 72$

$\sigma(163350) = (1+2)(1+3+9+27)(1+5+25)(1+11+121)$

$= 3 \cdot 40 \cdot 31 \cdot 133$

$= 494\,760$

$\phi(163350) = 2^0(2-1)\,3^2(3-1)\,5^1(5-1)\,11^1(11-1)$

$= 9 \cdot 2 \cdot 5 \cdot 4 \cdot 11 \cdot 10$

$= 39600$

(d) $\sigma(163350) - 163350$

$= 494760 - 163350$

$= 331410 > 163350$

Hence 163350 is abundant.

---

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

(a) $x = 56^{10551}$ and $m = 587$

Since 587 is prime, by Fermat's Theorem

$56^{586} \equiv 1 \mod 587$

So $56^{10551} \equiv 56^{586(18)+3} \equiv (56^{586})^{18} \cdot 56^3 \mod 587$

$\equiv 1^{18} \cdot 56^3 \equiv 175616 \equiv 103 \mod 587$

The least residue of x is 103.

(b) $x = 56^{11044}$ and $m = 527$

Since $527 = 17 \times 31$ and so $\phi(527) = 16 \times 30 = 480$, by Euler's Theorem, $56^{480} \equiv 1 \mod 527$.

So $56^{11044} \equiv 56^{480(23)+4} \equiv (56^{480})^{23} \cdot 56^4 \mod 527$

$\equiv 1^{23} \cdot 56^4 \equiv 9834496 \equiv 149 \mod 527$

The least residue of x is 149.

(c) $x = (570)(569)\cdots(58)(57)(55)(54)\cdots(3)(2)(1)$ and $m = 571$

[Here, x is the product of all numbers less than or equal to 570 EXCEPT 56.]

Since 571 is prime, by Wilson's Theorem,

$570! \equiv -1 \mod 571$.

Hence $56x \equiv -1 \mod 571$

$(51)56x \equiv (51)(-1) \mod 571$

$x \equiv -51 \equiv 520$

$571 = 56(10) + 11$
$56 = 11(5) + 1$
$\Downarrow$
$1 = 56 + 11(-5)$
$= 571(-5) + 56(51)$

The least residue of x is 520.

[8] 5. Given the public information for an RSA encryption is $(n, e) = (2279, 421)$, find the decrypt key d.

$n = 2279 = 43 \times 53$

$\phi(n) = 42 \times 52 = 2184$

So $421d \equiv 1 \mod 2184$

$2184 = 421(5) + 79$

$421 = 79(5) + 26$

$79 = 26(3) + 1$

$\Downarrow$

$1 = 79 + 26(-3)$

$= 421(-3) + 79(16)$

$= 2184(16) + 421(-83)$

So $d \equiv -83 \equiv 2101 \mod 2184$

The decrypt key is 2101.

[5] 6. Prove, without using the notion of prime power decomposition, that if $(a, c) = 1$ and $(b, c) = 1$, then $(ab, c) = 1$.

[Note: There are several correct ways to prove this, I present just one of these ways]

Since $(a,c)=1$, there exist integers x and y such that $ax + cy = 1$. Similarly, there are integers r and s such that $br + cs = 1$

Now $(ax + cy)(br + cs) = 1$

$axbr + axcs + cybr + cycs = 1$

$ab(xr) + c(axs + bry + cys) = 1$

Since $(ab, c) \mid 1$, we get that $(ab, c) = 1$.

[8] 7. Use induction to prove

$$3+8+13+18+\cdots+(10n-2)=n(10n+1).$$

Let $P(n)$: $3+8+13+18+\cdots+(10n-2)=n(10n+1)$

When $n=1$,

$10(1)-2=8$

So $3+8=11$ and $1(10(1)+1)=11$

So $P(1)$ is true.

Suppose $P(k)$ is true, so

$3+8+13+18+\cdots+(10k-2)=k(10k+1)$

Then

$3+8+13+18+\cdots+(10(k+1)-2)$

$= 3+8+13+18+\cdots+(10k+8)$

$= 3+8+13+18+\cdots+(10k-2)+(10k+3)+(10k+8)$

(by induction hypothesis) $= k(10k+1)+(10k+3)+(10k+8)$

$= 10k^2+k+20k+11$

$= 10k^2+21k+11$

$= (k+1)(10k+11)$

$= (k+1)(10(k+1)+1)$

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

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

---

[9] 8. (a) Show that if n is odd, then $\phi(2n) = \phi(n)$.

Since n is odd $(2, n) = 1$

Since ϕ is multiplicative

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

$$= \phi(n).$$

(b) Show that if n is even, then $\phi(2n) = 2\phi(n)$.

If n is even, we can write $n = 2^e m$ where m is odd. Since m is odd, $(2^a, m) = 1$.

Now $\phi(n) = \phi(2^e m) = \phi(2^e)\,\phi(m)$ (Since ϕ is multiplicative)

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

And $\phi(2n) = \phi(2^{e+1} m) = \phi(2^{e+1})\,\phi(m)$ (again since ϕ is multiplicative)

$$= 2^e\,\phi(m)$$

$$= 2(\phi(m)).$$

UNIVERSITY OF MANITOBA

DATE: March 7, 2013

MIDTERM
PAGE: 8 of 8
TIME: 90 minutes
EXAMINER: M. Davidson

COURSE NO: MATH 2500
EXAMINATION:
Introduction to Number Theory

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