NAME ANSWER KEY

Math 125-B01, Summer 2014, Test #2, O'Beirne

1	a	(6)	18
	b	(6)	
	c	(6)	
2	a	(12)	16
	b	(4)	
3	a	(10)	16
	b	(6)	
4		~~(17)~~(15)	
5	a	(15)	20
	b	(5)	
6		16	

Answer all questions. You must show the work that allows me to see how you arrived at your answer, even if your calculator was involved. **There will be a deduction of points if no work is shown, even if the answer is correct.** The Honor Code is in effect. Each of the six questions is approximately equal in value.

(6) 1.(a) Find the GCD of 9427 and 2319 1

Work:

$$
\begin{aligned}
9427 &= 4(2319) + 151\\
2319 &= 15(151) + 54\\
151 &= 2(54) + 43\\
54 &= 1(43) + 11\\
43 &= 3(11) + 10\\
11 &= 1(10) + 1 \leftarrow \text{gcd}\\
10 &= 10(1) + 0
\end{aligned}
$$

$$
\left(
\begin{aligned}
9247 &= 3(2319) + 2290\\
2319 &= 1(2290) + 29\\
2290 &= 78(29) + 28\\
29 &= 1(28) + 1\\
28 &= 28(1) + 0
\end{aligned}
\right)
$$

(6) (b) Find the LCM of ~~9247~~ 9427 and 2319 21,861,213

Work:

$$\text{LCM} = \frac{9427 \cdot 2319}{1}$$

$$\left(\text{LCM} = \frac{9247 \cdot 2319}{1} = 21{,}443{,}793 \right)$$

Alt answer

(6) (c) Find m,n such that ~~9247~~ 9427m + 2319n = gcd(~~9247~~ 9427, 2319) m = -215 n = 874

Work: Check your answer!!

	9427	2319	
9427	1	0	4
2319	0	1	15
151	1	-4	2
54	-15	61	1
43	31	-126	3
11	-46	187	1
10	169	-687	10
1	-215	874	

	9247	2319	
9247	1	0	3
2319	0	1	1
2290	1	-3	78
29	-1	4	1
28	79	-315	28
1	-80	319	

Alt answer: m = -80 n = 319

2. (a) Write the binary, octal, hexadecimal and base-5 representations of the number 2014_{10}

11111011110_2 $\quad$ 3736_8 $\quad$ $7DE_{16}$ $\quad$ 31024_5 $\quad$ (12)

Work:

2 | 2014
2 | 1007   0
2 | 503   1
2 | 251   1
2 | 125   1
2 | 62   1
2 | 31   0
2 | 15   1
2 | 7   1
2 | 3   1
2 | 1   1
0   1

1 1 1 1 1 0 1 1 1 1 0

$$\underbrace{0\,1\,1}_{3}\ \underbrace{1\,1\,1}_{7}\ \underbrace{0\,1\,1}_{3}\ \underbrace{1\,1\,0}_{6}$$

$$\underbrace{0\,1\,1\,1}_{7}\ \underbrace{1\,1\,0\,1}_{D}\ \underbrace{1\,1\,1\,0}_{E}$$

5 | 2014
5 | 402   4
5 | 80   2
5 | 16   0
5 | 3   1
0   3

31024

(b) Write the base-6 representation of 2014_7 = 3121_6 $\quad$ (4)

Work:

In decimal 2014_7 is $4 + 7 + 0 + 2 \cdot 7^3 = 697$

6 | 697
6 | 116   1
6 | 19   2
6 | 3   1
0   3

3121

Check $3121_6 = 1 + 2(6) + 1(6^2) + 3(6^3) = 697$ ✓

3. (a) Given $577x \equiv 143 \pmod{880}$ Solve for $0 \le x < 880$ x = 319 (10)

Note: x must be between 0 and 880

Either show the solution or explain why there is none:

Reason if no solution:

Work if there is a solution:

Check your answer!!

~~880 = 1 (577) + 303~~

~~577 = 1 (303) + [illegible]~~

~~303 = 1 (247) + 56~~

~~246 = 4 (56) + 22~~

~~56 = [illegible] + [illegible]~~

~~2(22) + 2~~

~~22 = 1 (12) + 10~~

~~12 = 1 (10) + 2~~

~~10 = 5 (2) + 0~~

$577^{-1} 577 x = 577^{-1} 143 \pmod{880}$

$x \equiv 39{,}039 \pmod{880}$

$x = 319$

$880 = 1(577) + 303$

$577 = 1(303) + 274$

$303 = 1(274) + 29$

$274 = 9(29) + 13$

$29 = 2(13) + 3$

$13 = 4(3) + 1$ ←

$3 = 3(1) + 0$

	880	577	
880	1	0	1
577	0	1	1
303	1	-1	1
274	-1	2	9
29	2	-3	2
13	-19	29	4
3	40	-61	3
1	-179	273	

$-179(880) + 273(577) = 1$

So $\boxed{577^{-1} = 273}$

(b) Solve for $0 \le x < 73$ $72^{74} \equiv x \pmod{73}$ (6)

(Hint: Consider a really easy way) **Note: Your answer must be between 0 and 73.**

Work:

$72^{72} \equiv 1 \pmod{73}$

$72^{74} \equiv 72^2 \pmod{73}$

$\equiv 1 \pmod{73}$

$\boxed{x = 1}$

$$\begin{array}{r} 71 \\ 73\overline{)5184} \\ 5183 \\ \hline 1 \end{array}$$

(15)
(~~14~~)

4. (a) Solve for $0 \leq x < 552$ $\quad x \equiv 19 \pmod{23}$ $\quad$ x = 525

$x \equiv 21 \pmod{24}$

Work: **Note: Your answer must be between 0 and 552. Check your answer!**

$24 = 1(23) + 1$

$23 = 23(1) + 0$

$1 = 1(24) + (-1)(23)$

$x = 19(1)(24) + 21(-1)(23)$

$= 456 - 483 \pmod{552}$

$= 525 \pmod{552}$

Check ~~$23\overline{)552}$ 2 46 92~~ ~~$525\overline{)552}$ 1 525 27~~

$$23\overset{22}{\overline{)525}}$$

46

65

46

19 ✓

$$24\overset{21}{\overline{)525}}$$

48

45

24

21 ✓

5. (a) Use the RSA algorithm to decrypt the 4-digit encrypted message E that was emailed to you (a copy of the email is at the end of this test). Original message M = "__________" VARIOUS

Work: p = 89 q = 47 r=4183 s = 3 a = ______ b = __________ (15)

(b) Which two famous theorems from number theory were used in developing the RSA algorithm? (5)

Fermat's Little Theorem and

Chinese Remainder Theorem .

(16) 6. Use the Principal of Mathematical Induction to prove that for all $n \geq 1$

(4+12) $1 + 2^1 + 2^2 + 2^3 + \dots\dots + 2^n = 2^{n+1} - 1$

Work: Verify for $n = 1$

$1 + 2^1 = 2^2 - 1 = 3$ ✓

If true for $n = k$

$1 + 2^1 + 2^2 + \dots + 2^k = 2^{k+1} - 1$

Consider $n = k+1$

$\underbrace{1 + 2^1 + 2^2 + \dots + 2^k} + 2^{k+1} = ?$ (Want $2^{k+2} - 1$)

$2^{k+1} - 1 + 2^{k+1}$

$2 \cdot 2^{k+1} - 1$

$2^{k+2} - 1$ ✓