CS-2050-All-Sections Exam 3 Blue

Vidit Dharmendra Pokharna

TOTAL POINTS

90 / 100

QUESTION 1

1 MC 1 **0 / 5**

- **- 0 pts** A
- **- 5 pts** B
- ✓ **- 5 pts** *C*
- **- 5 pts** D
- **- 5 pts** E
- **- 5 pts** No Answer

QUESTION 2

2 MC 2 **5 / 5**

- ✓ **- 0 pts** *C*
- **- 5 pts** A
- **- 5 pts** B
- **- 5 pts** D
- **- 5 pts** E
- **- 5 pts** No Answer

QUESTION 3

3 MC 3 **0 / 5**

- **- 0 pts** D
- **- 5 pts** A
- **- 5 pts** B
- ✓ **- 5 pts** *C*
- **- 5 pts** E
- **- 5 pts** No Answer

QUESTION 4

4 MC 4 **5 / 5**

- ✓ **- 0 pts** *B*
- **- 5 pts** A
- **- 5 pts** C
- **- 5 pts** D
- **- 5 pts** E
- **- 5 pts** No Answer

QUESTION 5

5 MC 5 **5 / 5**

- ✓ **- 0 pts** *C*
- **- 5 pts** A
- **- 5 pts** B
- **- 5 pts** D
- **- 5 pts** E
- **- 5 pts** No Answer

QUESTION 6

6 Short Response 1 (Euclid Algorithm) **5 / 5**

- ✓ **- 0 pts** *$$\gcd(135, 51) = 3$$*
- **- 2 pts** Minor Error
- **- 3 pts** Major Error
- **- 4 pts** Correct answer but did not show any work
- **- 5 pts** Incorrect / No Answer

QUESTION 7

Short Response 2 (Prime) 10 pts

7.1 i **3 / 3**

✓ **- 0 pts** *$$2^3 * 5$$*

- 3 pts Incorrect / No Answer

7.2 ii **5 / 5**

✓ **- 0 pts** *16*

- 5 pts Incorrect / No Answer

7.3 iii **2 / 2**

✓ **- 0 pts** *Any 3 numbers relatively prime to n*

- 2 pts Incorrect / No Answer

QUESTION 8

8 Short Response 3 (CRT) 10 / 10

✓ **- 0 pts** *$$x = 22$$ or $$x \equiv 22 (\text{mod} ~105)$$ and showed work using the Chinese Remainder Theorem (refer to answer key)*

- 3 pts Does not check/indicate whether 3, 5, 7 are pairwise relatively prime.

Math errors

- 2 pts 1 Math error

- 4 pts 2 Math errors

- 6 pts 3 Math errors

- 4 pts 4+ Math errors

- 5 pts Major jump in work / logic

- 10 pts No work using Chinese Remainder theorem is shown

- 10 pts Incorrect / No Answer

QUESTION 9

9 Short Response 4 5 / 5

✓ **- 0 pts** *False, because multiples of 7 not removed according to Sieves*

- 2.5 pts False, partly correct explanation

- 4 pts False, no explanation

- 5 pts Incorrect / No Answer

QUESTION 10

10 Short Response 5 (Shift Cipher) 5 / 5

✓ **- 0 pts** *PIRATE PARTY TIME*

Incorrect characters

- 1 pts 1 Incorrect characters

- 2 pts 2 Incorrect characters

- 3 pts 3 Incorrect characters

- 4 pts 4+ Incorrect characters

- 4 pts Shift in wrong direction

- 5 pts Incorrect / No Answer

QUESTION 11

11 Proof 1 (Divisibility) 10 / 10

✓ **- 0 pts** *Correct*

- 2 pts Missing/incorrect introduction (doesn't mention proof type and/or match assumptions made)

- 2 pts Does not state assumption(s) in introduction or proof body

- 3 pts Invalid assumption (e.g. assumes entire statement is true, assumes conclusion is true in a direct proof, etc.)

Common Errors

- 1 pts Missing domain for 1 variable

- 2 pts Missing domain for 2+ vairables

- 2 pts Uses the same variable for different definitions of divisibility (e.g., saying $$b = ak$$ and $$c = bk$$)

Invalid Steps

- **3 pts** 1 Invalid Step
- **6 pts** 2 Invalid steps
- **9 pts** 3+ Invalid Steps

Skipped Steps

- **3 pts** 1 Skipped Step
- **6 pts** 2 Skipped Steps
- **9 pts** 3+ Skipped Steps

Miscited Steps

- **2 pts** 1 Miscited Steps
- **4 pts** 2 Miscited Steps
- **6 pts** 3 Miscited Steps
- **8 pts** 4+ Miscited Steps

- **2 pts** Missing or Incorrect Conclusion

Must say that if $ac| bc$ then $a | b$

- **10 pts** No Answer

QUESTION 12

12 Short Response 6 (RSA) **5 / 5**

✓ **- 0 pts** *Any e that is relatively prime to totient of 35*
e.g. 5, 7, 11, 13

- **2.5 pts** Missing or incorrect explanation
- **5 pts** Incorrect / No Answer

QUESTION 13

13 Short Response 7 (RSA) **5 / 5**

✓ **- 0 pts** *$d = 11$*

- **2 pts** Correct use of $ed \equiv 1 \pmod{(p-1)(q-1)}$, but math error
- **5 pts** Incorrect / No Answer

QUESTION 14

14 Short Response 8 (Binary Expansion`) **5 / 5**

✓ **- 0 pts** *$(10010000)_2$*

- **2 pts** Did not put subscript of 2
- **5 pts** Incorrect / No Answer

QUESTION 15

15 Short Response 9 (Octal Expansion) **5 / 5**

✓ **- 0 pts** *$(264)_8$*

- **2 pts** Did not put subscript of 8
- **5 pts** Incorrect / No Answer

QUESTION 16

16 Short Response 10 (Congruency) **5 / 5**

✓ **- 0 pts** *$b = 0$*

- **5 pts** Incorrect / No Answer

QUESTION 17

17 Short Response 11 (Modular Artihmetic) **5 / 5**

✓ **- 0 pts** *$c = 4$*

- **5 pts** Incorrect / No Answer
- **1 pts** used $\equiv$ instead of = OR kept (mod n) in answer

gradescope

CS 2050-Exam 3 Blue

Name: Vidit Pokharna
GTID: 903772087

No notes, calculators, or other aids are allowed. Read all directions carefully and write your answers in the space provided.
Taking this exam signifies you are aware of and in accordance with the Academic Honor Code of Georgia.
Do not separate any pages from the rest of your exam.

Exam 3 Blue

100 points

$64 \times 5 = 320 + 16 = 336$

64×3

[5] 1. Find the sum of the following integers: $(216)_8$ and $(305)_8$

- ○ $(523)_8$
- ○ $(521)_8$
- ● $(523)_{10}$
- ○ $(521)_{10}$
- ○ None of the above

128
64
192

$6 + 8 + 128$
14
142

$\underline{5}\,\underline{2}\,\underline{3}$

$5 + 192$
197
142
339

[5] 2. Let

$$x = 3^7 5^3 17^3$$

$$y = 3^5 5^3 23$$

What is the $lcm(x, y)$

- ○ $3^5 * 5^3$
- ○ $3^5 * 5^3 * 17^3 * 23$
- ● $3^7 * 5^3 * 17^3 * 23$
- ○ $3^5 * 5^3 * 17^3$
- ○ None of the above

$3^7 . 5^3 . 17^3 . 23$

[5] 3. You want to determine if 111 is composite. Which of the following approaches will be the quickest method for determining if 111 is composite?

- ○ Check all integers between 2 and 111 inclusive to see if any of them are a factor of 111.
- ○ Check all integers between 2 and 11 inclusive to see if any of them are a factor of 111
- ● Check all primes between 2 and 11 inclusive to see if any of them are a factor of 111
- ○ Check all primes between 2 and 7 inclusive to see if any of them are a factor of 111.
- ○ None of the above will work

[5] 4. Which of the following choices is the encryption of the string "PIRATE!" using a transposition cipher based on the permutation σ of the set $\{1, 2, 3, 4, 5\}$ with $\sigma(1) = 2$, $\sigma(2) = 1$, $\sigma(3) = 3$, $\sigma(4) = 5$, $\sigma(5) = 4$? Fill in the bubble for the single correct choice.

- ○ IPTRAE!XXX X
- ● IPRTA!EXXX
- ○ IPRAT!XEXX
- ○ PIRTA!EXXX X
- ○ None of the above

PIRAT E!XXX
IPRTA !EXXX

[5] 5. Suppose $lcm(a,b) = 14$ and $gcd(a,b) = 7$. What is ab?

- ○ 7
- ○ 14
- ● 98
- ○ 21
- ○ None of the above

$14 \cdot 7$

[5] 6. Use the Euclidean Algorithm as shown in class to find the $gcd(135, 51)$. Show your work for all divisions conducted to reach your answer.

$$\begin{array}{r} 2 \\ 51 \overline{)135} \\ \underline{102} \\ 33 \end{array}$$

$$\begin{array}{r} 1 \\ 33 \overline{)51} \\ \underline{33} \\ 18 \end{array}$$

$$\begin{array}{r} 1 \\ 18 \overline{)33} \\ \underline{18} \\ 15 \end{array}$$

$$\begin{array}{r} 1 \\ 15 \overline{)18} \\ \underline{15} \\ 3 \end{array}$$

$$\begin{array}{r} 5 \\ 3 \overline{)15} \\ \underline{15} \\ 0 \end{array}$$

$135 = 2 \cdot 51 + 33$

$51 = 1 \cdot 33 + 18$

$33 = 1 \cdot 18 + 15$

$18 = 1 \cdot 15 + 3$

$15 = 5 \cdot 3 + 0$

$\boxed{gcd(135, 51) = 3}$

7. Let $n = 40$

[3] (i) Find the prime factorization of n

$\frac{40}{2} = \frac{20}{2} = \frac{10}{2} = 5$

$\boxed{40 = 2^3 \times 5}$

[5] (ii) Calculate how many integers less than n are relatively prime to n. You must show your work using Euler's Totient Function.

$\phi(40) = 40(1-\frac{1}{2})(1-\frac{1}{5}) =$

$40 \cdot \frac{1}{2} \cdot \frac{4}{5} = 20 \cdot \frac{4}{5} = \boxed{16}$

1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 35

[2] (iii) List any 3 of the integers that are included in the total found in part (ii) above.

$\boxed{3, 13, 23}$

[10] 8. Use the Chinese Remainder Theorem to find the smallest positive value for x given the following congruences. You may not bruteforce your solution. Use the algorithm taught in class. Show all your work for full credit.

$$x \equiv 1 \pmod 3$$
$$x \equiv 2 \pmod 5$$
$$x \equiv 1 \pmod 7$$

$\left.\begin{array}{l}\gcd(3,5)=1\\ \gcd(3,7)=1\\ \gcd(5,7)=1\end{array}\right\}$ (3, 5, 7) are relatively prime

$M = 3 \times 5 \times 7 = 105$

mod	compare	#	inverse expression	inverse	product
3	1	$105/3 = 35$	$35v \equiv 1 \bmod 3 \to 2v \equiv 1$	$v = 2$	$1 \cdot 35 \cdot 2 = 70$
5	2	$105/5 = 21$	$21v \equiv 1 \bmod 5 \to v \equiv 1$	$v = 1$	$2 \cdot 21 \cdot 1 = 42$
7	1	$105/7 = 15$	$15v \equiv 1 \bmod 7 \to v \equiv 1$	$v = 1$	$1 \cdot 15 \cdot 1 = 15$

$(70 + 42 + 15) \bmod 105 = 127 \bmod 105 = 22$

$\boxed{x = 22}$

[5] 9. Determine whether the following statement is True or False and explain why:
"Consider all integers from 2 to 50. All of the multiples of 2, 3, and 5 are removed except for 2, 3, and 5 themselves. All remaining integers are prime."

This is false as 49 still remains. This value is neither prime, nor a multiple of 2, 3, or 5. Therefore, not all values remaining would be prime. 49 is the square of a prime greater than 5 but 49 is still less than 50.

[5] 10. The following message was created using a shift cipher with k = 10. Decrypt the message.
ZSBKDO ZKBDI DSWO

-10 or +16

25 18 1 10 3 14 25 10 1 3 8
15 8 17 0 19 4 15 0 17 19 24
PIRATE PARTY

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

3 18 22 14
19 8 12 4
TIME

decryption
PIRATE PARTY TIME

[10] 11. Suppose that a, b, and c are integers where $a \neq 0$ and $c \neq 0$. Prove the following: If $ac|bc$ then $a|b$

I will prove that "if $ac|bc$, then $a|b$, given $a \neq 0$ and $c \neq 0$."

Statement	Reason
$ac \mid bc$	Given
$\frac{bc}{ac} = x,\ x \in \mathbb{Z}$	Definition of "divides"
$\frac{bc}{ac} \cdot c = x \cdot c$	Multiply by c on both sides
$\frac{bc}{a} = x \cdot c$	Simplify
$\frac{\frac{bc}{a}}{c} = \frac{xc}{c}$	Divide by c on both sides
$\frac{b}{a} = x$	Simplify
$a \mid b$	Definition of "divides"

∴ By direct proof, if $ac|bc$ then $a|b$ given $a \neq 0$ and $c \neq 0$

$n=35$

[5] 12. Consider the RSA cryptosystem as taught in class. Suppose you have the primes $p = 7, q = 5$.

Choose a value for the encryption key e. Write your chosen value for e in the blank provided. Use the empty space below to explain in detail why your answer is valid based on the information provided.

$e =$ 5

$6 \times 4 = 24 = 2^3 \times 3$

Given p and q are 7 and 5, we know n=35. $\Phi(35) = (7-1)(5-1) = (6)(4) = 24$. Based on rules of RSA encryption, $\phi(n)$ and e must be relatively prime. We know that 2 and 3 would not work as they are factors of 24. Therefore, we can choose 5 as it is relatively prime with 24.

[5] 13. Find a private key d that could be used to decode messages encrypted using the public key $(55, 11)$. Show your work. Please write your final answer in the designated space below.

$d =$ 11

$11d \equiv 1 \bmod \Phi(55) \rightarrow \phi(55) = (11-1)(5-1) = 10 \cdot 4 = 40$

$11d \equiv 1 \bmod 40$

$11d + 1 = 40X$

41

81

$121 = 11 \cdot 11$

$121 \bmod 40 = 1$

[5] 14. Find the binary expansion of $(144)_{10}$. Show your work.

$\frac{1}{2^7}\ \frac{0}{2^6}\ \frac{0}{2^5}\ \frac{1}{2^4}\ \frac{0}{2^3}\ \frac{0}{2^2}\ \frac{0}{2^1}\ \frac{0}{2^0}$

128 64 32 16 8 4 2 1

144
−128
16
−16
0

$144/2 = 77$ R0
$72/2 = 36$ R0
$36/2 = 18$ R0
$18/2 = 9$ R0
$9/2 = 4$ R1
$4/2 = 2$ R0
$2/2 = 1$ R0
$1/2 = 0$ R1

$\boxed{(144)_{10} = (10010000)_2}$

10010000

[5] 15. Find the octal expansion of $(B4)_{16}$. Show your work.

11 in base 2

$\frac{1}{8}\ \frac{0}{4}\ \frac{1}{2}\ \frac{1}{1}$

4 in base 2

$\frac{0}{8}\ \frac{1}{4}\ \frac{0}{2}\ \frac{0}{1}$

$4 + 176 = 180$

2 6 4

180
−128
52
−48
4

$\underset{4\,2\,1}{010}\ \underset{4\,2\,1}{110}\ \underset{4\,2\,1}{100}$

264

$\boxed{(B4)_{16} = (264)_8}$

$2^4 5^{-4} 3^2$

[5] 16. Find the unique integers b such that $0 \le b \le 7$, and $b \equiv_8 10^4 3^2$. Show your work.

$$b \equiv_8 10^4 3^2$$

$$(10^4 3^2) \bmod 8 = [(10^4 \bmod 8)(3^2 \bmod 8)] \bmod 8$$

$$= [((10 \bmod 8)^4 \bmod 8)(9 \bmod 8)] \bmod 8$$

$$= [((2)^4 \bmod 8)(1)] \bmod 8$$

$$= [(16 \bmod 8)(1)] \bmod 8$$

$$= [0 \cdot 1] \bmod 8$$

$$= 0 \bmod 8 = 0 \rightarrow \boxed{b = 0}$$

[5] 17. Let $a \equiv_7 3$ and $b \equiv_7 2$. Find the unique integer c such that $0 \le c \le 6$, and $c \equiv_7 2a^3 + ab$. Show your work.

$a = 3$, $b = 2$

$$(2)(3)^3 + (3)(2) = 54 + 6 = 60 \bmod 7 =$$

$$60 - 7\left\lfloor \frac{60}{7} \right\rfloor = 60 - 7 \cdot 8 = 60 - 56 = \boxed{4}$$

$$\boxed{c = 4}$$

This page provides extra space if needed. Clearly mark any question that has its answer here.

$((10^4 \bmod 8)(3^2 \bmod 8)) \bmod 8$

$(((10 \bmod 8)^4 \bmod 8) \cdot (9 \bmod 8)) \bmod 8$

$((2^4 \bmod 8) \cdot 1) \bmod 8$

$((16 \bmod 8) \cdot 1) \bmod 8$

$(0 \cdot 1) \bmod 8$

$0 \bmod 8 = 0$

$\boxed{b = 0}$