Test 2

Total: ____________ **/ 150**

Printed Name: Demetrius Johnson

GRADER/TA: ***[No CO Data]***

I, Demetrius Johnson, have neither given nor received assistance on this examination except that which is provided by, or approved by, the instructor.

1. [15 pts] Bob wants to send a secret message to Alice using RSA. Alice's public key is $PU_A = \{e, n\} = \{11, 15\}$

   $e = 11$ $n = 15$

   Bob wants to send the message M = 4

   Show your calculations, and the resultant ciphertext, C

use: $C = M^e \bmod n$

$= 4^{11} \bmod 15$

$\boxed{C = 4}$

- use product rules of modulus
- $4^2 = 16$, $16 \bmod 15 = 1$
- $4^{11} = 4 \cdot (4^2)^5 \rightarrow 4 \cdot (4^2)^5 \bmod 15$
- $[(4 \bmod 15)((16)^5 \bmod 15)] \bmod 15$
- $[(4 \bmod 15)(1)^5] \bmod 15 \rightarrow 4 \bmod 15 = 4$

2. [15 pts] Alice receives the ciphertext, C, from Bob (resulting from question 1 above.) She wants to decrypt the message, M, using the ciphertext, and her private key $PR_A = \{d, n\} = \{3, 15\}$

   Show the calculations for decryption, and the result.

$M = C^d \bmod n$; $c = 4$, $d = 3$, $n = 15$

$M = 4^3 \bmod 15$

$M = [(4^2 \bmod 15)(4 \bmod 15)] \bmod 15$

$M = ((1)(4)) \bmod 15 = 4 \bmod 15 = 4$

$M = 4$

3. [15 pts] Solve the following modular arithmetic questions, using the integer representation discussed in class, namely, x = cq + r (find the remainder, r. Hint: r should *always* be non-negative)

(overshoot method)

a. -14 mod 3

- $-14 = c \cdot 3 + r$
- let $c = -5$
- $-14 = -15 + r$
- $\boxed{r = 1}$

b. 21 mod 4

- $21 = c \cdot 4 + r$
- let $c = 5$
- $21 = 20 + r$
- $\boxed{r = 1}$

c. -42 mod 4

- $-42 = c \cdot 4 + r$
- let $c = 11$
- $-42 = -44 + r$
- $r = 2$

4. [15 pts] Determine whether the following congruences hold using the modular difference/division property [Hint: (a-b)/c is an integer?]

a. Is 11 ≡ 7 mod 4?

$\frac{11-7}{4} = \frac{4}{4} = 1$ ✓ yes, because 1 is an integer.

b. Is -5 ≡ 5 mod 3?

$\frac{-5-5}{3} = \frac{-10}{3} = -3 + -\frac{1}{3}$ ✗ $-3\frac{1}{3}$ is not an integer. So No

c. Is 14 ≡ 4 mod 3?

$\frac{14-4}{3} = \frac{10}{3} = 3\frac{1}{3}$ ✗; No does not hold; thus there is no congruence.

$14 \% 3 = 2$
$4 \% 3 = 1$
$2 \neq 1$

5. [20 pts] Use Euclid's algorithm the find the following greatest common divisors (GCDs)

a. GCD(20, 55)

- let $n = 55$, $m = 20$
- $GCD(55, 20) = GCD(n \bmod m, m)$
- $GCD(55 \bmod 20, 20) = GCD(5, 20)$
- $55 \bmod 20 = 5$
- let $n = 20$, $m = 5 \rightarrow GCD(20 \bmod 5, 5)$
- $20 \bmod 5 = 0 \rightarrow GCD(0, 5)$; thus:

$$\boxed{GCD(20, 55) = 5}$$

b. GCD(14, 28)

- let $n = 28$, $m = 14$
- $GCD(28, 14) = GCD(28 \bmod 14, 14)$
- $28 \bmod 14 = 0 \rightarrow GCD(0, 14)$

Thus: $\boxed{GCD(14, 28) = 14}$

6. [20 pts] The following are **clear equilibrium strategies** for you and your opponent. Find the pairs of choices (yours, opponents), e.g., (a, x), (b, y), etc. (you don't need mini-max solution for this – the choice should be obvious given your goals and your opponents' goals, and that you are both rational.)

a.

Opponent

		x	y
You	a	2	4
	b	6	8

Dominating strategy

Also Dominating strategy

Nash Equilibrium: (b, y)

b.

Opponent

		x	y
You	a	12	10
	b	9	8

Dominant

Dominant

Nash Equilibrium: (a, x)

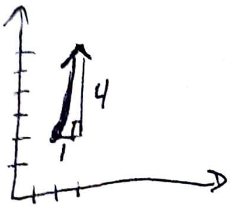
$a^2+b^2=c^2$; $c=\sqrt{a^2+b^2}$

$a=\sqrt{c^2-b^2}$

$y=mx+b$

7. [15 pts] Consider the line segments connecting points p_1 and p_2 in each of the following scenarios. Find a vector $\vec{V}$ = (x, y) that represents these line segments.

a. p_1 = (2, 2) and p_2 = (3, 6)



$\text{slope} = \frac{\text{rise}}{\text{run}} = \frac{6-2}{3-2} = \frac{4}{1} = 4$

$\boxed{\vec{V} = (1\hat{i}, 4\hat{j})}$

b. p_1 = (-4, 2) and p_2 = (4, 15)

$\text{rise} = 15-2 = 13$

$\text{run} = 4 - -4 = 4+4 = 8$ → put into

unit vector form: $\frac{13}{8} = \frac{(13/8)}{1} = \frac{1.625}{1}$ ✓ unit vector

$\boxed{\vec{v} = 8(1\hat{i}, 1.625\hat{j})}$

$\vec{v} = \boxed{\vec{v}(8\hat{i}, 13\hat{j})}$

c. p_1 = (5, 4) and p_2 = (6, 6)

$\text{rise} = 6-4 = 2$

$\text{run} = 6-5 = 1$ $\boxed{\vec{V} = (1\hat{i}, 2\hat{j})}$

8. [15 pts] Given your solutions in question (7) above, find the **magnitudes** of each of the vectors.

a. $|\vec{V}|$ =

$a^2+b^2=c^2$; $c=\sqrt{a^2+b^2} \rightarrow \sqrt{1^2+4^2} = \sqrt{17}$

$\boxed{|\vec{v}| = \sqrt{17}} = 4.123$

b. $|\vec{V}|$ =

$|\vec{v}| = \sqrt{8^2+13^2} = \boxed{\sqrt{233} = 15.26} = |\vec{v}|$

c. $|\vec{V}|$ =

$|\vec{v}| = \sqrt{1^2+2^2} = \boxed{\sqrt{5}} = 2.236$

9. [10 pts] Find the distances from a point to a line, given the following information

a. You are given a point (3, 3) **not** on the line, and two points (1, 2) and (12, 20) through which the line passes

- $y = mx + b \rightarrow m = \frac{20-2}{12-1} = \frac{18}{11}$
- using $(1, 2) \rightarrow 2 = \left(\frac{18}{11}\right)(1) + b$
- $b = \frac{22}{11} - \frac{18}{11} = \frac{4}{11}$
- So $y = \frac{18}{11}x + \frac{4}{11}$

- multiplicative, negative inverse of slope $\frac{18}{11} \Rightarrow -\frac{11}{18}$
- ~~Find intersection t~~ Fan
- Find a line with slope $-\frac{11}{18}$ that intersects line $\frac{18}{11}x + \frac{4}{11}$ and point (3, 3).
- $y = mx + b$; $3 = -\frac{11}{18}(3) + b$

$b = \frac{54}{18} + \frac{33}{18} = \frac{87}{18}$

question 9A Continued

- So, perpendicular line to $y = \frac{18}{11}x + \frac{4}{11}$ containing point 3,3 $\Longrightarrow y = \frac{-11}{18}x + \frac{87}{18}$
- Find intersection:

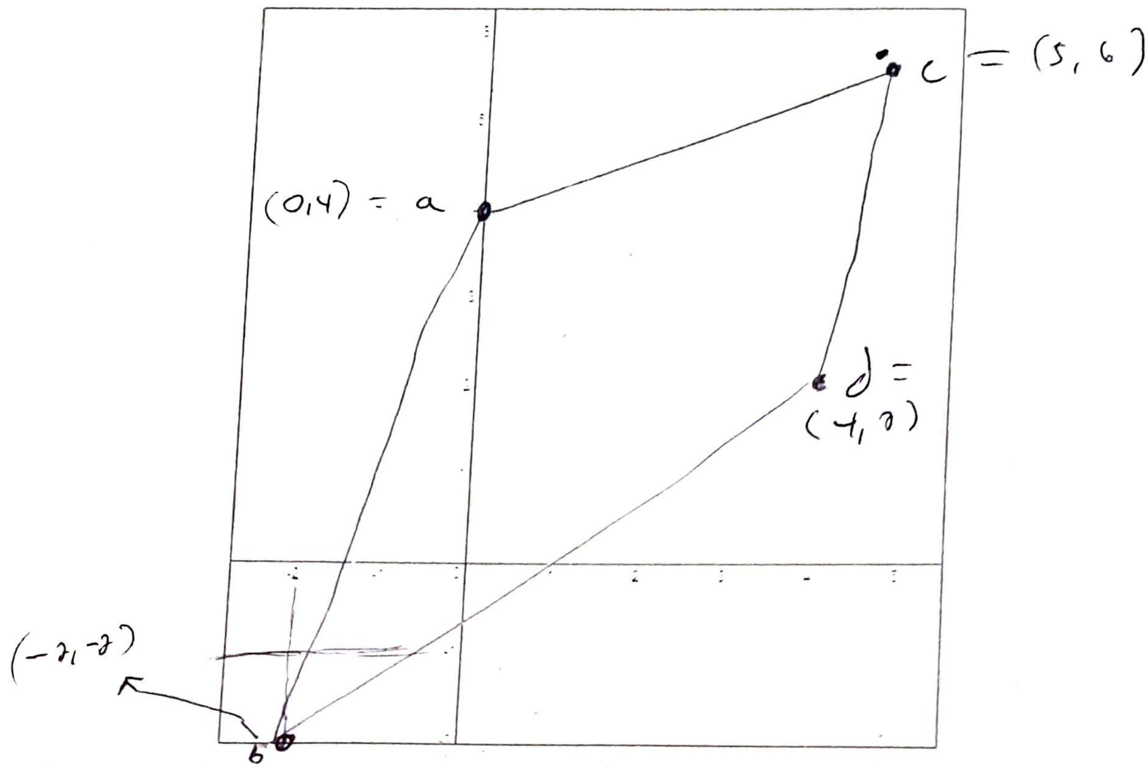
- $y = 1.64x + 0.36$
- $y = -0.61x + 4.83$
- $1.64x + 0.36 = -0.61x + 4.83$
- $2.25x = 4.47$; $x = 1.987$
- $y = (1.64)(1.987) + 0.36 = 3.618$
- So: intersection of $\perp$ lines is $\underline{(1.99, 3.62)}$
- Now we need distance between $(1.99, 3.62)$ and $(3, 3)$.

b. You are given a point (6, 4) **not** on the line, and a line y = 2x + 4

- $y = 2x + 4$
- $\perp$ of $y = 2x+4 \rightarrow y = -\frac{1}{2}x + 4$
- Find a line $y = -\frac{1}{2}x + 4$ that passes through (6, 4)
- $4 = 6 \cdot -\frac{1}{2} + b$
- $b = 7$; so $y = -\frac{1}{2}x + 7$
- Now Find ~~Distance between~~ intersection:
- $-\frac{1}{2}x + 7 = 2x + 4 \rightarrow \frac{5}{2}x = 3$; $x = \frac{6}{5}$
- $y = 2\left(\frac{6}{5}\right) + 4 = 6.4$
- Thus intersection is ~~(1.2, 6.4)~~

  (1.2, 6.4)
- Now Find distance between (1.2, 6.4) and (6, 4)

10. [10 pts] Given the following polygon, use the Surveyor's Formula to find its area



The ordered pairs of vertices, in counter-clockwise order are thus (a, b, d, c)

a = (0, 4) **b = (-2, -2)** **d = (4,2)** **c = (5,6)**

$$\begin{array}{c} a \\ b \\ d \\ c \end{array} \begin{bmatrix} 0 & 4 \\ -2 & -2 \\ 4 & 2 \\ 5 & 6 \end{bmatrix}$$

$$A = \frac{1}{2}\left[(0 \cdot -2 + -2 \cdot 2 + 4 \cdot 6) - (4 \cdot -2 + -2 \cdot 4 + 2 \cdot 5)\right]$$

$$A = \frac{1}{2}\left[(0 + -4 + 24) - (-8 + -8 + 10)\right]$$

$$A = \frac{1}{2}[20 - -6]$$

$$A = \frac{1}{2}(26)$$

$$\boxed{A = 13}$$