INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE CÓMPUTO

Nombre: _Sanchez Mendez Edmundo Josue__

ESCOM

Evaluación de conocimientos del primer parcial.

1. Clasifica el cifrador Atbash _____
2. Suponga que MCD(a,n)=d con d>1 entonces a^{-1}mod n no existe, explique porque.
3. Find φ(9438)=_____
4. 111 mod 17 =____ -111 mod 17 ____ 1/111 mod 17 =____ -1/111 mod 17 =____
5. Cálcula: $17^{-1} \bmod 101$ utilizando el Algoritmo Extendido de Euclides.
6. The following ciphertext was encrypted by Affine Cipher VMBAON. The plaintext ends with ar. Decrypt the message. Show the Dk
7. The ciphertext XNQV was encrypted using the affine function 15p + 13. Find the plaintext. Show the Dk
8. The ciphertext FRVSEUIW was encrypted using Vigenere cipher with the key *mars*. Find the plaintext Show the decryption key
9. Eve captures Bob´s Hill cipher machine, which uses a 2x2 matrix M mod 26. She tries to find de key, she knows that the plaintext *dont* encrypts to *ELNI*. Find matrix K?

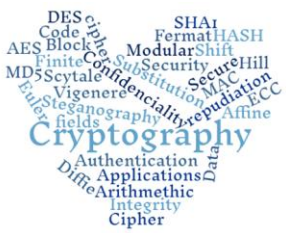
10. Using block cipher with CBC mode. Show that if an error occurs in the transmission of a block Ci, but all the others blocks are transmitted correctly. Show in a diagram which decrypted blocks affects?

11. Betito recibió la siguiente imagen bmp de 24 bits cifrada. Sabe que Alicia utilizó Hill m=3 cuya llave
    11.- IV 26, 13, 9

k=$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix}$ y con el modo de operación CBC.

C1			C2		
40	171	36	236	184	95
C3			C4		
47	97	212	194	9	97

Ayuda a Betito a encontrar **P2** (al finalizar utiliza un generador de colores RGB para ilustrarlo).



M. en C. Nidia A. Cortez Duarte

Evaluación de conocimientos del primer parcial.

Sanchez Mendez Edmundo Josue

1. Clasifica el criptosistema Atbash: _____

2. Supongan que MCD(a,n)=d con d>1 entonces $a^{-1} \bmod n$ no existe, explíquen porque

R= Para que exista $a^{-1} \bmod n$ se necesita que a y n sean coprimos o primos relativos, lo cual viene dado por gcd(a,n)=1 y además sabemos que si MCD(a,n)=1 => gcd(a,n)=1 es posible.

∴ Como MCD(a,n)=d y d>1, => $a^{-1} \bmod n$ no existe

3. Find $\varphi(9438) = 2640$

9438 | 2
4719 | 3
1573 | 11
143 | 11
13 | 13
1 |

$\varphi(9438) = 2 \cdot 3 \cdot 11^2 \cdot 13 \left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{11}\right)\left(1-\frac{1}{13}\right)$

$= 2 \cdot 3 \cdot 11^2 \cdot 13 \left(\frac{2-1}{2}\right)\left(\frac{3-1}{3}\right)\left(\frac{11-1}{11}\right)\left(\frac{13-1}{13}\right)$

$= 11(2-1)(3-1)(11-1)(13-1) =$

$= 11(1)(2)(10)(12) = 2640$

4. $111 \bmod 17 = 9$

$17 \overline{)111}\ 6$
102
9

$-111 \bmod 17 = -9 \bmod 17 = 8$

$1/111 \bmod 17 = 1 \cdot 111^{-1} \bmod 17 = 1 \cdot 9^{-1} \bmod 17 = 2$

$111^{-1} \bmod 17 = 9^{-1} \bmod 17$

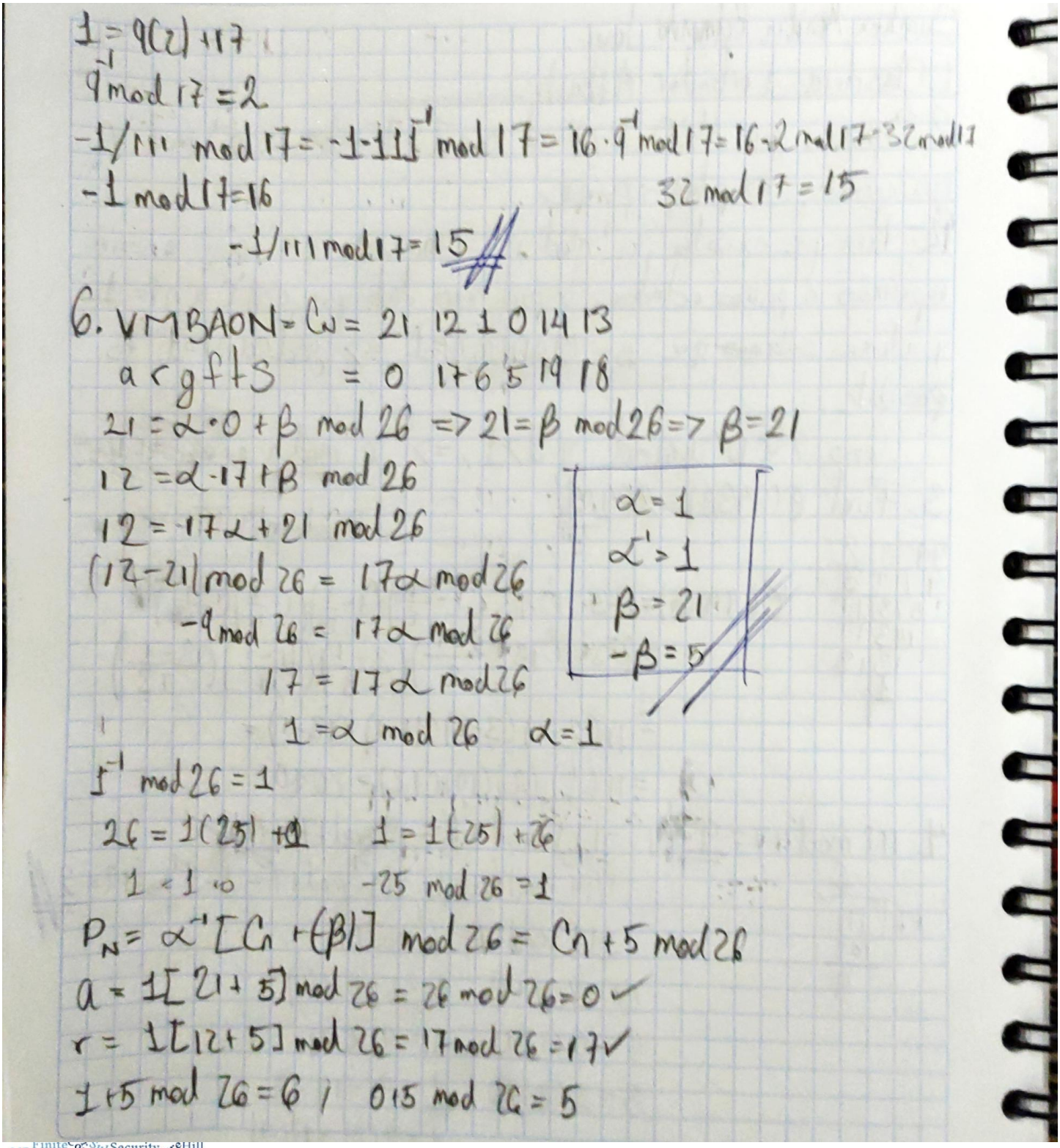
$17 = 9(1) + 8 \quad 8 = 17 - 9(1)$

$9 = 8(1) + 1 \quad 1 = 9 - 8(1)$

$8 = 1(8) + 0 \quad 1 = 9 - 17 + 9$

$1 = 9(2) + 17(-1)$

Evaluación de conocimientos del primer parcial.



1 = 9(2) + 17

$9^{-1} \bmod 17 = 2$

$-1/111 \bmod 17 = -1 \cdot 111^{-1} \bmod 17 = 16 \cdot 9^{-1} \bmod 17 = 16 \cdot 2 \bmod 17 = 32 \bmod 17$

$-1 \bmod 17 = 16$ $\quad 32 \bmod 17 = 15$

$-1/111 \bmod 17 = 15$ //

6. VMBAON = Cn = 21 12 1 0 14 13

argfts = 0 17 6 5 19 18

$21 = \alpha \cdot 0 + \beta \bmod 26 \Rightarrow 21 = \beta \bmod 26 \Rightarrow \beta = 21$

$12 = \alpha \cdot 17 + \beta \bmod 26$

$12 = 17\alpha + 21 \bmod 26$

$(12 - 21) \bmod 26 = 17\alpha \bmod 26$

$-9 \bmod 26 = 17\alpha \bmod 26$

$17 = 17\alpha \bmod 26$

$1 = \alpha \bmod 26 \quad \alpha = 1$

$\alpha = 1$
$\alpha^{-1} = 1$
$\beta = 21$
$-\beta = 5$

$1^{-1} \bmod 26 = 1$

$26 = 1(25) + 1 \quad 1 = 1(25) + 26$

$1 = 1 \checkmark \quad -25 \bmod 26 = 1$

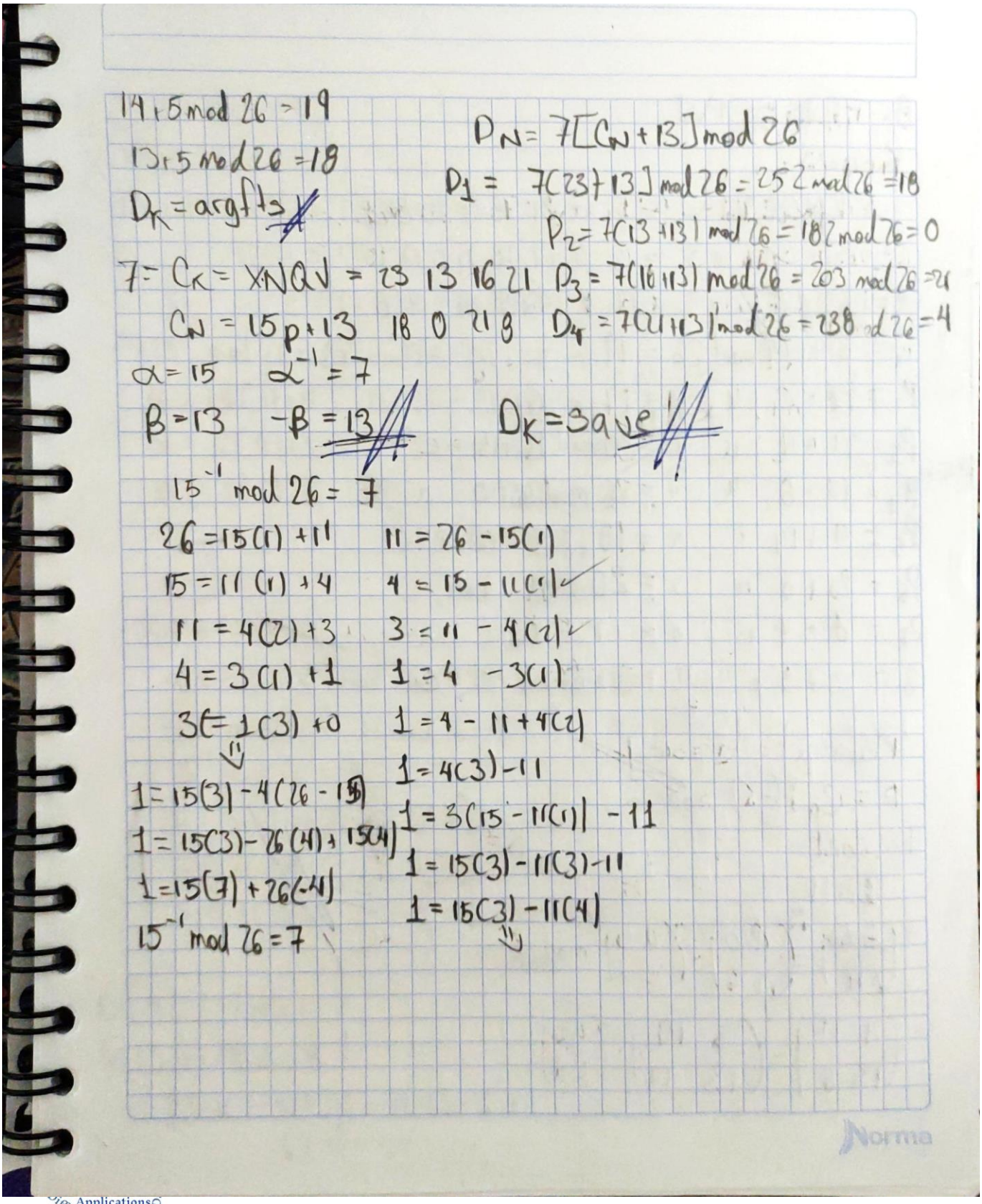
$P_N = \alpha^{-1}[C_n + (\beta)] \bmod 26 = C_n + 5 \bmod 26$

$a = 1[21 + 5] \bmod 26 = 26 \bmod 26 = 0$ ✓

$r = 1[12 + 5] \bmod 26 = 17 \bmod 26 = 17$ ✓

$1 + 5 \bmod 26 = 6$ / $015 \bmod 26 = 5$

Evaluación de conocimientos del primer parcial.



Evaluación de conocimientos del primer parcial.

8. FRVSEUIW

K = mars

FRVSEUIW = 5 17 21 18 4 20 8 22

K = marsmars = 12 0 17 18 12 0 17 18

-K = 14 0 9 8 = 14 0 9 8 14 0 9 8

$P_1 = 5 + 14 \bmod 26 = 19 = t$

$P_2 = 17 + 0 \bmod 26 = 17 = r$

$P_3 = 21 + 9 \bmod 26 = 4 = e$

$P_4 = 18 + 8 \bmod 26 = 0 = a$

$P_5 = 4 + 14 \bmod 26 = 18 = s$

$P_6 = 20 + 0 \bmod 26 = 20 = u$

$P_7 = 8 + 9 \bmod 26 = 17 = r$

$P_8 = 22 + 8 \bmod 26 = 4 = e$

Plaintext = treasure

$P = C_n + (-K) \bmod 26$

9. dont

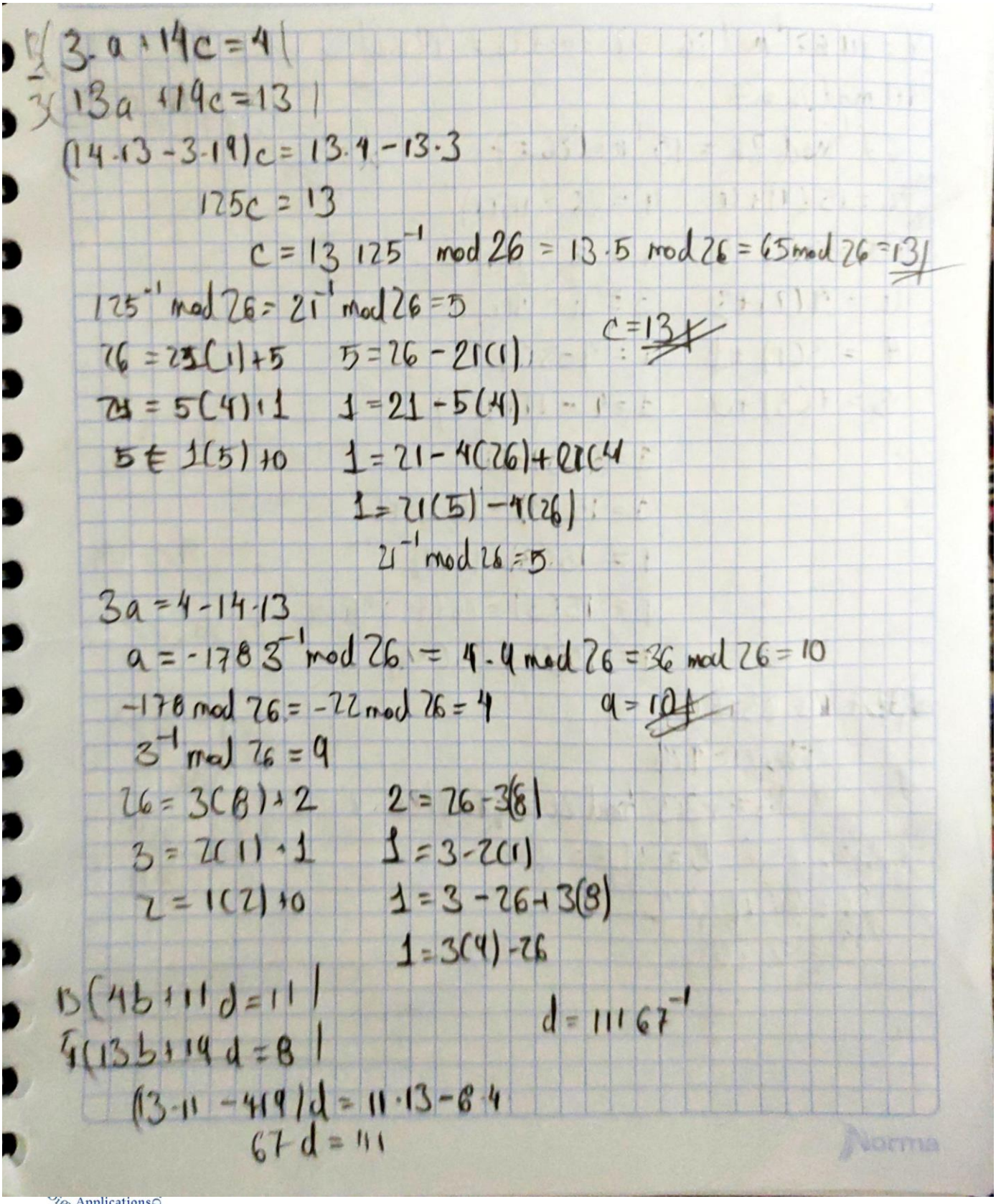
ELNI

$K = \begin{pmatrix} 10 & 19 \\ 13 & 23 \end{pmatrix}$

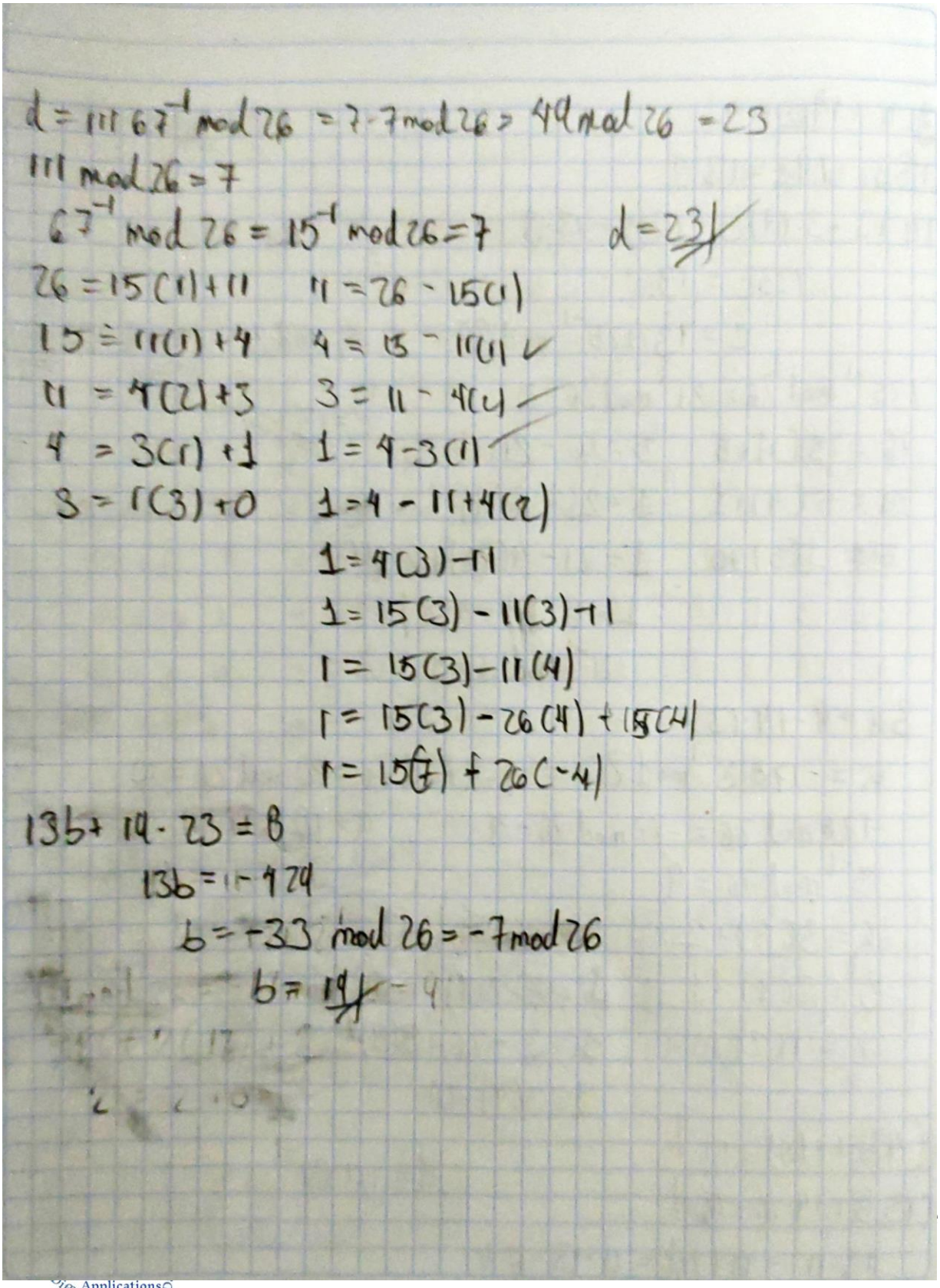
$\begin{pmatrix} E & L \\ N & I \end{pmatrix} = \begin{pmatrix} d & 0 \\ n & 6 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} \bmod 26$

$\begin{pmatrix} 4 & 11 \\ 13 & 8 \end{pmatrix} = \begin{pmatrix} 3 & 14 \\ 13 & 19 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

Evaluación de conocimientos del primer parcial.



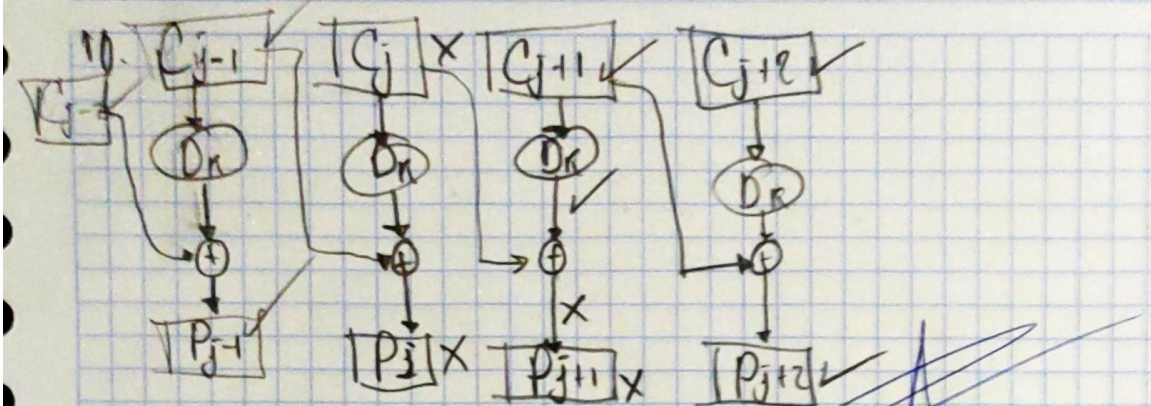
Evaluación de conocimientos del primer parcial.



z Duarte

Evaluación de conocimientos del primer parcial.

10.



11

$$K^{-1} = \begin{pmatrix} 96 & 167 & 1 \\ 74 & 179 & 254 \\ 177 & 81 & 1 \end{pmatrix}$$

$P_2 \Rightarrow P_1$ y C_2

$$(236, 184, 95)\begin{pmatrix} 96 & 167 & 1 \\ 74 & 179 & 254 \\ 177 & 81 & 1 \end{pmatrix} = (53087, 80643, 47067) \bmod 256$$

(95 171 214)

xor

40 171 36

119 0 255

1011111
0101000
1110111

11011011
00100100
11111111

$P_2 = (119\ 0\ 255)$

Evaluación de conocimientos del primer parcial.

$$\begin{pmatrix}1&2&3\\4&5&6\\11&9&8\end{pmatrix}^{-1} \Rightarrow \left(\begin{array}{ccc|ccc}1&2&3&1&0&0\\4&5&6&0&1&0\\11&9&8&0&0&1\end{array}\right) \Leftrightarrow \begin{matrix}F_2-4F_1\\F_3-11F_1\end{matrix}$$

$$\left(\begin{array}{ccc|ccc}1&2&3&1&0&0\\0&-3&-6&-4&1&0\\0&-13&-25&-11&0&1\end{array}\right) \Leftrightarrow -\frac{F_2}{3}\left(\begin{array}{ccc|ccc}1&2&3&1&0&0\\0&1&2&4/3&-1/3&0\\0&-13&-25&-11&0&1\end{array}\right) \Leftrightarrow \begin{matrix}F_1-2F_2\\F_3+13F_2\end{matrix}$$

$$\left(\begin{array}{ccc|ccc}1&0&-1&-5/3&2/3&0\\0&1&2&4/3&-1/3&0\\0&0&1&\frac{19}{3}&-13/3&1\end{array}\right) \Leftrightarrow F_2-2F_3 \; F_1+F_3 \left(\begin{array}{ccc|ccc}1&0&0&14/3&-11/3&1\\0&1&0&-34/3&25/3&-2\\0&0&1&19/3&-13/3&1\end{array}\right)$$

$$K^{-1} = \begin{pmatrix}14/3&-11/3&1\\-34/3&25/3&-2\\19/3&-13/3&1\end{pmatrix} \bmod 256 = \begin{pmatrix}a&b&c\\d&e&f\\g&h&i\end{pmatrix}$$

(a) $14 \cdot 3^{-1} \bmod 256 = 14 \cdot 171 \bmod 256 = 2394 \bmod 256 = 90$

$3^{-1} \bmod 256 = 171$

$256 = 3(85) + 1 \quad 1 = 256 - 3(85)$

$3 = 1(3) + 0 \quad 1 = 256 + 3(-85)$

$3^{-1} \bmod 256 = -85 \bmod 256$

$3^{-1} \bmod 256 = 171$

Comprobación

$3 \cdot 171 \bmod 256 = 1$

$a = 90$

Duarte

Evaluación de conocimientos del primer parcial.