2019-10-23

Trabajo de repaso

David Corzo
20190432

Se llaman divisores de cero a cualesquiera $a, b \in \mathbb{Z}$, con $a \neq 0 \neq b$, tales que $a \cdot b \equiv_n 0$. Encuentre los divisores de cero $\mathbb{Z}_6$, $\mathbb{Z}_7$, $\mathbb{Z}_8$ & $\mathbb{Z}_{15}$.

- $\mathbb{Z}_6$: residuos $\text{mod}(6) = \{0, 1, 2, 3, 4, 5\}$

  $6 = 2 \cdot 3$

  descomposición prima de 6.

  R// Todos los numeros multiplos de dos & de tres menores que 6. $\{2, 4, 3\}$ son divisores de cero

- $\mathbb{Z}_7$:

  R// todos los numeros son invertibles en este módulo, no hay divisores de cero.

- $\mathbb{Z}_8$: $8 = 2^3$

  R// todos los números múltiplos de dos menores a 8.

- $\mathbb{Z}_{15}$: $15 = 3 \cdot 5$

  R// todos los números multiplos de 3 & de 5 menores a 15.

2) Encuentre los inversos de:

a) $6 \in \mathbb{Z}_{17}$

$a = 6 \qquad n = 17$

$a \cdot a^{-1} \equiv_{17} 1$

$1 \equiv_{17} 18$

$18 = 6 \cdot 3$

$6 \cdot 3 \equiv_{17} 1$

$\boxed{a^{-1} \equiv_{17} 3}$

b) $3 \in \mathbb{Z}_{10}$

$a = 3 \qquad n = 10$

$a \cdot a^{-1} \equiv_{10} 1$

$1 \equiv_{10} 11 \equiv 21$

$21 = 3 \cdot 7$

$3 \cdot 7 \equiv 1$

$\boxed{a^{-1} = 7}$

c) $5 \in \mathbb{Z}_{12}$

$a = 5 \qquad n = 12$

$5 \cdot a^{-1} \equiv_{12} 1$

$1 \equiv_{12} 13 \equiv_{12} 25$

$25 = 5 \cdot 5$

$5 \cdot 5 \equiv_{12} 1$

$\boxed{a^{-1} = 5}$

d) $7 \in \mathbb{Z}_{16}$

$a = 7 \qquad n = 16$

$7 \cdot a^{-1} \equiv_{16} 1$

$1 \equiv_{16} 17 \equiv_{16} 33 \equiv_{16} 49$

$49 = 7 \cdot 7$

$\boxed{a^{-1} = 7}$

e) $777 \in \mathbb{Z}_{1009}$

$\text{mcd}(1009, 777)$

$1009 = 777 \cdot \boxed{1} + 232$ (7)

$\text{mcd}(777, 232)$

$777 = 232 \cdot \boxed{3} + 81$ (6)

$\text{mcd}(232, 81)$

$232 = 81 \cdot \boxed{2} + 70$ (5)

$\text{mcd}(81, 70)$

$81 = 70 \cdot \boxed{1} + 11$ (4)

$\text{mcd}(70, 11)$

$70 = 11 \cdot \boxed{6} + 4$ (3)

$\text{mcd}(11, 4)$

$11 = 4 \cdot \boxed{2} + 3$ (2)

$\text{mcd}(4, 3)$

$4 = 3 \cdot \boxed{1} + 1$ (1)

$\text{mcd}(3, 1)$

$3 = 1 \cdot \boxed{3} + 0$ (0)

$\text{mcd}(1, 0) = 1$

filtrar el módulo

$211 \cdot 1009 - 274 \cdot 777 = 1$

$\mathbb{Z}_{1009}$

$211 \cdot 0 \quad 735 \cdot 777$

El inverso es: 735

master

$4 - 3 \cdot 1 = 1$

master, (2)

$4 - (11 - 4 \cdot 2) = 1$

$4 - 11 + 4 \cdot 2$

$3 \cdot 4 - 11 = 1$

master (3)

$3(70 - 11 \cdot 6) - 11 = 1$

$3 \cdot 70 - 18 \cdot 11 - 11 = 1$

$3 \cdot 70 - 19 \cdot 11 = 1$

master (4)

$3 \cdot 70 - 19(81 - 70) = 1$

$3 \cdot 70 - 19 \cdot 81 + 19 \cdot 70 = 1$

$22 \cdot 70 - 19 \cdot 81 = 1$

master (5)

$22(232 - 81 \cdot 2) - 19 \cdot 81 = 1$

$22 \cdot 232 - 44 \cdot 81 - 19 \cdot 81 = 1$

$22 \cdot 232 - 63 \cdot 81 = 1$

master (6)

$22 \cdot 232 - 63(777 - 232 \cdot 3) = 1$

$22 \cdot 232 - 63 \cdot 777 + 189 \cdot 232 = 1$

$211 \cdot 232 - 63 \cdot 777 = 1$

master (7)

$211(1009 - 777) - 63 \cdot 777 = 1$

$211 \cdot 1009 - 211 \cdot 777 - 63 \cdot 777 = 1$

$\boxed{211 \cdot 1009 - 274 \cdot 777 = 1}$

3) a). $3^{15} \in \mathbb{Z}_{17}$

+ Sacar 15 en binario

$15_2 = 1111$

$2^3\ 2^2\ 2^1\ 2^0$

$= 3^{2^3 + 2^2 + 2^1 + 2^0}$

$= 3^{2^3} \cdot 3^{2^2} \cdot 3^{2^1} \cdot 3^{2^0}$

$\frac{15}{2} = 7 + \frac{1}{2}$

$\frac{7}{2} = 3 + \frac{1}{2}$

$\frac{3}{2} = 1 + \frac{1}{2}$

$\frac{1}{2} = 0 + \frac{1}{2}$

} 1111

LSB

Bits	a	$a^2 \bmod (n)$
1	3^{2^0}	$9 \equiv_{17} 9$
1	$3^{2^1} = 9$	$9^2 = 81 \equiv_{17} 13$
1	$3^{9^2} \equiv 13$	$13^2 = 169 \equiv_{17} 16$
1	$3^{2^3} = 16$	$16^2 = 256 \equiv_{17} 1$

$3^{15} = 3^{2^3} \cdot 3^{2^2} \cdot 3^{2^1} \cdot 3^{2^0}$ $\mathbb{Z}_{17}$

$\equiv_{17} \underbrace{16 \cdot 13}_{①} \cdot \underbrace{9 \cdot 3}_{②}$

① $208 = 16 \cdot 13$

$12 * 17 = 204$

$208 \equiv_{17} 4$

② $27 = 9 \cdot 3$

$27 \equiv_{17} 10$

$\equiv_{17} \underbrace{4 \cdot 10}_{40} \equiv_{17} \boxed{6}$

$40 = 4 \cdot 10$

$2 \cdot 17 = 34$

$40 - 34 = 6$

b) $125^{4577} \in \mathbb{Z}_{13}$

$4577_2 = 1\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,0\,1$
$\quad\quad 12\ 11\ 10\ 9\ 8\ 7\ 6\ 5\ 4\ 3\ 2\ 1\ 0$

✓ $4577 = 2^{12} + 2^8 + 2^7 + 2^6 + 2^5 + 2^0$
$\quad\quad 125 \quad\quad 125 \quad 125 \quad 125 \quad 125 \quad 125 \quad 125$

	Bits	a^{2^n}	$a^2 \bmod(n)$
LSB 0	* 1	$125^{2^0} = 125 \equiv_{13} 8$	$8^2 = 64 \equiv_{13} 12$
1	0	$125^{2^1} = 125^2 \equiv_{13} 12$	$12^2 \equiv_{13} 1$
2	0	$125^{2^2} = 125^4 \equiv_{13} 1$	$1^2 \equiv_{13} 1$
3	0	$125^{2^3} = 125^8 \equiv_{13} 1$	$1^2 \equiv_{13} 1$
4	0	$125^{2^4} = 125^{16} \equiv 1$	$1^2 \equiv_{13} 1$
5	* 1	$125^{2^5} = 125^{32} \equiv 1$	$1^2 \equiv_{13} 1$
6	* 1	$125^{2^6} = 125^{64} = 1$	$1^2 \equiv_{13} 1$
7	* 1	$125^{2^7} = 125^{128} = 1$	$1^2 \equiv_{13} 1$
8	* 1	$125^{2^8} = 125^{256} = 1$	$1^2 \equiv_{13} 1$
9	0	$125^{2^9} = 125^{512} = 1$	$1^2 \equiv_{13} 1$
10	0	$125^{2^{10}} = 125^{1024} = 1$	$1^2 \equiv_{13} 1$
11	0	$125^{2^{11}} = 125^{2048} = 1$	$1^2 \equiv_{13} 1$
12	* 1	$125^{2^{12}} = 125^{4097} = 1$	$1^2 \equiv_{13} 1$

$125^{4577} = \underbrace{125^{2^{12}}}_{1} \cdot \underbrace{125^{2^8}}_{1} \cdot \underbrace{125^{2^7}}_{1} \cdot \underbrace{125^{2^6}}_{1} \cdot \underbrace{125^{2^5}}_{1} \cdot 125^{2^0}$

$= 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 8$

$= \boxed{8}$

$\frac{4577}{2} = 2288 + \frac{1}{2}$

$\frac{2288}{2} = 1144 + \frac{0}{2}$

$\frac{1144}{2} = 572 + \frac{0}{2}$

$\frac{572}{2} = 286 + \frac{0}{2}$

$\frac{286}{2} = 143 + \frac{0}{2}$

$\frac{143}{2} = 71 + \frac{1}{2}$ ↑

$\frac{71}{2} = 35 + \frac{1}{2}$ ↑

$\frac{35}{2} = 17 + \frac{1}{2}$

$\frac{17}{2} = 8 + \frac{1}{2}$ ↑

$\frac{8}{2} = 4 + \frac{0}{2}$

$\frac{4}{2} = 2 + \frac{0}{2}$ ↑

$\frac{2}{2} = 1 + \frac{0}{2}$

MSB $\frac{1}{2} = 0 + \frac{1}{2}$ ↑

$1000\ 1111\ 0000\ 1$

c) $11^{954} \in \mathbb{Z}_{20}$

$954 = \underset{9\,8\,7}{111}\ \underset{6\,5}{00}\ \underset{4\,3\,2}{111}\ \underset{1\,0}{00}$

$11^{954} = 11^{2^9} \cdot 11^{2^8} \cdot 11^{2^7} \cdot 11^{2^4} \cdot 11^{2^3} \cdot 11^{2^2}$

Bits	a	$a^2 \bmod(n)$
0 0	$11^{2^0} = 11 \equiv_{20} 11$	$11^2 \equiv_{20} 1$
1 0	$11^{2^1} = 11^2 \equiv_{20} 1$	$1^2 \equiv_{20} 1$
2 1	$11^{2^2} = 11^4 \equiv_{20} 1$	$1^2 \equiv_{20} 1$
3 1	$11^{2^3} = 11^8 \equiv_{20} 1$	$1^2 \equiv_{20} 1$
4 1	$11^{2^4} = 11^{16} \equiv_{20} 1$	$1^2 \equiv_{20} 1$
5 0	$11^{2^5} = 11^{32} \equiv_{20} 1$	$1^2 \equiv_{20} 1$
6 0	$11^{2^6} = 11^{64} \equiv_{20} 1$	$1^2 \equiv_{20} 1$
7 1	$11^{2^7} = 11^{128} \equiv_{20} 1$	$1^2 \equiv_{20} 1$
8 1	$11^{2^8} = 11^{256} \equiv_{20} 1$	$1^2 \equiv_{20} 1$
9 1	$11^{2^9} = 11^{512} \equiv_{20} 1$	$1^2 \equiv_{20} 1$

LSB $\frac{924}{2} = 462 + \frac{0}{2}$

$\frac{462}{2} = 231 + \frac{0}{2}$

$\frac{231}{2} = 115 + \frac{1}{2}$

$\frac{115}{2} = 57 + \frac{1}{2}$

$\frac{57}{2} = 28 + \frac{1}{2}$

$\frac{28}{2} = 14 + \frac{0}{2}$

$\frac{14}{2} = 7 + \frac{0}{2}$

$\frac{7}{2} = 3 + \frac{1}{2}$

$\frac{3}{2} = 1 + \frac{1}{2}$

$\frac{1}{2} = 0 + \frac{1}{2}$

1110011100

$11^{954} = \underbrace{11^{2^9}}_{1} \cdot \underbrace{11^{2^8}}_{1} \cdot \underbrace{11^{2^7}}_{1} \cdot \underbrace{11^{2^4}}_{1} \cdot \underbrace{11^{2^3}}_{1} \cdot \underbrace{11^{2^2}}_{1} \quad \text{in } \mathbb{Z}_{20}$

$\equiv_{20} 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1$

$\equiv_{20} \boxed{1}$

d) $2^{340} \in \mathbb{Z}_{31}$

$340 = 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 0$
$\quad\ 8\ 7\ 6\ 5\ 4\ 3\ 2\ 1\ 0$

Bits		a^{2^n}	$a^2 \bmod(n)$
LSB 0	0	$2^{2^0} = 2 \equiv_{31} 2$	$2^2 \equiv_{31} 4$
1	0	$2^{2^1} = 2^2 \equiv_{31} 4$	$4^2 \equiv_{31} 16$
2	1	$2^{2^2} = 2^4 = 4^2 \equiv_{31} 16$	$16^2 \equiv_{31} 8$
3	0	$2^{2^3} = 2^8 \equiv_{31} 8$	$8^2 \equiv_{31} 2$
4	1	$2^{2^4} = 2^{16} \equiv_{31} 2$	$2^2 \equiv_{31} 4$
5	0	$2^{2^5} = 2^{32} \equiv_{31} 4$	$4^2 \equiv_{31} 16$
6	1	$2^{2^6} = 2^{64} \equiv_{31} 16$	$16^2 \equiv_{31} 8$
7	0	$2^{2^7} = 2^{128} \equiv_{31} 8$	$8^2 \equiv_{31} 2$
8	1	$2^{2^8} = 2^{256} \equiv_{31} 2$	$2^2 \equiv_{31} 4$

LSB
$\frac{340}{2} = 170 + \frac{0}{2}$
$\frac{170}{2} = 85 + \frac{0}{2}$
$\frac{85}{2} = 42 + \frac{1}{2}$
$\frac{42}{2} = 21 + \frac{0}{2}$
$\frac{21}{2} = 10 + \frac{1}{2}$
$\frac{10}{2} = 5 + \frac{0}{2}$
$\frac{5}{2} = 2 + \frac{1}{2}$
$\frac{2}{2} = 1 + \frac{0}{2}$
MSB $\frac{1}{2} = 0 + \frac{1}{2}$

101010100

$16^2 = 256$
$\text{floor}(256 \div 31) = 8$
$31 * 8 = 248$
$256 - 248 = 8$

$8^2 = 64$
$\text{floor}(64 \div 31) = 2$
$31 * 2 = 62$
$64 - 62 = 2$

$2^{340} = 2^{2^8} \cdot 2^{2^6} \cdot 2^{2^4} \cdot 2^{2^2}$ $\quad \mathbb{Z}_{31}$

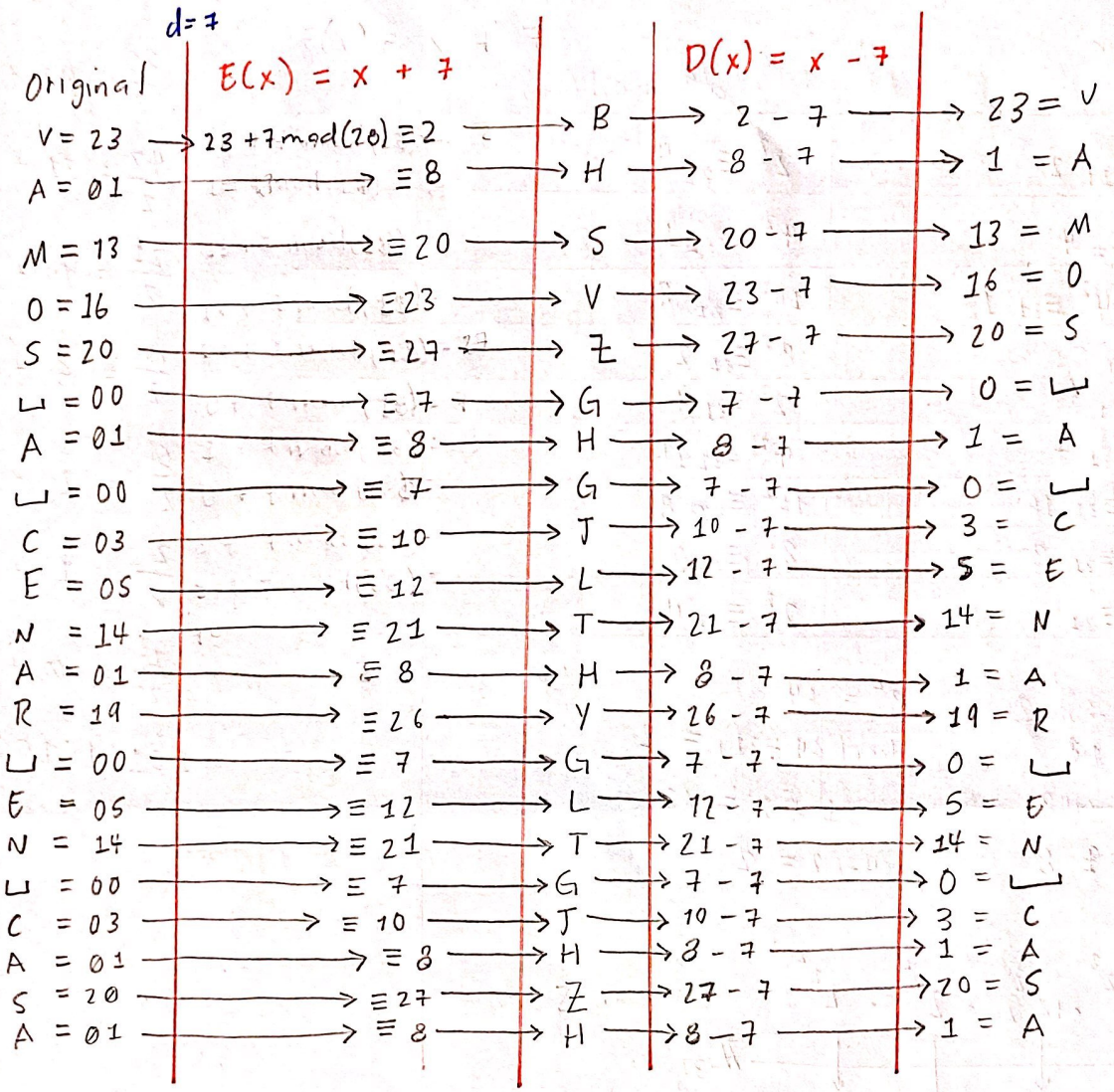
$\equiv_{31} 2 \cdot 16 \cdot 2 \cdot 16$

$\equiv_{31} 16^2 \cdot 2^2$

$\equiv_{31} 8 \cdot 4$

$\equiv_{31} 32 \equiv_{31} \boxed{1}$

4) a. Cifrado cesar con clave $d = 7$ para cifrar y descifrar el mensaje "VAMOS A CENAR EN CASA"



b) Se ha interceptado "WSHC␣C␣GSLSD" $k = 3$; $d = 0$

ORIGINAL	D(x)	
W = 24	$24 \cdot 19 - 0 = 8$	H
S = 20	$20 \cdot 19 - 0 = 16$	O
H = 8	$8 \cdot 19 - 0 = 12$	L
C = 3	$3 \cdot 19 - 0 = 1$	A
␣ = 0	$0 \cdot 19 - 0 = 0$	␣
C = 3	$3 \cdot 19 - 0 = 1$	A
␣ = 0	$0 \cdot 19 - 0 = 0$	␣
G = 7	$7 \cdot 19 - 0 = 21$	T
S = 20	$20 \cdot 19 - 0 = 16$	O
L = 12	$12 \cdot 19 - 0 = 4$	D
S = 20	$20 \cdot 19 - 0 = 16$	O
D = 4	$4 \cdot 19 - 0 = 20$	S

$E(x) = 3x + 0$

inversa de 3 mod 28

$a \cdot a^{-1} \equiv_{28} 1$

$a = 3 \quad n = 28$

mcd(28,3)

$28 = 3 \cdot \boxed{9} + 1$

mcd(3,1)

$3 = 1 \cdot \boxed{3} + 0$

mcd(1,0)

Bezout

$28 - 3 \cdot 9 = 1$

$28 - 9 \cdot 3 \equiv_{28} 1$

$0 + 19 \cdot 3 \equiv_{28} 1$

$a^{-1} = 19$

$24 \cdot 19 = 456 \equiv_{28} 8$

floor(456 ÷ 28) = 16

c) Se ha interceptado "CKI␣TAJOEDB" ; K=3 ; d=1

Original	D(x)	
C = 03	(3-1)·19 ≡ 10	J
K = 11	(11-1)·19 ≡ 28	U
I = 09	(9-1)·19 ≡ 12	L
␣ = 00	(0-1)·19 ≡ 9	I
T = 21	(21-1)·19 ≡ 16	O
A = 1	(1-1)·19 ≡ 0	␣
J = 10	(10-1)·19 ≡ 3	C
O = 16	(16-1)·19 ≡ 5	E
E = 05	(5-1)·19 ≡ 20	S
D = 04	(4-1)·19 ≡ 1	A
B = 02	(2-1)·19 ≡ 19	R

Tomando en cuenta la función de encriptado:

$$E'(x) = 3 \cdot x + 1$$

La inversa de 3 mod 28 = 19

$$D(x) = (x - 1) \cdot 19$$