Lista 04.

01. Construa as tabelas de adição e multiplicação de GF(13), utilizando a tabela encontre os inversos aditivos e multiplicativos de todos elementos GF(11)

GF(13) ADIÇÃO

+	0	1	2	3	4	5	6	7	8	9	10	11	12
0	0	1	2	3	4	5	6	7	8	9	10	11	12
1	1	2	3	4	5	6	7	8	9	10	11	12	0
2	2	3	4	5	6	7	8	9	10	11	12	0	1
3	3	4	5	6	7	8	9	10	11	12	0	1	2
4	4	5	6	7	8	9	10	11	12	0	1	2	3
5	5	6	7	8	9	10	11	12	0	1	2	3	4
6	6	7	8	9	10	11	12	0	1	2	3	4	5
7	7	8	9	10	11	12	0	1	2	3	4	5	6
8	8	9	10	11	12	0	1	2	3	4	5	6	7
9	9	10	11	12	0	1	2	3	4	5	6	7	8
10	10	11	12	0	1	2	3	4	5	6	7	8	9
11	11	12	0	1	2	3	4	5	6	7	8	9	10
12	12	0	1	2	3	4	5	6	7	8	9	10	11

inverso aditivos de GF(11)

3 = 10
4 = 9
5 = 8
6 = 7
7 = 6
8 = 5
9 = 4
10 = 3

x	0	1	2	3	4	5	6	7	8	9	10	11	12
0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12
2	0	2	4	6	8	10	12	1	3	5	7	9	11
3	0	3	6	9	12	2	5	8	11	1	4	7	10
4	0	4	8	12	3	7	11	2	6	10	1	5	9
5	0	5	10	2	7	12	4	9	1	6	11	3	8
6	0	6	12	5	11	4	10	3	9	2	8	1	7
7	0	7	1	8	2	9	3	10	4	11	5	12	6
8	0	8	3	11	6	1	9	4	12	7	2	10	5
9	0	9	5	1	10	6	2	11	7	3	12	8	4
10	0	10	7	4	1	11	8	5	2	12	9	6	3
11	0	11	9	7	5	3	1	12	10	8	6	4	2
12	0	12	11	10	9	8	7	6	5	4	3	2	1

inverso multiplicativos de GF(11)

1 = 1
2 = 7
3 = 9
4 = 10
5 = 8
7 = 3
8 = 5
9 = 3
10 = 4

/ / Primos: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43 e 47

02- Encontre 160^{-1} mod 953.

MDC(953, 160):

953	160^5	153^1	7^{21}	6^1
153	7	6	1	

$953 = 5 \cdot 160 + 153 \Rightarrow 153 : 953 - 5 \cdot 160$

$160 = 1 \cdot 153 + 7 \Rightarrow 7 : 160 - 1 \cdot 153$

$153 = 21 \cdot 7 + 6 \Rightarrow 6 : 153 - 21 \cdot 7$

$7 = 1 \cdot 6 + 1$

$1 = 7 - 1 \cdot 6$

$1 = 7 - 1 \cdot (153 - 21 \cdot 7) \Rightarrow 1 = 7 - 153 + 21 \cdot 7 \Rightarrow 1 = 153 + (1 + 21) \cdot 7$

$1 = 153 + 22 \cdot 7$

$1 = 153 + 22 (160 - 1 \cdot 153)$

$1 = 153 + 22 \cdot 160 - 22 \cdot 153 \Rightarrow 1 = 22 \cdot 160 - (1 - 22) \cdot 153 \Rightarrow 1 = 22 \cdot 160 - 23153$

$1 = 22 \cdot 160 - 23 \cdot (953 - 5 \cdot 160)$

$1 = 22 \cdot 160 - 23 \cdot 953 + 23 \cdot -5 \cdot 160$

$1 = 22 \cdot 160 - 23 \cdot 953 + 115 \cdot 160$

$1 = (22 + 115) \cdot 160 - 23 \cdot 953$

$1 = (137) 160 - 23 \cdot 953$

$R = 137$

03- $\phi(969)$

969	3
323	17
19	19
1	

$(3^1 - 3^0) \cdot (17^1 - 17^0) \cdot (19^1 - 19^0)$

$2 \cdot 16 \cdot 18$

$= 576$

04- No banco "TAMBURETE" há 5 funcionários responsáveis pela manutenção da senha de um cofre, e pelo menos 3 pessoas ($K = 3$) têm que estar presentes para a abertura do mesmo. Vamos determinar uma senha $S = 640$. Verificar como três funcionários fariam para abrir o cofre deste banco, considerando o conjunto $L = \{7, 11, 13, 17, 19\}$ composto de elementos que são

(5,3):

640 | 7 — 7 mod 640 mod 7

números primos relativamente pequenos. Determine o conjunto S e mostre como três funcionários obtêm a senha s. S = 640

L = Um conjunto de n inteiros positivos, dois a dois coprimos

N = O produto dos K's menores elementos.

M = O produto dos K-1 maiores elementos de L

S = Conjunto gerador de senhas ⇒ pares da forma (p, sp) — sp: forma reduzida de s (mod p)

Sabemos que K = 3

N = 7 · 11 · 13 = 1001

M = K - 1 · 2 ⇒ 2 maiores = 17 · 19 = 323

323 < S < 1001 ✓

S = {(7, 640 mod 7), (11, 640 mod 11), (13, 640 mod 13), (17, 640 mod 17), (19, 640 mod 19)}

S = {(7, 3), (11, 2), (13, 3), (17, 11), (19, 13)}

Funcionários: $\begin{cases} x \equiv 3 \bmod 7 \\ x \equiv 2 \bmod 11 \\ x \equiv 3 \bmod 13 \end{cases}$ M = 7 · 11 · 13 = 1001

$M_1 = \frac{1001}{7} = 143 \bmod 7 = 3 \Rightarrow 3^{-1} \bmod 5 = M_1' = 2$

$M_2 = \frac{1001}{11} = 91 \bmod 11 = 3 \Rightarrow 3^{-1} \bmod 11 = M_2' = 4$

$M_3 = \frac{1001}{13} = 77 \bmod 13 = 12 \Rightarrow 12^{-1} \bmod 13 = M_3' = 12$

$x = (4 \cdot 143 \cdot 2 + 2 \cdot 91 \cdot 4 + 3 \cdot 77 \cdot 12) \bmod 1001$

x = 640

05. Uma macro empresa possui um grande cofre, no qual por motivos de segurança, todos os 6 gerentes desta macro empresa estão de posse de uma chave de acesso e sua abertura somente é permitida com a presença de no mínimo 3 chaves de acesso. (a) Suponha que for utilizada a partilha de senhas como segurança e que o conjunto L escolhido foi {11, 13, 15, 17, 19, 23}

e a senha escolhida s é 1500, construir as chaves a serem entregues a cada gerente. (b) Escolhendo-se 3 chaves aleatórias, descubra a senha confirmando que realmente s = 1500.

$S = \{(11, 1500 \bmod 11), (13, 1500 \bmod 13), (15, 1500 \bmod 15), (17, 1500 \bmod 17), (19, 1500 \bmod 19), (23, 1500 \bmod 23)\}$.

A) $S = \{(11,4), (13,5), (15,0), (17,4), (19,18), (23,5)\}$

B) $\Rightarrow L = 1001$, $M = 437 \Rightarrow 437 < S < 1001$ ✓

Gerentes: $\begin{cases} X \equiv 4 \bmod 11 \\ X \equiv 5 \bmod 13 \\ X \equiv 4 \bmod 17 \end{cases}$ $M = 11 \cdot 13 \cdot 17 = 2431$

$M_1 = \frac{2431}{11} = 221 \bmod 11 = 1 \Rightarrow 1^{-1} \bmod 11 = M_1' = 1$

$M_2 = \frac{2431}{13} = 187 \bmod 13 = 5 \Rightarrow 5^{-1} \bmod 13 = M_2' = 8$

$M_3 = \frac{2431}{17} = 143 \bmod 17 = 7 \Rightarrow 7^{-1} \bmod 17 = M_3' = 5$

$X = (4 \cdot 221 \cdot 1 + 5 \cdot 187 \cdot 8 + 4 \cdot 143 \cdot 5) \bmod 2431$

$X = 11224 \bmod 2431 = 1500$ ✓

06. Considerando o problema anterior, suponha que houve uma troca da senha e no momento da abertura do cofre dispõe-se das chaves (11,1), (13,0), (23,21). Qual é a senha?

$\begin{cases} X \equiv 1 \bmod 11 \\ X \equiv 0 \bmod 13 \\ X \equiv 21 \bmod 23 \end{cases}$ $M = 11 \cdot 13 \cdot 23 = 3289$

$M_1 = 3289/11 = 299 \bmod 11 = 2 \Rightarrow 2^{-1} \bmod 11 = 6$

$M_2 = 3289/13 = 253 \bmod 13 = 6 \Rightarrow 6^{-1} \bmod 13 = 11$

$M_3 = 3289/23 = 143 \bmod 23 = 5 \Rightarrow 5^{-1} \bmod 23 = 14$

$X = (1 \cdot 299 \cdot 6 + 0 \cdot 253 \cdot 11 + 21 \cdot 143 \cdot 14) \bmod 3289$

$X = 43836 \bmod 3289 = 1079$ ✓

Algoritmo

d = 1

Para i = K faça -1 até 0

d = (d x d) mod n

se b_i = 1 então

d = (d x a) mod n

fim se

fim para

retorno d

07- a) 13^{46} mod 47 → a^{p-1} mod P, seja P primo, então

$a^{p-1} \equiv 1 \pmod{P}$

Logo 13^{46} mod 47 = 1

b) 11^{48} mod 49 → a^m mod n

ALGORITMO

m = 48 = 1 1 0 0 0 0

b_5 b_4 b_3 b_2 b_1 b_0

$d = 15_{10}$

11^{48} mod 49 = 15

d	a	m	n	i	K	b_i
1	11	48	49	5	5	$b_5 = 1$
1						
d = 1 · 11 mod 49						
d = 11						
d = d · d				4		$b_4 = 1$
d = 11 · 11 mod 49						
d = 23						
$b_4 = 1$ → d · a						
d = 23 · 11 mod 49						
d = 8						
d = 8 · 8 mod 49				3		$b_3 = 0$
d = 15						
d = 15 · 15 mod 49				2		$b_2 = 0$
d = 29						
d = 29 · 29 mod 49				1		$b_1 = 0$
d = 8						
d = 8 · 8 mod 49 = 15				0		$b_0 = 0$

20 mod 6 = 2

191 e 193 primos

08- Encontre $\phi(n)$ para todos os n's inteiros de 190 a 195

$\phi(190)$: 190 | 2 ; 95 | 5 ; 19 | 19 ; 1

$(2^1-2^0)\cdot(5^1-5^0)\cdot(19^1-19^0)$

$1 \cdot 4 \cdot 18$

$= 72$

$\phi(191)$ = é primo, logo 1

$\phi(192)$: 192 | 2 ; 96 | 3 ; 32 | 2 ; 16 | 2 ; 8 | 2 ; 4 | 2 ; 2 | 2 ; 1

$(2^6-2^5)\cdot(3^1-3^0)$

$(64-32)\cdot 2$

64

$\phi(193)$ = 193 é primo, logo = 1

$\phi(194)$: 194 | 2 ; 97 | 97 ; 1

$(2^1-2^0)\cdot(97^1-97^0)$

$1 \cdot 96$

$= 96$

$\phi(195)$: 195 | 5 ; 39 | 3 ; 13 | 13 ; 1

$(5^1-5^0)\cdot(3^1-3^0)\cdot(13^1-13^0)$

$4 \cdot 2 \cdot 12$

96

09- Multiplique $2345_{(6)}$ por $234_{(6)}$:

$2345_{(6)} \times 234_{(6)}$

	1	1	1		
	1	2	2		
1	2	3	4	5	(6)
		2	3	4	(6)
	1	4	3	1	2
1	1	5	2	3	
	5	1	3	4	
0	3	0	3	4	2 (6)

20 | 6 ; 18 | 3 → sobe ; 2 → base

19 | 6 ; 18 | 3

15 | 6 ; 12 | 2 ; 3

10 | 6 ; 6 | 1 ; 1

15 | 6 ; 14 | 6 ; 2

11 | 6 ; 6 | 1 ; 7 | 6 ; 1 ; 5 ; 1

10 | 6 ; 4 ; 1 ; 9 | 6 ; 3 ; 1 ; 7 | 6 ; 1 ; 1

9 mod 6 = 3

12 mod 6 = 0

25 | 16
16 | 1
9

154 | 16
144 | 9

10. Multiplicar BA_H por $1C_H$ módulo $11B_H$, utilizando a operação polinomial em $GF(2^8)$, operação utilizada no AES

$BA_H \cdot 1C_H$ → Se fosse 1 $x^0 = 1$

$10111010 \cdot 00011100$

$(x^7 + x^5 + x^4 + x^3 + x^1) \cdot (x^4 + x^3 + x^2)$

$x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^7 + x^6 + x^5 + x^5 + x^4 + x^3$

↳ divide por $11B_H \Rightarrow 0001\,0001\,1011 \Rightarrow x^8 + x^4 + x^3 + x + 1$

↳ Acha o resultado, mas farei com a tabela pois é mais fácil

$L(BA) = A1 \quad L(1C) = F8$

(L: linha, C: coluna)

$A1 \rightarrow 10 \cdot 16^1 + 1 \cdot 16^0 = 161_{(10)}$

$F8 \rightarrow 15 \cdot 16^1 + 8 \cdot 16^0 = 248_{(10)}$

$199_{(H)} \longleftarrow 409_{(10)}$

↳ $409_{(10)} \rightarrow HEXA = \frac{409}{16} = 25 \rightarrow$ resto 9

reduzir em mod 255 (FF)

$\frac{25}{16} = 1 \rightarrow$ resto 9

$\frac{1}{16} = 0 \rightarrow$ resto 1

199 (FF)

↳ 409 | 255
255 | 1

$154_{(10)} \rightarrow HEXA = \frac{154}{16} = 9 \rightarrow$ resto 10 → (A)

$154 = 9A_{(H)}$

$BA \cdot 1C = 9A$