Confirmar o resultado de $84_h \cdot C1_h = 7E_h$

↳ Pela tabela logaritmo ⇒ $L(84) = F4$ → $L(C1) = B2$

$F4 + B2 = 1A6$

$$\begin{array}{r} F4 \\ B2 \\ \hline 1A6 \end{array}$$

↳ Reduzir em modulo 255

$1A6_h \;|\; FF$ → Resto $A7_h$

$FF_h \;\; 1$

$A7_h$ → Resto

Na tabela de exponente isso deve dar o resultado encontrado (7E)

$A7_h$ → $7E_h$ na tabela

Confirmar se $57_h \cdot 83_h = C1_h$

↳ $L(57) = 62$ $L(83) = 50$

Linha Coluna

$$\begin{array}{r} 62_h \\ +\,50_h \\ \hline B2_h \end{array}$$

$B2_h \;|\; FF_h$

$B2 \;\; 1$

0 → Resto → Tabela de exponente ⇒ $E(B2) = C1_h$ (correto)

Lista 02.

1- Multiplicar $B4_h$ por $C1_h$ módulo $11B_h$ em $GF(2^8)$

$B4_h \cdot C1_h$

↳ $L(B4) = Fb$ $L(C1) = b2$

$$\begin{array}{r} Fb \\ +\,b2 \\ \hline 1AD \end{array}$$

$1AD \;|\; FF$

$FF \;\; 1$

AE → $E(AE) = 89$

20 | 11 → 11 | 1 → 9 | 1

12 | 11 → 11 | 1 → 1

13 | 11 → 11 | 1 → 2

100 | 11 → 99 | 9 → 1

Q2. Calcular $7C_h + 35_h$, com a representação polinomial em GF(2^8)

$7C_h \rightarrow 7\ 12_{10}$ $\quad 35_h \rightarrow 3\ 5_{10}$

$0111\ 1100_2$ $\quad 0011\ 0101_2$

$(x^6 + x^5 + x^4 + x^3 + x^2) + (x^5 + x^4 + x^2 + 1)$

$x^6 + 2x^5 + x^4 + x^3 + 2x^2 + 1 \Rightarrow x^6 + x^4 + x^3 + 1$

$\underbrace{0\ 1\ 0\ 1}_{5}\ \underbrace{1\ 0\ 0\ 1}_{9} = 59_h$

Q3. Construa as tabelas de adição e multiplicação para GF(11) e GF(19) e encontre os inversos aditivo e multiplicativo.

GF(11)

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

GF(11)

×	0	1	2	3	4	5	6	7	8	9	10
0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10
2	0	2	4	6	8	10	1	3	5	7	9
3	0	3	6	9	1	4	7	10	2	5	8
4	0	4	8	1	5	9	2	6	10	3	7
5	0	5	10	4	9	3	8	2	7	1	6
6	0	6	1	7	2	8	3	9	4	10	5
7	0	7	3	10	6	2	9	5	1	8	4
8	0	8	5	2	10	7	4	1	9	6	3
9	0	9	7	5	3	1	10	8	6	4	2
10	0	10	9	8	7	6	5	4	3	2	1

inversos aditivos: 1=10, 2=9, 3=8, 4=7

5=6, 6=5, 7=4, 8=3, 9=2, 10=1

inversos mult.: 1=1, 2=6, 3=4, 4=3, 5=9

6=2, 7=8, 8=7, 9=5, 10=10

GF(19)

+	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	0
2	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	0	1
3	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	0	1	2
4	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	0	1	2	3
5	5	6	7	8	9	10	11	12	13	14	15	16	17	18	0	1	2	3	4
6	6	7	8	9	10	11	12	13	14	15	16	17	18	0	1	2	3	4	5
7	7	8	9	10	11	12	13	14	15	16	17	18	0	1	2	3	4	5	6
8	8	9	10	11	12	13	14	15	16	17	18	0	1	2	3	4	5	6	7
9	9	10	11	12	13	14	15	16	17	18	0	1	2	3	4	5	6	7	8
10	10	11	12	13	14	15	16	17	18	0	1	2	3	4	5	6	7	8	9
11	11	12	13	14	15	16	17	18	0	1	2	3	4	5	6	7	8	9	10
12	12	13	14	15	16	17	18	0	1	2	3	4	5	6	7	8	9	10	11
13	13	14	15	16	17	18	0	1	2	3	4	5	6	7	8	9	10	11	12
14	14	15	16	17	18	0	1	2	3	4	5	6	7	8	9	10	11	12	13
15	15	16	17	18	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
16	16	17	18	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
17	17	18	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
18	18	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17

INVERSO ADITIVO - 1 = 18

2 = 17

3 = 16

4 = 15

5 = 14

6 = 13

7 = 12

8 = 11

9 = 10

10 = 9

11 = 8

12 = 7

13 = 6

14 = 5

15 = 4

16 = 3

17 = 2

18 = 1

GF (19)

X	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
0	0	0	0	0	0	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	13	14	15	16	17	18
2	0	2	4	6	8	10	12	14	16	18	1	3	5	7	9	11	13	15	17
3	0	3	6	9	12	15	18	2	5	8	11	14	17	1	4	7	10	13	16
4	0	4	8	12	16	1	5	9	13	17	2	6	10	14	18	3	7	11	15
5	0	5	10	15	1	6	11	16	2	7	12	17	3	8	13	18	4	9	14
6	0	6	12	18	5	11	17	4	10	16	3	9	15	2	8	14	1	7	13
7	0	7	14	2	9	16	4	11	18	6	13	1	8	15	3	10	17	5	12
8	0	8	16	5	13	2	10	18	7	15	4	12	1	9	17	6	14	3	11
9	0	9	18	8	17	7	16	6	15	5	14	4	13	3	12	2	11	1	10
10	0	10	1	11	2	12	3	13	4	11	5	15	6	16	7	17	8	18	9
11	0	11	3	14	6	17	9	1	12	4	15	7	18	10	2	13	5	16	3
12	0	12	5	17	10	3	15	8	1	13	6	18	11	4	16	9	2	14	7
13	0	13	7	1	14	8	2	15	9	3	16	10	4	17	11	5	18	12	6
14	0	14	9	4	18	13	8	3	17	12	7	2	16	11	6	1	15	10	5
15	0	15	11	7	3	18	14	10	6	2	17	13	9	5	1	16	12	8	4
16	0	16	13	10	7	4	1	17	14	11	8	5	2	18	15	12	9	6	3
17	0	17	15	13	11	9	7	5	3	1	18	16	14	12	10	8	6	4	2
18	0	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

Inversos multip.:

1 = 1
2 = 10
3 = 13
4 = 5
5 = 4
6 = 16
7 = 11
8 = 12
9 = 17
10 = 2
11 = 7
12 = 8
13 = 3
14 = 15
15 = 14
16 = 6
17 = 9
18 = 18

4. Com polinômio em Z_{10}

a) $(7x+2)-(3x^2+5)$

$7x+2-3x^2-5$

$-3x^2+7x+(2-5)$ → -3

↳ $-3 \equiv 7 \mod 10$ → $-3+10=7$

$-3x^2+7x+7$

↳ Acima temos que -3 no módulo 10 é 7

$R = 7x^2+7x+7$

b) $(6x^2+x+3)\cdot(4x^2+2)$

↳ $24x^4+12x^2+4x^3+2x+12x^2+6$

$24x^4+4x^3+24x^2+2x+6$

↳ Z_{10} => $24 \equiv 4 \mod 10$

$4 \equiv 4 \mod 10$

$24 \equiv 4 \mod 10$

$2 \equiv 2 \mod 10$ → resto

$6 \equiv 6 \mod 10$

$R = 4x^4+4x^3+4x^2+2x+6$

5. Três satélites passarão sobre o Rio este norte. O primeiro à 2h da madrugada, o segundo às 5h e o terceiro às 8h da manhã. Cada satélite tem um período diferente. O primeiro leva 13h para completar uma volta em torno da terra, o segundo 15 e o terceiro 19 horas. Determine quantas horas decorrerão, a partir desta meia noite, até que os três satélites passem ao mesmo tempo sobre o R.O.

Resolvendo utilizando o teorema do Chinês =

/ /

: equações modulares :

Satélite 1 → $t \equiv 2 \pmod{13}$ → passa as 2h e repete a cada 13h

Satélite 2 → $t \equiv 5 \pmod{15}$

Satélite 3 → $t \equiv 8 \pmod{19}$

$M = 13 \cdot 15 \cdot 19$

$M = 3705$

$M_1 = \frac{3705}{13} = 285$

$M_2 = \frac{3705}{15} = 247$

$M_3 = \frac{3705}{19} = 195$

$M_1 = 285 \bmod 13$ ↔ $M_1^{-1} = 12^{-1} \bmod 13 = 12$

↳ $285 \equiv 12 \bmod 13$

$M_2 = 247 \bmod 15$ ↔ $M_2^{-1} = 7^{-1} \bmod 15 = 13$

↳ $247 \equiv 7 \bmod 15$

$M_3 = 195 \bmod 19$ ↔ $M_3^{-1} = 5^{-1} \bmod 19 = 4$

↳ $195 \equiv 5 \bmod 19$

$t = (2 \cdot 285 \cdot 12) + (5 \cdot 247 \cdot 13) + (8 \cdot 195 \cdot 4)$

$t = 29135$

$t \bmod M \rightarrow 29135 \bmod 3705 = 1055$

1055 um dias e horas = 43 dias e 23 horas

6. Menor inteiro positivo que dissa resto 2 na divisão por 5, resto 4 na divisão por 7 e resto 5 na divisão por 11 Teorema do Resto Chinês

$t \equiv 2 \bmod 5$

$t \equiv 4 \bmod 7$

$t \equiv 5 \bmod 11$

$M = 5 \cdot 7 \cdot 11 = 385$

$M_1 = \frac{385}{5} = 77 \rightarrow 77 \bmod 5 = 2 \rightarrow M_1^{-1} = 2^{-1} \bmod 5 = 3$

$M_2 = \frac{385}{7} = 55 \rightarrow 55 \bmod 7 = 6 \rightarrow M_2^{-1} = 6^{-1} \bmod 7 = 6$

$M_3 = \frac{385}{11} = 35 \rightarrow 35 \bmod 11 = 2 \rightarrow M_3^{-1} = 2^{-1} \bmod 11 = 6$

$t = (2 \cdot 77 \cdot 3) + (4 \cdot 55 \cdot 6) + (5 \cdot 35 \cdot 6) = 2832 \rightarrow 2832 \bmod 385 = 137$ //

SOLDADOS

7. $x \equiv 5 \mod 7$ Onde $x > 1500$

$x \equiv 4 \mod 9$

$x \equiv 1 \mod 10$

$M = 7 \cdot 9 \cdot 10 = 630$

$M_1 = \frac{630}{7} = 90 \rightarrow 90 \mod 7 = 6 \rightarrow 6^{-1} \mod 7 = 6$

$M_2 = \frac{630}{9} = 70 \rightarrow 70 \mod 9 = 7 \rightarrow 7^{-1} \mod 9 = 4$

$M_3 = \frac{630}{10} = 63 \rightarrow 63 \mod 10 = 3 \rightarrow 3^{-1} \mod 10 = 7$

$tot x = (5 \cdot 90 \cdot 6) + (4 \cdot 70 \cdot 4) + (1 \cdot 63 \cdot 7) = 4261$

$4261 \mod 630 = 481$

481 menor que 1500

↳ Como usamos no 2630 → $481 + 630 = 1111$ menor

↳ $1111 + 630 = 1741$ maior que 1500

INÍCIO = 2000 SOLDADOS

Soldados Mortos = $2000 - 1741 = 259$ ↳

8. $\begin{cases} x \equiv 4 \mod 5 \\ x \equiv 3 \mod 7 \\ x \equiv 5 \mod 16 \end{cases}$ $M = 5 \cdot 7 \cdot 16 = 560$

$M_1 = 560/5 = 112 \mod 5 = 2$,

$M_2 = 560/7 = 80 \mod 7 = 3$,

$M_3 = 560/16 = 35 \mod 16 = 3$,

$M_1' = 2^{-1} \mod 5 = 3$

$M_2' = 3^{-1} \mod 7 = 5$

$M_3' = 3^{-1} \mod 16 = 11$

$tot x = (4 \cdot 112 \cdot 3) + (3 \cdot 80 \cdot 5) + (5 \cdot 35 \cdot 1) = 4469$

$4469 \mod 560 = 549$ ↳

Ex no Slide

11. $\begin{cases} z \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$

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

$M_1 = \frac{105}{3} = 35 \bmod 3 = 1 \Rightarrow 1^{-1} \bmod 3 = 2 \bmod 3$

$M_2 = \frac{105}{5} = 21 \Rightarrow M_2' = 1 \pmod 5$

$M_3 = \frac{105}{7} = 15 \Rightarrow M_3' = 1 \pmod 7$

$z = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233 \equiv 23 \pmod{105}$

9. $\begin{cases} x \equiv 3 \bmod 5 \\ x \equiv 5 \bmod 3 \\ x \equiv 11 \bmod 7 \\ x \equiv 3 \bmod 4 \end{cases}$

$M_1 = \frac{420}{5} = 84 \bmod 5 = 4$

$M_2 = \frac{420}{3} = 140 \bmod 3 = 2$

$M_3 = \frac{420}{7} = 60 \bmod 7 = 4$

$M_4 = \frac{420}{4} = 105 \bmod 4 = 1$

$M = 5 \cdot 3 \cdot 7 \cdot 4 = 420$

$M_1' = 4^{-1} \bmod 5 = 4$

$M_2' = 2^{-1} \bmod 3 = 2$

$M_3' = 4^{-1} \bmod 7 = 2$

$M_4' = 1^{-1} \bmod 4 = 1$

$\therefore x = (3 \cdot 84 \cdot 4) + (5 \cdot 140 \cdot 2) + (60 \cdot 11 \cdot 2) + (3 \cdot 105 \cdot 1) \bmod M$

$x = 4043 \bmod 420$

$x = 263 \bmod 420$

10. Problema de confiança Empresarial: O cofre de valores da empresa X somente será aberto com a digitação das senhas de 2 dos 5 funcionários responsáveis pela manutenção do mesmo, ou seja, os dois funcionários tem que estarem presentes para digitação de suas respectivas senhas. Seja $S = \{(7,6), (11,3), (13,4), (17,1), (19,12)\}$ o conjunto das senhas secretas dos 5 funcionários. Qual a senha s para abrir o cofre?

Utilizando os funcionários (7,6) e (13,4).

$\begin{cases} x \equiv 6 \mod 7 \\ x \equiv 4 \mod 13 \end{cases}$

$M = 7 \cdot 13 = 91$

$M_1 = \frac{91}{7} = 13 \mod 7 = 6$

$M_2 = \frac{91}{13} = 7 \mod 13 = 7$

$M_1' = 6^{-1} \mod 7 = 6$

$M_2' = 7^{-1} \mod 13 = 2$

$x = (6 \cdot 13 \cdot 6) + (4 \cdot 7 \cdot 2) \mod M$

$x = 524 \mod 91$

$x = 69 \mod 91$

Senha 69