LISTA 4

NOME: GABRIEL ALMEIDA MENDES DRE: 117204959

(1) a) ACHAR $330\alpha + 240\beta = 210$

$330\alpha + 240\beta = mdc(330, 240)$

RESTO	QUOCIENTE	α	β
330	*	1	0
240	*	0	1
90	1	$1-(1)\cdot 0 = 1$	$0-(1)\cdot 1 = -1$
60	2	$0-(2)\cdot 1 = -2$	$1-(2)\cdot(-1) = 3$
30	1	$1-(1)\cdot(-2) = 3$	$-1-(1)\cdot(+3) = -4$
0	2	*	*

$\alpha = 3$ $\beta = -4$ $mdc(330, 240) = 30 \longrightarrow 210/30 = 7$

$330\cdot 3 + 240\cdot(-4) = 30(\cdot 7)$

$330\cdot(3)(7) + 240(-4)(7) = 30\cdot(7)$

$330(21) - 240(28) = 210$

R: OS MULTIPLOS SÃO 21 E 28

b) AS SOLUÇÕES INTEIRAS SÃO: $330\cdot(3\cdot 7 - 240k) + 240(-4\cdot 7 + 330k) = 210$

(2) JOGO COM DOIS TIPOS DE PONTUAÇÃO: 5 E 11

POSSIVEL PONTUAÇÃO DE: 86×39

$86\alpha + 39\beta = mdc(86, 39)$

RESTO	QUOCIENTE	α	β
86	*	1	0
39	*	0	1
8	2	$1-(2)\cdot 0 = 1$	$0-(2)(1) = -2$
7	4	$0-(4)\cdot 1 = -4$	$1-(4)(-2) = 9$
1	1	$1-(1)\cdot(-4) = 5$	$-2-(1)(9) = -11$
0	7	*	*

R: SIM É POSSIVEL. POR QUE DADO O MDC ENTRE ELES É POSSIVEL ACHAR VALORES DE α E β IGUAL A 5 E 11.

(3) DETERMINE TODOS OS POSSIVEIS VALORES DE $mdc(a, p^2)$

R: PARA $MDC(a, p^2)$, TENDO p COMO PRIMO OU SEJA $p = p*1$, CONCLUI-MOS QUE EM a EXISTE PELO MENOS UM NUMERO p COMO FATOR COMUM QUE DIVIDE OS DOIS E OS DEMAIS DIFERENTES DE P.

PORTANTO EXISTE VALOR p QUE DIVIDE a, p^2

(5) SEJA $m > 0 \in \mathbb{Z}^*$ COMPOSTO e p SEU MENOR FATOR PRIMO. SABE-SE QUE $p \geq \sqrt{m}$ E QUE $p-4$ DIVIDE $mdc(6m+7, 3m+2)$. DETERMINE TODOS OS POSSIVEIS VALORES m.

RESPOSTA: SENDO p PRIMO E MENOR FATOR DE m, TEMOS $p \leq \sqrt{m}$. MAS POR HIPOTESE, $p \geq \sqrt{m}$ AQUI; OU SEJA $p = \sqrt{m}$ É A UNICA SITUAÇÃO POSSIVEL.

$mdc(6m+7, 3m+2) = \pm 1$

RESTO	QUOCIENTE
$6m+7$	*
$2 \cdot 3m+2$	1
-3	1
± 1	*

COMO TEMOS QUE: $p-4 \mid mdc(6m+7, 3m$

ENTÃO: $p-4 \mid \pm 1$

DOIS CASOS = $1 = (p-4) \cdot q$
$-1 = (p-4) \cdot q$

PARA EM AMBOS OS CASOS, PARA $q = 1$, p PRECISSA SER 3 e/ou 5.

$$\begin{cases} p = 3 \rightarrow 3 = \sqrt{m} = 9 = m \\ p = 5 \rightarrow 5 = \sqrt{m} = 25 = m \end{cases}$$

R = OS VALORES POSSIVEIS PARA m SÃO 9 E 25

(6) MOSTRE QUE EXISTE UM INTEIRO MÚLTIPLO DE 241^2 QUE TERMINA EM 241.

RESPOSTA: MÚLTIPLO DE 241^2 É O MESMO QUE DIZER $a = 241^2 \cdot q$

TEMOS $a = 1000m + 241$, ENTÃO $1000m + 241 = 241^2 \cdot q$

USANDO A IDENTIDADE DE BEZOUT PODE MONTAR A EQUAÇÃO ASSIM:

$$1000m - 241^2 q = -241(-1)$$

$$241^2 q - 1000m = 241$$

$$58081q - 1000m = 241$$

COMO QUEREMOS ENCONTRAR VALORES QUE SATISFAÇÃO m, FAREMOS O EUCLIDIANO ESTENDIDO

RESTO	QUOCIENTE	m
58081	*	0
1000	*	1
81	58	$0-(58)\cdot 1 = -58$
28	12	$1-(12)\cdot(-58) = 697$
25	2	$-58-(2)(697) = -1459$
3	1	$697-(1)\cdot(-1459) = 2149$
1	8	$-1459-(8)(2149) = -18644$
0	3	*

$241/1 = 241$

$$58081 \cdot q - 1000m = 1$$

$$58081 \cdot q - 1000(-18644) = 1$$

$$58081 \cdot q + 1000(18644) = 1(241)$$

$$58081 \cdot 241 \cdot q + 1000 \cdot (4493204) = 241$$

ACHAMOS $m = 4493204$, AGORA SUBSTITUINDO E CALCULANDO

$1000(4493204) + 241 = 4493204241$.

O INTEIRO MÚLTIPLO DE 241^2 QUE TERMINA EM 241 É 4493204241.

7) a) ENCONTRE X E Y, CUJO MDC(X,Y)=1 DEMORE 5 PASSOS PARA SE ENCONTRADO.

RESPOSTA: ENTENDO O FUNCIONAMENTO DO MDC PODEMOS FAZER O ALGORITMO AO CONTRARIO E CONTAR OS PASSOS

NO ULTIMO PASSO TERIAMOS DOIS NUMEROS QUE SERIAM PRIMOS ENTRE SI, ASSIM:

$(a, 1) = 1$

TOMEMOS a UM Nº QUALQUER QUE SATISFAÇA A CONTA:

$(2, 1) = 1 \to$ 1º PASSO

NO PASSO SEGUINTE PEGAMOS O a QUALQUER E FAZEMOS: $(b, 2)$

PARA ACHAR b TEMOS QUE LEVA EM CONTA QUE O QUOCIENTE DA DIVISÃO É 1 ENTÃO $b = 2K + 1$, ONDE K É O QUOCIENTE QUE DÁ 1, ENTÃO: $b = 2 \cdot 1 + \underline{1} \to b = 3$

$(3, 2) \to$ 2º PASSO

CONTINUAMOS FAZENDO ISSO SEMPRE ALTERNANDO OS NÚMEROS PEGAMOS

$(c, 3)$ E $c = 3(1) + \underline{2} \to c = 5$

3º PASSO $\leftarrow (5, 3)$

PROXIMO CASO TEMOS:

$(d, 5)$ E $d = 5(1) + 3 \to d = 8$

ENTÃO: $(8, 5) \to$ 4º PASSO

PROXIMO CASO TEMOS:

$(e, 8)$ E $e = 8(1) + 4 \to e = 12$

ENTÃO: $(12, 8) = 4$ NÃO SERVE

$(e, 8)$ E $e = 8(1) + \underline{5} \to e = 13$

ENTÃO: $(13, 8) = 1 \to$ 5º PASSO

OS DOIS NÚMEROS QUE DEMORAM 5 PASSO PARA MDC IGUAL A 1 É 13 E 8.

b) ENCONTRE X E Y, CUJO MDC(X,Y)=1 DEMORE 6 PASSO PARA SE ENCONTRADO,

RESPOSTA: BASTA CONTINUAR DE ONDE PAROU O EXERCICIO 7.a

PROXIMO CASO TEMOS: $(f, 13)$ E $f = 13(1) + 6 \to f = 19$

ENTÃO: $(19, 13) = 1$

$f = 13(1) + 7 \to f = 20$

ENTÃO: $(20, 13) = 1$

MAS NÃO SERVE POIS NÃO POSSIBILITA PADRAO

$f = 13(1) + 8 \to f = 21$

ENTÃO: $(21, 13) = 1$

c) NOTE QUE A DIFERENÇA DOS PARES, QUE SÃO OS QUOCIENTE, FORMOS UM PADRÃO, QUANDO POSTOS EM SEQUENCIA, A SEQUENCIA DE FIBONACCI. ENTÃO PODEMOS USAR UM TERMO GENERALIZADO:

$$F_K = F_{K-1} + F_{K-2}$$

(9) $a, b, c, d \in \mathbb{N}$. PROVE OU REFUTE:

b) $(a|b$ ou $a|c)$ SSE $a|bc$

PROVE: $a|b \to a|bc$ ou $a|c \to a|bc$.

SUPONHA $a|b \to b = aq$ E $a|c \to c = aq$

MULTIPLIQUE POR c OU b $\to bc = (aq)c$ E $cb = (aq)b$

REORGANIZANDO $bc = a(qc)$ E $cb = a(qb)$

ENTÃO $a|bc$ SE CONFIRMA VERDADEIRO

(10) $\text{mmc}(a,b) = \dfrac{ab}{\text{mdc}(a,b)}$, PROVE AS SEGUINTES AFIRMAÇÕES

a) $\text{mmc}(a,b) \cdot \text{mdc}(a,b) = ab$

LEMA 1: SEJAM $(a,b) \in \mathbb{Z}^*$ E $d = \text{mdc}(a,b)$ ENTÃO $a = dq_1$, $b = dq_2$ E $\text{mdc}(q_1, q_2) = 1$

LEMA 2: SEJAM $(a,b) \in \mathbb{Z}^*$ E $m = \text{mmc}(a,b)$ ENTÃO $m = ah_1$, $m = bh_2$ E $\text{mdc}(h_1, h_2) = 1$

AGORA PROVAMOS O TEOREMA INICIAL

$d = \text{mdc}(a,b)$

$a = dq_1$

$b = dq_2$

$\text{mdc}(q_1, q_2) = 1$

$m = \text{mmc}(a,b)$

$m = ah_1 \to h_1 = \dfrac{m}{a}$

$m = bh_2 \to h_2 = \dfrac{m}{b}$

$\text{mdc}(h_1, h_2) = 1$

$$\left.\begin{array}{l} m = a \cdot h_1 \to m = (dq_1)h_1 \\ m = b \cdot h_2 \to m = (dq_2)h_2 \end{array}\right\} \cancel{d}q_1h_1 = \cancel{d}q_2h_2$$

$q_1h_1 = q_2h_2$ ENTÃO:

$h_1|q_2$, $h_2|q_1$, $q_1|h_2$, $q_2|h_1$

ISSO TUDO SÓ POSSIVEL SE $q_1 = h_2$ E $q_2 = h_1$

ASSIM: $\left.\begin{array}{l} a = dq_1 = dh_2 \\ b = dq_2 = dh_1 \end{array}\right\}$

$a \cdot b = dh_2 \cdot dh_1$

$ab = d^2 h_2 h_1$

$ab = d^2 \dfrac{m}{a} \cdot \dfrac{m}{b} \to ab = \dfrac{d^2m^2}{ab} \to a^2b^2 = d^2m^2 \to ab = \underset{\text{mdc}}{d} \cdot \underset{\text{mmc}}{m}$

PROVADO

b) PROVE QUE mmc(a,b) = ab SSE mdc(a,b) = 1.

$$mmc(a,b) = \frac{ab}{mdc(a,b)}$$

$$mmc(a,b) = \frac{ab}{1}$$, ENTÃO

$$mmc(a,b) = ab.$$

e) $m \in \mathbb{N}$, TEMOS $(a|m$ E $b|m)$ SSE $mmc(a,b)|m$

$m = aq_1$ $\quad m' = a \cdot h_1$ $\quad m = mmc(a,b)q_3$

$m = bq_2$ $\quad m' = b \cdot h_2$ $\quad m = m'q_3$

$m = \frac{m'}{h_1} \cdot q_1$ $\quad \frac{m'}{h_1} = a$ $\quad \frac{mh_1}{q_1} = \frac{mh_2}{q_2} = \frac{h_1}{q_1} = \frac{h_2}{q_2}$

$m = \frac{m'}{h_2} q_2$ $\quad \frac{m'}{h_2} = b$ $\quad h_1 q_2 = h_2 q_1$

SÓ POSSÍVEL SE: $h_1 = q_1$ E $h_2 = q_2$

$m = \frac{m' q_1}{q_1}$ $\quad m = \frac{m' q_2}{q_2}$