Álgebra 1

Lista 03

(Divisão Euclidiana e M.D.C)

3.1. (Sequência de Fibonacci). Prove que, na sequência $0, 1, 1, 2, 3, 5, 8, 13, ...,$ na qual cada termo a partir do terceiro é a soma dos dois precedentes, o m.d.c. de quaisquer dois termos consecutivos é igual a 1.

Seja F_n e F_{n+1} dois termos consecutivos quaisquer da sequência de Fibonacci.

Sabemos, por definação, que :

$$F_{n+1} = F_n + F_{n-1}, n \geq 2$$

Pensando na sequência como uma divisão euclidiana de quociente igual à 1 temos,

$$F_{n+1} = (1) \cdot F_n + F_{n-1}$$

Logo, o $mdc(F_{n+1}, F_n) = mdc(F_n, F_{n-1})$ pois se $a = b \cdot q + r$ então $mdc(a, b) = mdc(b, r)$

Aplicando essa lógica redutiva até os primeiros termos da sequência temos :

$\ldots = mdc(3, 2) = mdc(2, 1) = 1$

3.2. $(GL_2(\mathbb{Z}))$. Se p, q, r e s são inteiros tais que $ps - qr = \pm 1$, e a, b, a', b' são inteiros tais que

$$\begin{cases} a' = pa + qb, \\ b' = ra + sb \end{cases}$$

prove que $m.d.c.(a', b') = m.d.c.(a, b)$.

A ideia é mostrar que $mdc(a, b) \mid mdc(a', b')$ pois a única maneira de inteiros positivos se dividirem mutualmente e se eles forem **iguais**

I. $mdc(a, b) = d$
   - $d \mid a \to a = d \cdot k_1$
   - $d \mid b \to b = d \cdot k_2$

   Substituindo no sistema temos,

$$\begin{cases} a' = p(dk_1) + q(dk_2) = d \cdot (pk_1 + qk_2) \\ b' = r(dk_1) + s(dk_2) = d \cdot (rk_1 + sk_2) \end{cases}$$

   Como $d \mid a'$ e $d \mid b'$, por definição, $d|mdc(a', b') = \boxed{mdc(a, b)|mdc(a', b')}$

II. Pelo Sistema,

   $L_1 \cdot s - L_2 \cdot q \Rightarrow sa' - b'q = psa + qsb - qra - qsb$

   $sa' - b'q = a \cdot (ps - qr),$ logo $a = \pm(a's - b'q)$

   De forma Analoga, $b = \pm(pb' - ra')$

   Assim, seja $mdc(a', b') = d'$

   Como, $d' \mid a'$ e $d' \mid b'$, então d' divide qualquer combinação linear entre eles

   Logo, $d' \mid a$ e $d' \mid b$ portanto $d' \mid mdc(a, b) = \boxed{mdc(a', b') \mid mdc(a, b)}$

3.3. (Para no m.d.c.). Sejam a e b dois inteiros > 0. Faça $a_0 = a, a_1 = b$, e para $n \geq 1$ defina a_{n+1} por $a_{n-1} = a_n q_n + a_{n+1}$, com $0 \leq a_{n+1} < a_n$ desde que $a_n > 0$. Demonstre que existe $N \geq 1$ tal que $a_{N+1} = 0$, e que $a_N = m.d.c.(a, b)$.

$a_0 = 0, a_1 = b$

$a_{n-1} = a_n q_n + a_{n+1}$, com $0 \leq a_{n+1} < a_n$

I. Existe $N \geq 1$ tal que $a_{N+1} = 0$

Pela condição do algoritmo o resto das divisões é uma sequência de inteiros decrescentes e não negativa

Assim, pelo Princípio da Boa Ordenação em algum momento essa sequência deve atingir o menor inteiro não negativo que é o 0.

II. $a_N = mdc(a, b)$

Quando o resto é 0 temos o seguinte :

$a_{N-1} = a_N \cdot q_N \to a_{N-1} \mid a_N$

$a_{N-2} = a_{N-1} \cdot q_{N-1} + a_N$, como a_N divide ambos os termos ele também divide a_{N-2}

Aplicando o mesmo processo cheagamos que $a_N \mid a$ e $a_N \mid b$

Além disso, seja d um divisor comum qualquer de a e b, temos que :

$a_0 = a_1 q_1 + a_2 \Leftrightarrow a_2 = a_0 - a_1 q_1$, como $d \mid a_0$ e $d \mid a_1 q_1$,logo d divide a diferença entre eles.

Descendo por todas as equações chegamos que d divide todos os restos $a_2, a_3, \ldots, a_n$

Se todo divisor comum de a e b também divide a_n, então $a_n \geq$ que qualquer outro divisor comum

Portanto $mdc(a, b) = a_n$

3.4. (M.d.c. e combinação linear). Usando a notação do exercício 3.3, mostre que a_n pode ser escrito na forma $ax + by$ com x e y inteiros, para cada $n \geq 0$ e $\leq N$.

Seja $a = a_0$ e $b = a_1$, $a_n = ax_n + by_n$

para $n = 0$ temos :

$a_0 = a = a(1) + b(0)$, onde $x_0 = 1, y_0 = 0$

para $n = 1$ temos :

$a_1 = b = a(0) + b(1)$, onde $x_0 = 0, y_0 = 1$

Suponhamos que essa propriedade seja válida para cada n com $0 \leq n \leq N$

Daí,

$$
\begin{aligned}
a_{N-1} a_{N-1} \cdot q_{N-1} + a_N \to a_N &= a_{N-2} - a_{N-1} \cdot q_{N-1} \\
a_N &= (a \cdot x_{N-2} + b \cdot y_{N-2}) - (a \cdot x_{N-1} + b \cdot y_{N-1}) \cdot q_{N-1} \\
a_N &= a(x_{N-2} - x_{N-1} \cdot q_{N-1}) + b(y_{N-2} - y_{N-1} \cdot q_{N-1}) \\
&= a(x_N) + b(y_N)
\end{aligned}
$$

Logo, pelo Princípio da Indução Matemática a afirmação é válida para cada n com $0 \leq n \leq N$

3.5. (Calculando m.d.c. I). Use o procedimento descrito nos Exercícios 3.3 e 3.4 para encontrar $m.d.c.(a, b)$ e resolver $ax + by = m.d.c.(a, b)$ em cada um dos seguintes casos:

(i) $a = 6188, b = 4709$

$$\begin{aligned} 6188 &= (1) \cdot 4709 + 1479 \\ 4709 &= (3) \cdot 1479 + 272 \\ 1479 &= (5) \cdot 272 + 119 \\ 272 &= (2) \cdot 119 + 34 \\ 119 &= (3) \cdot 34 + 17 \\ 34 &= (2) \cdot 17 + 0 \end{aligned} \qquad \begin{aligned} 17 &= 119 + (-3) \cdot 34 \\ 17 &= (-3) \cdot 272 + (7) \cdot 119 \\ 17 &= (7) \cdot 1479 + (-38) \cdot 272 \\ 17 &= (-38) \cdot 4709 + (121) \cdot 1479 \\ 17 &= (121) \cdot 6188 + (-159) \cdot 4709 \end{aligned}$$

$\boxed{x = 121, y = -159}$

(ii) $a = 81719, b = 52003$

$$\begin{aligned} 81719 &= (1) \cdot 52003 + 29716 \\ 52003 &= (1) \cdot 29716 + 22287 \\ 29716 &= (1) \cdot 22287 + 7429 \\ 22287 &= (3) \cdot 7429 + 0 \end{aligned} \qquad \begin{aligned} 7429 &= (-1) \cdot 22287 + (1) \cdot 29716 \\ 7429 &= (-1) \cdot 52003 + (2) \cdot 29716 \\ 7429 &= (2) \cdot 29716 + (-3) \cdot 52003 \end{aligned}$$

$\boxed{x = 2, y = -3}$

(iii) $a = 33649, b = 30107$

$$\begin{aligned} 33649 &= (1) \cdot 30107 + 3542 \\ 30107 &= (8) \cdot 3542 + 1771 \\ 3542 &= (2) \cdot 1771 + 0 \end{aligned} \qquad \begin{aligned} 1771 &= 30107 + (-8) \cdot 3542 \\ 1771 &= (-8) \cdot 33649 + (9) \cdot 30107 \end{aligned}$$

$\boxed{x = 8, y = -9}$

3.6. (Homogeneidade). Se $a, b, \ldots, c$ e m são inteiros e $m > 0$, mostre que :

$m.d.c.(ma, mb, \ldots, mc) = m \cdot m.d.c.(a, b, \ldots, c)$.

Seja $mdc(a, b, \ldots, c) = ax + by + \ldots + cz$

Neste caso,

$mdc(ma, mb, \ldots, mc) = max + mby + \ldots + mcz$

$= m \cdot (ax + by + \ldots cz)$

$= m \cdot mdc(a, b, \ldots, c)$

3.7. (Representação canônica de números racionais). Prove que cada número racional pode ser escrito de maneira única como $\frac{m}{n}$ com $m.d.c.(m, n) = 1$ e $n > 0$.

Suponha que um número racional q tenha duas representações

$q = \frac{m_1}{n_1} = \frac{m_2}{n_2}$, onde $mdc(m_1, n_1) = 1, n_1 > 0$ e $mdc(m_2, n_2) = 1, n_2 > 0$

Assim, $m_1 n_2 = m_2 n_1$

Como o $mdc(m_1, n_1) = 1$ então n_1 deve dividir n_2 e de forma análoga n_2 deve dividir n_1

Logo, $n_1 = n_2$ pois $n_1 \mid n_2$ e $n_2 \mid n_1$

$n_1 = n_2 \Rightarrow m_1 = m_2$

Como $m_1 = m_2$ e $n_1 e n_2$ as representações são identicas e únicas.

3.8. (Mínimo múltiplo comum). Dados a e b dois inteiros positivos não-nulos, mostre que na igualdade $ab = dm$ vale que d é o m.d.c. de a e b se, e somente se, m é o m.m.c. de a e b (i.e., m é um inteiro ≥ 0, a divide m e b divide m, e para cada inteiro $m' \geq 0$ tal que a divide m' e b divide m', vale que m divide m').