Revista da Olimpíada - IME - UFG, nº 12, outubro de 2017. 58-71

MDC e MMC

R. Garcia

Resumo. Neste trabalho são analisadas as propriedades básicas do mínimo múltiplo comum e do máximo divisor comum e as aplicamos a alguns problemas elementares.

Introdução

Neste artigo temos como objetivo descrever algumas propriedades básicas sobre operações elementares de números inteiros, em especial as propriedades do mínimo múltiplo comum (mmc) e do máximo divisor comum (mdc). As definições de mdc e mmc apoiam-se no Teorema Fundamental da Aritmética, isto é, todo número inteiro pode ser escrito de maneira única como produto de números primos, i.e., um número natural se decompõe em fatores de números primos.

Por exemplo,

$$\begin{array}{ll} 2016 = 2^5 \times 3^2 \times 7, & 2019 = 3 \times 673 \\ 2017 = 1 \times 2017, & 2020 = 2^2 \times 5 \times 101 \\ 2018 = 2 \times 1009, & \ldots \\ & 2048 = 2^{11}. \end{array}$$

Por outro lado, escrever um número natural como soma de primos não temos unicidade e se exigirmos uma quantidade mínima de parcelas de primos é um problema super difícil, veja por exemplo a conjectura formula em 1742 por C. Golbach (*"todo número par maior do que 2 é a soma de dois números primos"*). Esta conjectura ainda não foi resolvida.

Por exemplo,

$$2016 = 2003 + 13 = 1019 + 997 = 1033 + 983 \text{ e } 2017 = 3 + 11 + 2003.$$

Propriedades básicas

Nesta seção iremos abordar as propriedades aritméticas e algébricas dos conceitos de mínimo múltiplo comum e máximo divisor comum. Estes conceitos já estavam presentes nos livros Elementos de Euclides (séc III a.C.). Veja [11, págs. 102 e 103]. Estes conceitos são importantes na teoria das proporções, semelhanças, comensurabilidade de grandezas, sincronismo de eventos, etc. Provavelmente, o primeiro contato com estes conceitos, abordados nos livros didáticos, seja na adição de frações e simplificação de números racionais. Contudo, para somar frações podemos adotar a definição $\frac{a}{b} + \frac{c}{d} = \frac{ad}{bd} + \frac{bc}{bd} = \frac{ad+bc}{bd}$ e evitar o uso de mmc em situações concretas. O mais importante é o conceito de soma e não as possíveis tecnicalidades presentes no cálculo da forma reduzida da fração. A fatoração de números inteiros em fatores primos é um tema muito relevante e com aplicações práticas, em especial na criptografia e transmissão de dados. Veja [15].

Definição 1. *Dados dois números naturais a e b, o mínimo múltiplo comum entre a e b é o menor inteiro positivo que é múltiplo de a e b simultaneamente. Este número será denotado por $mmc(a, b)$ e também denotaremos por $a \vee b$.*

Definição 2. *Dados dois números naturais a e b, o máximo divisor comum entre a e b é o maior inteiro positivo que divide a e b simultaneamente. Este número será denotado por $mdc(a, b)$ e também denotaremos por $a \wedge b$.*

Exemplo 1. *Temos que:*

$$\begin{aligned}
mdc(5, 15) &= 5 \wedge 15 = 5, \\
mmc(10, 30) &= 10 \vee 30 = 30, \\
mmc(2016, 2020) &= 2016 \vee 2020 = 4, \\
mmc(256, 144) &= 256 \vee 144 = 2304 = (2^8)(3^2), \\
mdc(144, 256) &= 144 \wedge 256 = 16 = 2^4 \quad e \\
mmc(2016, 2020) &= 2016 \vee 2020 \\
&= (2)^5(3)^2(7) \vee (2)^2(5)(101) \\
&= (2)^5(3)^2(5)(7)(101) = 1018080.
\end{aligned}$$

Definição 3. *Uma operação nos naturais é uma função* $S : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$.

Figura 1.1: Representação do conceito de função (operação) entre dois números naturais.

Os exemplos mais evidentes de operações são a soma $S(a,b) = a+b$ e o produto $P(a,b) = a \times b$. Também $\text{mmc}(a,b)$ e $\text{mdc}(a,b)$ são operações.

Em geral, as operações cumprem propriedades adicionais em relação as operações de produto e soma.

Embora o conceito de função seja simples e vital, costuma ser fonte de problemas no seu correto entendimento. Diremos apenas que função é uma máquina determinística, tem a entrada (domínio) a saída (contradomínio) e o processamento dos dados da entrada (máquina determinística que não pode cometer erros ou fazer interpretações dos dados) produzindo o produto final.

Proposição 1. *As operações* $\wedge$ *e* $\vee$ *possuem as propriedades: associativa, comutativa e idempotência. Além disso, a operação* $\vee$ *possui a propriedade do elemento neutro e a operação* $\wedge$ *possui a propriedade* $mdc(a,1) = 1$. *Isto é,*

i) $(a \vee b) \vee c = a \vee (b \vee c)$, $a \vee b = b \vee a$.

ii) $(a \wedge b) \wedge c = a \wedge (b \wedge c)$, $a \wedge b = b \wedge a$.

iii) $a \vee 1 = a$ *e* $a \wedge 1 = 1$.

iv) $a \wedge a = a$ *e* $a \vee a = a$.

v) Se a *e* b *são números primos entre si, isto é,* $a \wedge b = 1$, *então* $a \vee b = ab$.

vi) $a \wedge b$ *divide* $a \vee b$, *isto é,* $a \vee b = k(a \wedge b)$.

Demonstração. Exercício. □

Proposição 2. *Temos que* $ab = mdc(a,b) \times mmc(a,b) = (a \vee b) \times (a \wedge b)$.

Demonstração. Sejam $a = p_1^{k_1}p_2^{k_2}\dots p_n^{k_n}$ e $b = p_1^{\ell_1}p_2^{\ell_2}\dots p_n^{\ell_n}$ as decomposições (fatorações) de a e b em fatores primos. Nas decomposições acima $k_i \geq 0$, $\ell_i \geq 0$ e $p_k^0 = 1$.

Temos que $\text{mmc}(a,b) = p_1^{r_1}p_2^{r_2}\dots p_n^{r_n}$ e $\text{mdc}(a,b) = p_1^{s_1}p_2^{s_2}\dots p_n^{s_n}$ onde $r_i = \max\{k_i, \ell_i\}$ e $s_i = \min\{k_i, \ell_i\}$. Assim obtemos $ab = \text{mdc}(a,b)\times \text{mmc}(a,b)$. □

Sejam $L = a_1 \vee a_2 \vee \dots \vee a_n = \text{mmc}(a_1, \dots a_n)$ e $D = a_1 \wedge a_2 \wedge \dots \wedge a_n = \text{mdc}(a_1, \dots a_n)$.

Considere os quocientes definidos por $q_i D = a_i$ e $q_i' a_i = L$.

A seguinte proposição foi obtida em [16].

Proposição 3. *Sejam $a_1, \dots a_n \in \mathbb{N}$ e considere $L = a_1 \vee a_2 \vee \dots \vee a_n = mmc(a_1, \dots a_n)$, $D = a_1 \wedge a_2 \wedge \dots \wedge a_n = mdc(a_1, \dots a_n)$ e os quocientes definidos por $q_i D = a_i$ e $q_i' a_i = L$. Então*

$$mdc(q_1, \dots, q_n) = 1 \text{ e } mdc(q_1', \dots, q_n') = 1.$$

Além disso, temos que

$$q_1 q_1' = \dots = q_n q_n' = L/D \text{ e } mmc(q_1, \dots q_n) = mmc(q_1', \dots, q_n') = L/D.$$

Demonstração. Pela construção das sequências q_i e q_i' temos

$$\text{mdc}(q_1, \dots, q_n) = 1 \quad \text{e} \quad \text{mdc}(q_1', \dots, q_n') = 1.$$

Multiplicando $q_i D = a_i$ e $q_i' a_i = L$ obtemos $q_i D q_i' a_i = a_i L$ e portanto $q_i q_i' = L/D$. □

Exercício 1. *Encontre três números naturais a, b e c tais que*

$$mdc(a,b,c) = 10,\ mmc(a,b,c) = 900 \quad e\ que \quad a+b+c = 250.$$

Proposição 3. *Seja $s : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ uma função satisfazendo as propriedades (associativa, comutativa, elemento neutro, idempotência) descritas na Proposição 1 e $s(a,b) = ab$ quando a e b são números primos entre si.*

Então $s(a,b) = mmc(a,b)$ para todo $(a,b) \in \mathbb{N} \times \mathbb{N}$.

Demonstração. Considere que $\text{mdc}(a,b) = r > 1$. Logo temos que $a = a_1 r$ e $b = b_1 r$ com $\text{mdc}(a_1, b_1) = 1$.

Portanto, é suficiente mostrar que $s(a,b) = \text{mmc}(a,b) = a_1 b_1 r$.

Suponha inicialmente que r é primo.

Usando as propriedades (associativa $s(s(x,y),z) = s(x,s(y,z))$, comutativa $s(x,y) = s(y,x)$, idempotência $s(x,x) = x$ e que $s(a_1,b_1) = a_1 b_1$) obtemos

$$\begin{aligned} s(a,b) &= s(a_1 r, b_1 r) = s(s(a_1,r), s(b_1,r)) = s(s(a_1,b_1), s(r,r)) \\ &= s(a_1 b_1, r) = a_1 b_1 r = \text{mmc}(a,b). \end{aligned}$$

Aqui usamos que $\text{mdc}(a_1 b_1, r) = 1, s(a_1, r) = a_1 r$ e $s(b_1, r) = b_1 r$. O caso geral segue por indução finita no número de fatores primos de r. Confiamos ao leitor fazer os detalhes. □

Exercício 2. *Na Proposição 3, substituir a hipótese $s(a,b) = ab$ quando a e b são números primos entre si por $s(a,b) = ab$ quando a e b forem primos e concluir que $s = mmc$.*

Algumas Propriedades curiosas

Esta seção foi inspirada no artigo [1] no qual é apresentado a identidade,

$$24 + 36 = \text{mmc}(24,36) - \text{mdc}(24,36),$$

observando que $(24,36) = (2 \times 12, 3 \times 12) = (2k, 3k)$.

Esta igualdade expressa uma relação linear entre mdc e mmc de dois números naturais.

Teorema 1. *Sejam a, b números naturais e p_1, p_2 números primos distintos. Temos que*

$$a + b = mmc(a,b) + (p_1 + p_2 - p_1 p_2) mdc(a,b) \tag{1.1}$$

se, e somente se, $(a,b) = (p_1 k, p_2 k)$, com $k \in \mathbb{N}$.

Demonstração. Temos que

$$a = \text{mdc}(a,b) a_1, \; b = \text{mdc}(a,b) b_1 \quad \text{com } \text{mdc}(a_1, b_1) = 1.$$

Logo $\text{mmc}(a,b) = \text{mdc}(a,b)\,\text{mmc}(a_1,b_1) = \text{mdc}(a,b) a_1 b_1$.

Portanto, da equação (1.1) temos que

$$\begin{aligned} a+b =& (a_1+b_1)\text{mdc}(a,b) = \text{mmc}(a,b) + (p_1+p_2-p_1p_2)\,\text{mdc}(a,b) \\ =& (a_1+b_1)\,\text{mdc}(a,b) \\ =& \text{mdc}(a,b)\,a_1b_1 + (p_1+p_2-p_1p_2)\,\text{mdc}(a,b). \end{aligned}$$

Assim, obtemos

$$a_1+b_1 = a_1b_1 + p_1 + p_2 - p_1p_2.$$

Portanto, $a_1 = p_1$ e $b_1 = p_2$ é uma solução da equação acima.
Reciprocamente, suponha $a = p_1k$ e $b = p_2k$. Logo

$$\text{mmc}(a,b) = p_1p_2k \quad \text{e} \quad \text{mdc}(a,b) = k.$$

Portanto $a+b = (p_1+p_2)k = p_1p_2k+(p_1+p_2-p_1p_2)k = \text{mmc}(a,b)+(p_1+p_2-p_1p_2)\text{mdc}(a,b)$. □

Observação 1. *Para obter a equação* (1.1) *supomos que* $(a,b) = (p_1k, p_2k)$ *e resolvemos a equação diofantina linear* $a+b = x\ mmc(a,b)+y\ mdc(a,b)$ *nas variáveis* x *e* y *para vários valores de* k *obtendo a solução geral* $x = t, y = p_1+p_2-tp_1p_2,\ t \in \mathbb{N}$.

Teorema 2. *Sejam* a, b *números naturais e* p_1, p_2 *números primos distintos. números primos distintos. Temos que,*

$$a-b = mmc(a,b) + (p_1-p_2-p_1p_2)\,mdc(a,b) \tag{1.2}$$

se, e somente se, $(a,b) = (p_1k, p_2k)$, *com* $k \in \mathbb{N}$.

Demonstração. Exercício. Proceda como na prova do Teorema 1. □

Teorema 3. *Dados* a b *e* c *números naturais distintos. Temos que,*

$$a+b+c = mmc(a,b,c) - 20mdc(a,b,c) \tag{1.3}$$

se, e somente se, $(a,b,c) = (2k, 3k, 5k)$, *com* $k \in \mathbb{N}$.

Demonstração. Temos que $a = \text{mdc}(a,b,c)a_1,\ b = \text{mdc}(a,b,c)b_1$ e $c = \text{mdc}(a,b,c)c_1$ com $\text{mdc}(a_1,b_1,c_1) = 1$.

Logo $\text{mmc}(a,b,c) = \text{mdc}(a,b,c)\text{mmc}(a_1,b_1,c1) = \text{mdc}(a,b,c)\,a_1b_1c_1$.

Portanto, da equação (1.3) temos que

$$\begin{aligned} a+b+c =& (a_1+b_1+c_1)\text{mdc}(a,b,c) = \text{mmc}(a,b,c) - 20\text{mdc}(a,b,c) \\ =& (a_1+b_1+c_1)\text{mdc}(a,b,c) \\ =& \text{mdc}(a,b,c)\, a_1b_1c_1 - 20\text{mdc}(a,b,c). \end{aligned}$$

Assim obtemos,

$$a_1+b_1+c_1 = a_1b_1c_1 - 20.$$

Portanto, $(a_1,b_1,c_1) = (2,3,5)$ é uma solução da equação acima.
Reciprocamente, suponha $a = 2k$, $b = 3k$ e $c = 5k$. Logo

$$\text{mmc}(a,b,c) = 30k \text{ e } \text{mdc}(a,b,c) = k.$$

Portanto, $a+b+c = 10k = 30k-20k = \text{mmc}(a,b,c) - 20\,\text{mdc}(a,b,c)$. □

Teorema 4. *Dados a, b e c números naturais distintos e p_1, p_2 e p_3 números primos distintos. Temos que,*

$$a+b+c = mmc(a,b,c) - (p_1+p_2+p_3-p_1p_2p_3)mdc(a,b,c) \qquad (1.4)$$

se, e somente se, $(a,b,c) = (kp_1, kp_2, kp_3)$, com $k \in \mathbb{N}$.

Demonstração. Exercício. □

Algoritmo de Euclides

Dados dois números inteiros positivos $a < b$, considere as sequências definidas por $a_1 = a$, $b_1 = b$ e $a_{i+1} = \min\{b_i - a_i, a_i\}$ e $b_{i+1} = \max\{b_i - a_i, a_i\}$. Para todo $i > 1$, temos que a_i e b_i dividem a e b.

Então $\text{mdc}(a,b) = a_k = b_k$, onde k é o primeiro inteiro tal que $a_k = b_k$.

Exemplo 2. *O cálculo de $mdc(60,24)$ produz a seguinte sequência*

$$(24,60) \to (24,36) \to (12,24) \to (12,12)$$

e portanto $mdc(60,24) = 12$. Diretamente obtemos $mmc(24,60) = 24 \times 60/12 = 120$.

Dados três números inteiros positivos $a < b < c$ podemos usar o algoritmo anterior e a propriedade de associativa para calcular $\text{mdc}(a, b, c)$. De fato, temos

$$\text{mdc}(a, b, c) = (a \wedge b) \wedge c = (a \wedge b) \wedge (b \wedge c).$$

Exemplo 3. *Para* $mdc(8, 36, 144) = 4$ *temos as seguintes sequências:*
$(8, 36) \to (8, 28) \to (8, 20) \to (8, 12) \to (4, 8) \to (4, 4)$,
$(36, 144) \to (36, 108) \to (36, 72) \to (36, 36)$ *e*
$(4, 36) \to (4, 32) \to \cdots \to (4, 4)$.

Lema 1. *Seja* $a < b$ *e* $b = aq_1 + r_1$. *Então* $mdc(a, b) = mdc(r_1, a)$.

Demonstração. Exercício. □

Exercício 3. *Mostre que*

$$\min\{a, b\} = \frac{1}{2}(a + b - |a - b|) \text{ e } \max\{a, b\} = \frac{1}{2}(a + b + |a - b|).$$

Outra versão do algoritmo de Euclides é usualmente definido pelo seguinte procedimento. A seguir iremos supor $a < b$. Veja também [4] e [8] para informações adicionais sobre o assunto.

Relembramos o resultado clássico e importante, conhecido como lema de Bézout. Matemático francês Étienne Bézout (1730-1783).

Lema 2 (Bézout)**.** *Sejam* a *e* b *números naturais tais que* $mdc(a, b) = d$. *Então existem números inteiros* x *e* y *tais que* $ax + by = d$.

Demonstração. Veja https://en.wikipedia.org/wiki/Bézout's_identity. □

Exercício 4. *Mostre que a equação* $9x + 6y = 2$ *não possui solução* $(x, y) \in \mathbb{Z}^2$. *Mostre que as soluções da equação* $9x + 6y = 15$ *são dadas por* $x = 1 + 2k$ *e* $y = 1 - 3k$.

Definimos recursivamente,

$$r_0 = a, \;\; r_1 = b, \; \ldots, \; r_{i+1} = r_{i-1} - q_i r_i \;\text{ e }\; 0 \leq r_{i+1} < |r_i|.$$

Temos que $\text{mdc}(a, b) = r_k$, o último coeficiente não nulo da sequência r_i.

O algoritmo de Euclides estendido é definido pela sequência dupla

$$\begin{aligned} r_0 &= a \qquad r_1 = b \\ s_0 &= 1 \qquad s_1 = 0 \\ t_0 &= 0 \qquad t_1 = 1 \\ r_{i+1} &= r_{i-1} - q_i r_i \\ s_{i+1} &= s_{i-1} - q_i s_i \\ t_{i+1} &= t_{i-1} - q_i t_i \end{aligned}$$

Temos que $\text{mdc}(a,b) = r_k$, onde $r_{k+1} = 0$ e os coeficientes (s_k, t_k), chamados coeficientes de Bézout, tais que $\text{mdc}(a,b) = r_k = as_k + bt_k$ definem uma solução particular da equação diofantina $ax + by = \text{mdc}(a,b)$. Veja [2] e [5] para exemplos práticos no cálculo dos coeficientes de Bézout.

Exemplo 4. *Na tabela abaixo mostramos o procedimento dos cálculos de* $mdc(192, 72) = 24$ *e* $\boxed{-1} \times 192 + \boxed{3} \times 72 = 24$.

j	q_{j-1}	r_j	s_j	t_j
0		192	1	0
1		72	0	1
2	2	$192 - 2 \times 72 = 48$	$1 - 2 \times 0 = 1$	$0 - 2 \times 1 = -2$
3	1	$72 - 1 \times 48 = 24$	$0 - 1 \times 1 = \boxed{-1}$	$1 - 1 \times (-2) = \boxed{3}$
4	2	$48 - 2 \times 24 = 0$	$1 - 2 \times (-1) = 3$	$-2 - 2 \times 3 = -8$

Observação 2. *Em [12] é demonstrado que o algoritmo de Euclides estendido para calcular o mdc produz a solução da equação diofantina* $ax + by = mdc(a,b)$ *mais próxima da origem. De fato a solução* (x_0, y_0) *da equação* $ax + by = mdc(a,b)$. *mais próxima da origem é a única solução contida na região delimitda pelo círculo de raio* $\sqrt{a^2 + b^2}/(2mdc(a,b))$ *e centro na origem. Por exemplo, na equação* $13x + 2y = 1$ *o algoritmo de Euclides nos conduz a* $13 = 6 \times 2 + 1$ *e portanto* $1 \times 13 + (-6) \times 2 = 1$ *e temos que* $(1, -6)$ *é a solução da equação diofantina mais próxima da origem. A segunda mais próxima é* $(-1, 7)$. *A solução geral é* $x = 1 - 2t$, $y = -6 + 13t$.

Dinâmica simples

Considere a função $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ definida por

$$f(a, b) = (a \vee b, a \wedge b).$$

A órbita positiva $p_0 = (a_0, b_0)$ é o conjunto

$$\mathrm{Orb}^+(p_0) = \{f^n(p_0) : n \in \mathbb{N} \cup \{0\}\}.$$

A órbita negativa de um ponto p_0 é o conjunto

$$\mathrm{Orb}^-(p_0) = \{p \in \mathbb{N} \times \mathbb{N} : f^n(p) = p_0 : n \in \mathbb{N} \cup \{0\}\}.$$

Proposição 4. *Toda órbita positiva possui no máximo dois elementos e f definida acima possui infinitos pontos fixos.*

Toda órbita negativa é vazia ou possui no máximo dois elementos.

Demonstração. Seja $(a_1, b_1) = f(a_0, b_0)$. Então $f(a_1, b_1) = (a_1, b_1)$ pois $b_1 = a_0 \wedge b_0$ divide $a_1 = a_0 \vee b_0$. A demonstração da afirmação sobre a órbita negativa fica a cargo do leitor. □

Problema 1. *Encontre uma função $F : \mathbb{R}^2 \to \mathbb{R}^2$ a mais "simples" possível tal que F restrita ao conjunto $\mathbb{N} \times \mathbb{N}$ coincide com f, isto é $F|_{\mathbb{N}\times\mathbb{N}} = f$.*

A seguir consideramos a função $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ definida por

$$\begin{aligned} g(a, b) &= (a \vee b - 1, a \wedge b + 1) \\ &= (\mathrm{mmc}(a, b) - 1, \mathrm{mdc}(a, b) + 1). \end{aligned} \tag{1.5}$$

Exemplo 5. *A órbita positiva de $p_0 = (4, 3)$ é*

$$\begin{aligned} Orb^+(p_0) &= \{g^n(p_0) : n \in \mathbb{N}\} \\ &= \{(4, 3), (11, 2), (21, 2), (41, 2), (81, 2), (161, 2), \ldots, (\ldots, 2), \ldots\}. \end{aligned}$$

A órbita negativa de $p_0 = (3, 4)$ é vazia e a órbita negativa de $p_0 = (4, 3)$ também é vazia.

A órbita positiva de $p_0 = (8, 6)$ é $\{(8, 6), (23, 2), (45, 2), (89, 2), \ldots, \}$.

A órbita positiva de $p_0 = (2, 2)$ é $\{(2, 2), (1, 3), (2, 2)\}$. E portanto p_0 é um ponto de período 2. Sua órbita negativa é $\{(2, 2), (1, 3), (3, 1)\}$.

Também $q_0 = (3, 3)$ é um ponto de período 2 e sua órbita positiva é $\{(3, 3), (2, 4), (3, 3)\}$.

Exercício 5. *Encontre todas órbitas $p_n = g^n(p_1)$ do tipo $p_n = (a_n, 2)$ para todo $n \in \mathbb{N}$. Calcule explicitamente a órbita de $p_1 = (11, 2)$. É necessário resolver a equação a diferença $a_{n+1} = 2a_n - 1,\ a_1 = 11$.*

Proposição 5. *A função g definida pela equação (1.5) não possui pontos fixos. Toda órbita negativa de um ponto $p_0 = (a, b)$ por g é finita ou vazia.*

Demonstração. Suponha $a \geq b$. Da condição $g(a, b) = (a, b)$ obtemos $a \vee b = a + 1$ e $a \wedge b = b - 1$. Logo pela Proposição 2 temos que $ab = (a + 1)(b - 1)$ e portanto $a + b = 1$ com $a, b \in \mathbb{N}$. Esta equação linear não possui solução nos naturais. A demonstração da afirmação sobre a órbita negativa fica a cargo do leitor. □

Exercício 6. *No exemplo 5 acima temos que $p_0 = (2, 2)$ e $q_0 = (3, 3)$ são pontos periódicos de perído 2.*

i) Determine todos os pontos periódicos de período 2 da função g.

ii) Determine (se existir!) pontos periódicos de período $n > 2$ da função g.

Exercício 7. *Calcule as órbitas positivas dos pontos $(6, 6)$ e $(7, 7)$.*

Calcule a órbita negativa dos pontos $(694, 2)$ e $(109, 5)$.

Observação 3. *Para uma introdução ao estudo de dinâmica discreta veja [6] e [7].*

Exercício 8. *Encontre uma prova do lema de Bézout usando ideias de dinâmica discreta.*

Problemas envolvendo mmc e mdc

Esta seção foi desenvolvida com base em reminescências de problemas clássicos envolvendo mmc e cálculos rápidos de aritmética, veja [14].

Problema 2. *Calcule todos os números inteiros positivos que quando divididos por 2,3,4,5 e 6 tenham resto 1 e que sejam múltiplos de 7.*

Solução: Primeiro observamos que $\text{mmc}(2, 3, 4, 5, 6) = 60$ e portanto todos os números da forma $60n+1$ cumprem a primeira parte da questão. Para determinar todas as soluções devemos resolver a equação $60n+1 =$

$7m$ com m e n números inteiros positivos. Observamos que os números da forma $m = 60t + 43$ e $n = 7t + 5$ com $t \in \mathbb{N}$ cumprem o solicitado, resolvendo a equação diofantina. De fato, $60(7t + 5) + 1 = 7(43 + 60t)$. O menor número que cumpre esta propriedade é 301 e todos os números são da forma $420t + 301 = 7(60t + 43)$.

Problema 3. *Calcule todos os números inteiros positivos que quando divididos por 2,3,4,5 e 6 tenha resto 1 e que sejam múltiplos de 7 e 11.*

Solução: Agora observamos que devemos resolver o sistema de equações

$$\begin{cases} 60n + 1 = 7m \\ 60n + 1 = 11p. \end{cases}$$

Consideramos a equação $420t + 301 = 11p$ obtida na solução do problema 2. A solução geral da equação diofantina acima é

$$t = 11s - 2,\ p = 420s - 49,\ \text{com}\ s \in \mathbb{N}.$$

Logo a solução $11(420s-49)$ ou, equivalentemente, $4620(s-1)+4081 = 7.11(60(s-1)+53)$. O primeiro inteiro que cumpre as condições do problema é $4081 = 7 \times 11 \times 53$.

A solução do sistema é $n = 77s+68,\ m = 660s+583,\ p = 420s+371$ e confiamos ao leitor a tarefa de verificar a exatidão da afirmação.

Exercício 9. *Encontre números naturais a e b tais que*

$$mmc(a, b) = 2016 \ \ e \ \ mdc(a, b) = 14.$$

Exercício 10. *Considere a sequência de Fibonacci $F_1 = 1$, $F_2 = 1$, $F_3 = 2$, $F_4 = 3$, $F_5 = 5$, $F_6 = 8, \ldots$, $F_{n+1} = F_n + F_{n-1}$, ... Mostre que $mdc(F_m, F_n) = F_{mdc(m,n)}$. Em particular $mdc(F_n, F_{n+1}) = 1$. Veja [9] para mais fatos sobre mmc na sequência de Fibonacci.*

Exercício 11. *Considere a sequência definida pela recorrência $u_n = u_{n-1} + 3u_{n-2}$, com $u_1 = 1$ e $u_2 = 1$. Assim, por exemplo, $u_3 = 4$, $u_4 = 7$, $u_5 = 19$, $u_6 = 40$, $u_7 = 97$, $u_8 = 217$, $u_9 = 508, \ldots$. Mostre que $mdc(u_n, u_m) = u_{mdc(m,n)}$. Veja [13].*

Conclusão

Neste artigo revisamos os conceitos de mínimo múltiplo comum e relembramos as propriedades básicas desta operação (comutativa, associativa, elemento neutro e idempotência). Uma questão natural é descrever todas as funções $s : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ que cumprem tais propriedades.

Por exemplo, além da função mmc a função $s(m, n) = \max\{m, n\}$ cumpre as 4 propriedades descritas acima.

A generalização natural e importante de mdc e mmc é no anel de polinômios $\mathbb{R}[x]$ e dos inteiros de Gauss $\mathbb{Z}[i]$. Para uma introdução a estes tópicos veja por exemplo [10]. Estes conceitos se estendem a outras estruturas algébricas, em especial na teoria nos anéis fatoriais.

Agradecimento

O autor agradece ao Prof. José Hilário (IME/UFG) pela leitura crítica e ao parecerista pelos comentários e sugestões que foram incorporados na versão final.

Bibliografia

[1] J. Austin, *A Curious Result for GCDs and LCMs*. Mathematics Magazine, Vol. 89, No. 3 (June 2016), p. 190.

[2] J. Paulo Q. Carneiro, *Dispositivo prático para expressar o mdc de dois números como combinação linear deles*. Revista do Professor de Matemática, Vol. 37, SBM.

[3] J. Barnes, Nice Numbers, Birkhäuser, (2016).

[4] J. B. Pitombeira de Carvalho, *Euclides, Fibonacci e Lamé*, Revista do Professor de Matemática, Vol. 24, SBM.

[5] J. B. Pitombeira de Carvalho, *Uma representação matricial para o algoritmo de Euclides*, Revista do Professor de Matemática, Vol. 70, SBM.

[6] R. Devaney, Chaos, fractals and dynamics. Computer experiments in mathematics. Science Television, New York; distributed by the American Mathematical Society, Providence, RI, 1989.

[7] R. Devaney, A first course in chaotic dynamical systems. Theory and experiment. Addison-Wesley Publishing Company, m, Reading, MA, 1992.

[8] F. Dutenhefner e L. Cadar, *Encontros de Aritmética*, PIC, Programa de Iniciação Cientifica da OBMEP, IMPA, (2915).

[9] M. Farrokhi D. G., *Some Remarks on the Equation $F_n = kF_m$ in Fibonacci Numbers,* Journal of Integer Sequences, Vol. 10 (2007), Article 07.5.7

[10] S. Lang, Algebra, Graduate Texts in Mathematics, 221, Springer Verlag, (2002).

[11] Uta C. Merzbach and Carl B. Boyer, A History of Mathematics, Third edition, John Wiley & Sons, Inc. (2011)

[12] Rankin, *The Euclidean algorithm and the linear Diophantine equation $ax + by = gcd(a, b)$.* Amer. Math. Monthly 120 (2013), no. 6, 562-564.

[13] N. Robbins , *On the infinitude of primers of the form $3k + 1$.* Fibonacci Quart. 43 (2005), no. 1, 29-30.

[14] T. O'Conor Sloane, Rapid Arithmetic, D. Van Nostrand Company, New York, (1922), wwww.forgottenbooks.com

[15] M. Viana, *A criptografia moderna não existiria sem os números primos*, Folha de S. Paulo (29 de setembro de 2017), http://www1.folha.uol.com.br/colunas/marceloviana/2017/09/1922755-a-criptografia-moderna-nao-existiria-sem-os-numeros-primos.shtml

[16] B. F. Yanney, Notes on Greatest Common Divisor and Least Common Multiple of Integers. American Mathematical Monthly, Vol. 19, No. 1 (Jan., 1912), pp. 4-6.

Autor: Ronaldo Garcia
Endereço: Universidade Federal de Goiás,
Instituto de Matemática e Estatística
e-mail: ragarcia@ufg.br