4.1 Cálculo do *mdc*: algoritmo de Euclides – parte 1

O Algoritmo de Euclides para o cálculo do *mdc* baseia-se na seguinte propriedade dos números naturais. Observamos que essa propriedade está muito bem explicada no vídeo 9. Dê uma olhada.

Propriedade: Sejam a e b números naturais com $a < b$.

(a) Se d é um divisor comum de a e b, então d também é um divisor de $b - a$.

(b) Reciprocamente, se d é um divisor de a e de $b - a$, então d é um divisor de b.

Lembre-se de que esta propriedade já foi estudada nos exercícios 20 e 27 do encontro 2. Na verdade, esta propriedade está relacionada com o fato de que a soma e a diferença de dois múltiplos de um número d ainda são múltiplos de d.

Exemplos:

- É fácil ver que 84 e 35 são múltiplos de 7. Então $84 + 35 = 119$ e $84 - 35 = 49$ são múltiplos de 7.
- O número $d = 4$ é um divisor de $a = 20$ e de $b = 48$, pois $20 = 4 \cdot 5$ e $48 = 4 \cdot 12$. Daí $d = 4$ é um divisor de $b - a = 28$, pois $b - a = (4 \cdot 12) - (4 \cdot 5) = 4 \cdot (12 - 5) = 4 \cdot 7$.
- Para entender o item (b) vamos considerar que a e $b - a$ são múltiplos de d. Como $b = a + (b - a)$ é uma soma de múltiplos de d, segue que b também é um múltiplo de d.

É importante observar que a propriedade anterior implica que os divisores comuns de a e b são iguais aos divisores comuns de a e $b-a$.

Exercício 1: Se $a = 18$ e $b = 60$ calcule os conjuntos $D(a)$, $D(b)$ e $D(b-a)$ dos divisores de a, de b e de $b-a$. Em seguida verifique que $D(a) \cap D(b) = D(a) \cap D(b-a)$.

Solução.

$$D(a) = \{1, 2, 3, 6, 9, 18\}$$

$$D(b) = \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$$

$$D(b-a) = \{1, 2, 3, 6, 7, 14, 21, 42\}$$

Calculando os divisores comuns:

$$D(a) \cap D(b) \; = \; \{1, 2, 3, 6\} \; = \; D(a) \cap D(b-a).$$

As propriedades que acabamos de verificar implicam que os divisores comuns de a e b são iguais aos divisores comuns de a e $b-a$. Em particular, o maior divisor comum de a e b é igual ao maior divisor comum de a e $b-a$. Ou seja, acabamos de verificar a seguinte propriedade.

Propriedade: Se a e b são números naturais com $a < b$, então $mdc(a, b) = mdc(a, b-a)$. (Este teorema também está demonstrado no vídeo 9.)

Como veremos logo abaixo, esta propriedade permite ir reduzindo sucessivamente o cálculo do mdc de dois números ao cálculo do mdc de números cada vez menores. E como a única conta que deve ser feita é uma subtração, este método é mais fácil de ser aplicado do que os métodos anteriores, quando tínhamos que fatorar os números dados.

Exercício 2: Calcule $mdc(18, 60)$.

Solução.

$$mdc(18, 60) = mdc(18, 60-18) = mdc(18, 42) =$$

$$mdc(18,42) = mdc(18,42-18) = mdc(18,24) =$$
$$mdc(18,24) = mdc(18,24-18) = mdc(18,6) = 6.$$

Exercício 3: Calcule $mdc(459,595)$.

Solução.

$$mdc(459,595) = mdc(459,595-459) = mdc(459,136) =$$
$$mdc(136,459) = mdc(136,459-136) = mdc(136,323) =$$
$$mdc(136,323) = mdc(136,323-136) = mdc(136,187) =$$
$$mdc(136,187) = mdc(136,187-136) = mdc(136,51) =$$
$$mdc(51,136) = mdc(51,136-51) = mdc(51,85) =$$
$$mdc(51,85) = mdc(51,85-51) = mdc(51,34) =$$
$$mdc(34,51) = mdc(34,51-34) = mdc(34,17) = 17.$$

Exercício 4: Tente calcular o $mdc(1203,3099)$ usando uma fatoração simultânea e depois calcule este mdc usando a propriedade $mdc(a,b) = mdc(a,b-a)$.

Solução. Como $1203 = 3 \cdot 401$, $3099 = 3 \cdot 1033$, 401 e 1033 são números primos, aparentemente pode ser difícil obter as fatorações destes dois números. E se alguém ainda não achar este exemplo difícil, podemos facilmente dificultar mais, propondo exemplos com números cada vez maiores até convencer de que o cálculo do mdc por meio da propriedade $mdc(a,b) = mdc(a,b-a)$ sempre permite o cálculo do mdc, enquanto que para calcular o mdc via uma fatoração simultânea precisamos descobrir divisores primos dos números dados, e isto realmente pode ser uma tarefa muito complicada. Não está convencido? Tente calcular $mdc(398\,549\,358\ ,\ 398\,549\,415)$.

Utilizando sucessivamente a igualdade $mdc(a,b) = mdc(a,b-a)$, o cálculo do mdc desejado pode ser efetuado do seguinte modo.

$$mdc(1203, 3099) = mdc(1203, 3099 - 1203) = mdc(1203, 1896) =$$
$$mdc(1203, 1896) = mdc(1203, 1896 - 1203) = mdc(1203, 693) =$$
$$mdc(693, 1203) = mdc(693, 1203 - 693) = mdc(693, 510) =$$
$$mdc(510, 693) = mdc(510, 693 - 510) = mdc(510, 183) =$$
$$mdc(183, 510) = mdc(183, 510 - 183) = mdc(183, 327) =$$
$$mdc(183, 327) = mdc(183, 327 - 183) = mdc(183, 144) =$$
$$mdc(144, 183) = mdc(144, 183 - 144) = mdc(144, 39) = 3.$$

Na próxima seção veremos que é possível acelerar o método que acabamos de exemplificar para o cálculo do mdc. Antes disso, veja que a propriedade $mdc(a, b) = mdc(a, b-a)$ permite mostrar que dois números consecutivos sempre são relativamente primos. De fato,

$$mdc(n, n + 1) = mdc(n, n + 1 - n) = mdc(n, 1) = 1.$$

Antes de ver esta propriedade como você calcularia, por exemplo, $mdc(51834, 51835)$?

4.2 Cálculo do mdc: algoritmo de Euclides–parte 2

O Algoritmo de Euclides está explicado de um modo mais adequado para os alunos do grupo G1,1 no vídeo 9 do canal picobmep no YouTube. Neste vídeo o algoritmo é apresentado e demonstrado de um modo mais informal, sem o uso excessivo de álgebra. Dependendo da turma somente a explicação dada neste vídeo pode ser suficiente. Entretanto, no vídeo 21 é apresentada uma demonstração formal e completa do Algoritmo de Euclides. Pode ser que este vídeo não seja adequado a todos os alunos do grupo G1,1. Mesmo assim fica a sugestão para os alunos interessados em aprender cada vez mais.

No que segue apresentamos uma proposta de como o estudo do algoritmo de Euclides pode ser desenvolvido em um turma de alunos do grupo G1,1.

Na seção anterior vimos que se $a < b$ então $mdc(a, b) = mdc(a, b - a)$, e também vimos que esta propriedade permite que o mdc seja calculado, uma vez que trocamos a e b por números cada vez menores. Agora veremos que este processo pode ser acelerado.

Para ficar mais claro o que será feito, vamos analisar novamente o exercício 2 da seção anterior.

$$mdc(18, 60) = mdc(18, 60 - 18) = mdc(18, 42) =$$

$$mdc(18, 42 - 18) = mdc(18, 24) = mdc(18, 24 - 18) = mdc(18, 6).$$

Neste desenvolvimento a propriedade $mdc(a, b) = mdc(a, b - a)$ foi utilizada 3 vezes consecutivas, sendo que de 60 retiramos por 3 vezes o número 18. Assim, do cálculo do $mdc(18, 60)$ chegamos no cálculo do $mdc(18, 60 - 3 \cdot 18) = mdc(18, 60 - 54) = mdc(18, 6)$. Observando bem, utilizamos a igualdade $60 - 3 \cdot 18 = 6$, ou seja, $60 = 3 \cdot 18 + 6$, que nada mais é do que o algoritmo da divisão de 60 por 18. Portanto identificamos 6 como o resto da divisão de 60 por 18 e percebemos que, neste exemplo, trocamos o cálculo do mdc entre 18 e 60 pelo cálculo do mdc entre 18 e o resto da divisão de 60 por 18.

De modo análogo, na resolução do exercício 3 passamos por

$$mdc(51, 136) = mdc(51, 136 - 51) = mdc(51, 85) =$$

$$mdc(51, 85 - 51) = mdc(51, 34)$$

onde a propriedade $mdc(a, b) = mdc(a, b-a)$ foi utilizada duas vezes consecutivas: do cálculo do $mdc(51, 136)$ chegamos em $mdc(51, 136 - 2 \cdot 51) = mdc(51, 136 - 102) = mdc(51, 34)$. Da igualdade $136 - 2 \cdot 51 = 34$ identificamos 34 como o resto da divisão de 136 por 51 e concluímos que o mdc entre 51 e 136 é igual ao mdc entre 51 e o resto da divisão de 136 por 51.

Generalizando, aplicando consecutivamente a propriedade $mdc(a, b) = mdc(a, b - a)$, podemos subtrair de b múltiplos de a até, evidentemente, ainda termos números positivos. E, como fazemos isto até obter o menor número possível, de fato, chegamos em $r = b - aq$, resto da divisão de b por a. Estas observações demonstram a seguinte propriedade, que é uma generalização do que foi feito na seção anterior e que, como veremos, acelera o cálculo do mdc.

Propriedade: Se $a < b$ são números naturais e se r é o resto da divisão de b por a, então $mdc(a, b) = mdc(a, r)$.

De modo alternativo, pelas propriedades aritméticas do resto de uma divisão, observe que se d é um divisor comum de a e b, então d é um divisor comum de a e $r = b - aq$. Assim, de fato, é possível mostrar que o conjunto dos divisores comuns de a e b é igual ao conjunto dos divisores comuns de a e $r = b - aq$, em que r é o resto da divisão de b por a. Verifique esta propriedade na solução do seguinte exercício.

Exercício 5: Se $a = 84$ e $b = 330$ calcule o resto r da divisão de b por a, calcule os conjuntos $D(a)$, $D(b)$ e $D(r)$ dos divisores de a, de b e de r, e verifique que $D(a) \cap D(b) = D(a) \cap D(r)$.

Solução. Dividindo b por a obtemos $330 = 3 \cdot 84 + 78$, de modo que $r = 78$ é o resto da divisão de b por a.

$D(a) = \{1, 2, 3, 4, 6, 7, 12, 14, 21, 28, 42, 84\}$

$D(b) = \{1, 2, 3, 5, 6, 10, 11, 15, 22, 30, 33, 55, 66, 110, 165, 330\}$

$D(r) = \{1, 2, 3, 6, 13, 26, 39, 78\}$

Calculando os divisores comuns:

$$D(a) \cap D(b) \;=\; \{1, 2, 3, 6\} \;=\; D(a) \cap D(r).$$

Daí, como o conjunto dos divisores comuns de a e b é igual ao conjunto dos divisores comuns de a e r, tomando o maior dos elementos, concluímos que $mdc(a, b) = mdc(a, r)$.

Vamos ver agora alguns exercícios que nos mostram que a propriedade que acabamos de discutir pode ser utilizada para acelerar o cálculo do mdc.

Exercício 6: Calcule $mdc(162, 372)$.

Solução.

- Dividindo 372 por 162 obtemos $372 = 2 \cdot 162 + 48$. Assim $mdc(162, 372) = mdc(162, 48)$.
- Dividindo 162 por 48 obtemos $162 = 3 \cdot 48 + 18$. Daí $mdc(48, 162) = mdc(48, 18)$.
- Dividindo 48 por 18 obtemos $48 = 2 \cdot 18 + 12$ e portanto $mdc(18, 48) = mdc(18, 12)$.
- Dividindo 18 por 12 obtemos $18 = 1 \cdot 12 + 6$ e assim $mdc(12, 18) = mdc(12, 6)$.
- Portanto $mdc(162, 372) = mdc(6, 12) = 6$.

Pode ser interessante comparar esta resolução com aquela que deveria ser feita pelo método da seção anterior, quando aplicamos apenas a propriedade $mdc(a, b) = mdc(a, b - a)$.

$$mdc(162, 372) = mdc(162, 372 - 162) = mdc(162, 210) =$$
$$mdc(162, 210) = mdc(162, 210 - 162) = mdc(162, 48) =$$
$$mdc(48, 162) = mdc(48, 168 - 48) = mdc(48, 114) =$$
$$mdc(48, 114) = mdc(48, 114 - 48) = mdc(48, 66) =$$
$$mdc(48, 66) = mdc(48, 66 - 48) = mdc(48, 18) =$$
$$mdc(18, 48) = mdc(18, 48 - 18) = mdc(18, 30) =$$
$$mdc(18, 30) = mdc(18, 30 - 18) = mdc(18, 12) =$$
$$mdc(12, 18) = mdc(12, 18 - 12) = mdc(12, 6) = 6.$$

Exercício 7: Calcule $mdc(339, 1407)$.

Solução.

- Dividindo 1407 por 339 obtemos $1407 = 4 \cdot 339 + 51$. Assim $mdc(339, 1407) = mdc(339, 51)$.
- Agora dividimos 339 por 51, obtendo $339 = 6 \cdot 51 + 33$. Daí $mdc(51, 339) = mdc(51, 33)$.
- Dividindo 51 por 33 obtemos quociente 1 e resto 18. Daí $mdc(33, 51) = mdc(33, 18)$.
- Dividindo 18 por 33 obtemos quociente 1 e resto 15. Logo $mdc(18, 33) = mdc(18, 15)$.
- Dividindo 18 por 15 obtemos quociente 1 e resto 3, de modo que $mdc(15, 18) = mdc(15, 3)$.

Observar que o quociente 4 na divisão de 1407 por 339 significa que podemos aplicar quatro vezes consecutivas a propriedade $mdc(a, b) =$

$mdc(a, b-a)$, subtraindo quatro vezes 339 de 1407, caso se quisesse calcular este mdc como na seção anterior. Observe:

$$mdc(339, 1407) = mdc(339, 1407-339) = mdc(339, 1068) =$$

$$mdc(339, 1068) = mdc(339, 1068-339) = mdc(339, 729) =$$

$$mdc(339, 729) = mdc(339, 729-339) = mdc(339, 390) =$$

$$mdc(339, 390) = mdc(339, 390-339) = mdc(339, 51).$$

Isto explica porque trocando b pelo resto da divisão de b por a aceleramos o cálculo do mdc.

Exercício 8: Calcule $mdc(2282, 7063)$.

Solução.

- Dividindo 7063 por 2282 obtemos $7063 = 3 \cdot 2282 + 217$. Assim $mdc(2282, 7063) = mdc(2282, 217)$.
- Dividindo 2282 por 217 obtemos $2282 = 10 \cdot 217 + 112$. Logo $mdc(217, 2282) = mdc(217, 112)$.
- Dividindo 217 por 112 obtemos $217 = 1 \cdot 112 + 105$ e assim $mdc(112, 217) = mdc(112, 105)$.
- Dividindo 112 por 105 obtemos $112 = 1 \cdot 105 + 7$ de modo que $mdc(105, 112) = mdc(105, 7)$.

Exercício 9: Utilizando o Algoritmo de Euclides calcule:

(a) $mdc(1287, 2782)$.

(b) $mdc(2616, 3240)$.

(c) $mdc(1598, 14909)$.