Cheat Sheet: FMC - Unidade 2

Mateus Dias
Tecnologia da Informação - IMD/UFRN

03/10/2025

DEFINIÇÃO 0 - Divisores e Múltiplos

Essa definição não faz, realmente, parte do conteúdo, mas é fundamental para o entendimento de todas as próximas definições.

Parte 1 - Divisores

Um número inteiro d é divisor de um número inteiro a se, e somente se, ao dividir a por d, o resto for **zero**, ou seja, a divisão é exata.
Por exemplo, para o número 24 temos 8 divisores. São eles:

$$D = \{1, 2, 3, 4, 6, 8, 12, 24\}$$

Parte 2 - Múltiplos

Um número inteiro b é múltiplo de um número inteiro a se, e somente se, existe um número inteiro k tal que:

$$b = ak$$

Por exemplo, se $a = 3$, os múltiplos de 3 são:

- Se $k = 2$, $b = 3 \cdot 2 = 6$
- Se $k = 5$, $b = 3 \cdot 5 = 15$

O conjunto dos múltiplos de 3 é:

$$M(3) = \{\dots, -9, -6, -3, 0, 3, 6, 9, 12, \dots\}$$

Parte 3 - Relação entre Divisores e Múltiplos

Se b é um **múltiplo** de a, isso significa que a é um **divisor** de b. Esta relação será explorada melhor na definição de **divisibilidade**.

DEFINIÇÃO 1 - Divisibilidade

Sejam $a, b \in \mathbb{Z}$. Dizemos que a divide b se, e somente se $\exists k \in \mathbb{Z}$ tal que: $ak = b$.

$$a \mid b \iff (\exists k \in \mathbb{Z})(ak = b).$$

DEFINIÇÃO 2 - Módulo

Sejam $a, b, m \in \mathbb{Z}$. a é congruente a b módulo m se, e somente se $m \mid a - b$.

$$a \equiv b \pmod{m} \iff m \mid a - b$$

Também é possível usar o módulo para representar o resto de uma divisão. Pela definição de divisão euclidiana, sabe-se que um número arbitrário $D \in \mathbb{Z}$ pode ser representado como

$$D = dq + r.$$

Com **D** sendo o **dividendo**, **d** o **divisor**, **q** o **quociente** e **r** o **resto** $(0 \leq r < |d|)$.
Nesse sentido, podemos afirmar que:

$$D \bmod d = r.$$

TEOREMA 1

Sejam $a, b, m \in \mathbb{Z}$, com $m > 0$. a é congruente a b módulo m se, e somente se $a \bmod m = b \bmod m$.

$$a \equiv b \pmod{m} \iff a \bmod m = b \bmod m.$$

Prova ($\implies$)

Suponha $a, b, m \in \mathbb{Z}$ tal que $a \equiv b \pmod{m}$.
Pelas definições 2 e 1, respectivamente, temos que:

$$\begin{aligned}
&m \mid a - b \\
&mk = a - b \\
&a = b + mk \quad \textbf{(I)}
\end{aligned}$$

Pela definição do resto, ao dividir b por m, temos:

$$b = q_b \cdot m + r_b \quad \textbf{(II)}$$

Onde $q_b \in \mathbb{Z}$ e $r_b = b \bmod m$, com $0 \leq r_b < m$.
Substituindo **(II)** em **(I)**:

$$\begin{aligned} a &= (q_b \cdot m + r_b) + mk \\ a &= mq_b + mk + r_b \\ a &= m \cdot (q_b + k) + r_b \end{aligned}$$

Tome $q_a = q_b + k$. Como $q_a \in \mathbb{Z}$ e $0 \leq r_b < m$, podemos dizer que r_b é o resto da divisão de a por m, isto é, $a \bmod m = r_b$.
Como $r_b = b \bmod m$, temos que:

$$a \bmod m = b \bmod m.$$

Prova ($\Longleftarrow$)

Suponha $a, b, m \in \mathbb{Z}$ tal que $a \bmod m = b \bmod m$. Seja r o valor comum do resto, de forma que:

$$r = a \bmod m = b \bmod m$$

Pela definição do resto, podemos escrever a e b como:

$$\begin{aligned} a &= q_a \cdot m + r \\ b &= q_b \cdot m + r \end{aligned}$$

Onde $q_a, q_b \in \mathbb{Z}$ e $0 \leq r < m$. Dessa forma, a diferença $a - b$ fica desta forma:

$$\begin{aligned} a - b &= (q_a \cdot m + r) - (q_b \cdot m + r) \\ a - b &= q_a \cdot m + r - q_b \cdot m - r \\ a - b &= m \cdot (q_a - q_b) \end{aligned}$$

Seja $k = q_a - q_b$. Como $q_a \in \mathbb{Z}$ e $q_b \in \mathbb{Z}$ temos que $k \in \mathbb{Z}$. Portanto:

$$a - b = mk$$

Pela definição 1 e 2, respectivamente, temos que:

$$\begin{aligned} &m \mid a - b \\ &a \equiv b \pmod{m} \end{aligned}$$

■

DEFINIÇÃO 3 - Máximo Divisor Comum

Sejam $a, b \in \mathbb{Z}$ com $a, b \neq 0$. O MDC de a e b, denotado por $mdc(a, b)$ é o único inteiro positivo d que satisfaz as seguintes condições:

1. $d \mid a$
2. $d \mid b$
3. $\forall c \in \mathbb{Z}[((c \mid a) \wedge (c \mid b)) \implies c \mid d]$

Em outros termos, d é o maior número inteiro positivo que divide a e b ao mesmo tempo.

Exemplos

1. Calcular o $mdc(12, 18)$.

Divisores de 12: $\{1, 2, 3, 4, 6, 12\}$
Divisores de 18: $\{1, 2, 3, 6, 9, 18\}$
Divisores comuns: $\{1, 2, 3, 6\}$
Máximo Divisor Comum (MDC): 6

Algoritmo de Euclides

O algoritmo de Euclides é um método simples para encontrar o MDC entre dois números inteiros diferentes de zero. Ele é um derivado da divisão euclidiana:

$$D = dq + r.$$

Com **D** sendo o **dividendo**, **d** o **divisor**, **q** o **quociente** e **r** o **resto** $(0 \leq r < |d|)$.

Se queremos calcular $mdc(a, b)$, podemos assumir $D_1 = \max(a, b)$ como o dividendo inicial e $d_1 = \min(a, b)$ como o divisor inicial.

O algoritmo procede em etapas sucessivas, onde o resto de cada divisão se torna o novo divisor e o divisor anterior se torna o novo dividendo, até que $r_i = 0$ (onde i é o número de iterações). O último resto **não nulo** é o $mdc(a, b)$.

Exemplos

2. Calcular o $mdc(270, 192)$.

$$270 = 192 \cdot 1 + 78 \tag{1}$$
$$192 = 78 \cdot 2 + 36 \tag{2}$$
$$78 = 36 \cdot 2 + 6 \tag{3}$$
$$36 = 6 \cdot 6 + 0 \tag{4}$$

Portanto, o $\mathbf{mdc(270, 192)}$ é igual ao último resto não nulo, ou seja, **6**.

DEFINIÇÃO 4 - Mínimo Múltiplo Comum

Sejam $a, b \in \mathbb{Z}$. O $mmc(a, b)$ é o menor número inteiro positivo que é múltiplo de a e b simultaneamente.

Exemplos

1. Calcular o $mmc(4, 6)$.

$$\textbf{Múltiplos de 4: } \{4, 8, \mathbf{12}, 16, 20, 24, ...\}$$
$$\textbf{Múltiplos de 6: } \{6, \mathbf{12}, 18, 24, 30, 36, ...\}$$

O menor dos múltiplos comuns é 12, portanto $mmc(4, 6) = 12$.

Métodos para calcular o MMC

É possível conectar os conceitos de MMC e MDC com uma fórmula relacionada à Matemática Discreta:

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

Este é o método que apresenta maior eficiência computacional para calcular o MMC entre dois números, mas também existe o método da fatoração prima (mais útil para calcular o MMC entre três ou mais números):

1. **Fatore** todos os números em seus fatores primos;
2. O **MMC** é o produto de todos os fatores primos distintos, cada um elevado à maior potência em que ele aparece em qualquer uma das fatorações.

Exemplos

2. Calcular o $mmc(12, 18)$ usando o primeiro método.

1. Calcular o **mdc(12,18)**:
   Segundo o método apresentado na **definição 3**:

$$18 = 12 \cdot 1 + 6 \tag{1}$$
$$12 = 6 \cdot 2 + 0 \tag{2}$$

   Portanto, $mdc(12, 18) = \mathbf{6}$.

2. Substituir na fórmula:

$$mmc(12, 18) = \frac{|12 \cdot 18|}{6}$$

$$mmc(12, 18) = \frac{216}{6}$$

$$mmc(12, 18) = 36$$

3. Calcular o $mmc(12, 18)$ usando o segundo método.

1. Fatore 12 e 18 em seus respectivos fatores primos:

$$12 = 2^2 \cdot 3^1$$
$$18 = 2^1 \cdot 3^2$$

2. Fatores e maiores potências:
   - Fator 2: 2^2
   - Fator 3: 3^2

3. Cálculo:

$$mmc(12, 18) = 2^2 \cdot 3^2$$
$$mmc(12, 18) = 4 \cdot 9$$
$$mmc(12, 18) = 36$$

O MMC entre a e b também pode ser interpretado como "o primeiro número em que a irá *se encontrar* com b quando ambos forem multiplicados por números naturais".

TEOREMA 2 - Teorema de Bézout

Sejam $a, b \in \mathbb{Z}$ com $a, b > 0$. O $mdc(a, b)$ pode ser escrito como uma combinação linear de a e b:

$$mdc(a, b) = sa + tb$$

Com $s, t \in \mathbb{Z}$.
O método para descobrir os valores de s e t é substituir consecutivamente os valores no algoritmo de Euclides.

Exemplos

1. Expressar o mdc(270,192) como uma combinação linear de 270 e 192.

$$\begin{aligned}
&270 = 192 \cdot 1 + 78\\
&192 = 78 \cdot 2 + 36\\
&78 = 36 \cdot 2 + 6\\
&36 = 6 \cdot 6 + 0\\
\\
&6 = 78 - 2 \cdot 36\\
&6 = 78 - 2 \cdot (192 - 2 \cdot 78)\\
&6 = (270 - 1 \cdot 192) - 2 \cdot (192 - 2 \cdot (270 - 1 \cdot 192))\\
&6 = 270 - 1 \cdot 192 - 2 \cdot 192 + 4 \cdot 270 - 4 \cdot 192\\
&6 = 5 \cdot 270 - 7 \cdot 192
\end{aligned}$$

Portanto, $s = 5, t = -7$.

DEFINIÇÃO 5 - Inverso Multiplicativo Modular

Este é um conceito essencial que se relaciona com o conceito de equação modular (**definição 6**).

Sejam $a, m \in \mathbb{Z}$. O inverso multiplicativo modular de a mod m é o inteiro x tal que:

$$ax \equiv 1 \pmod{m}$$

Condição de existência

O inverso multiplicativo modular de a mod m existe se, e somente se $mdc(a, m) = 1$, isto é, se a e m forem **coprimos** ou **primos entre si**.

Métodos para encontrar

É possível encontrar o inverso multiplicativo de a mod m facilmente usando o **teorema 2 - teorema de Bézout**.

Ao escrever o $mdc(a, m)$ como uma combinação linear de a e m, o coeficiente de a é o seu inverso multiplicativo.

Exemplos

1. Encontrar o inverso multiplicativo de 3 mod 7.

$3x \equiv 1 \pmod 7$

Primeiro, precisamos calcular $mdc(3, 7)$.

$7 = 3 \cdot 2 + 1$
$3 = 1 \cdot 3 + 0$

Como $mdc(3, 7) = 1$, o inverso multiplicativo existe.
Agora, escrevemos 1 como uma combinação linear de 3 e 7.

$1 = 1 \cdot 7 - 2 \cdot 3$

O coeficiente de 3 é -2, então $x = -2$.

Como o inverso multiplicativo encontrado é um número negativo, podemos fazer a operação x mod m para encontrar um inverso multiplicativo positivo (o que é uma boa prática).

$$-2 \bmod 7 = 5$$

Logo, o inverso multiplicativo que procuramos é **5**.

Obs: Para encontrar um inverso multiplicativo positivo também é possível somar m a x até que x seja maior ou igual a 1.