# Leitura Complementar + Lista de Execícios

**SEMANA 09 - Primos, Máximo Divisor Comum e Mínimo Múltiplo Comum**

**2022.1**

**Notas de Aula de Matemática Discreta**

Prof. Samy Sá

Universidade Federal do Ceará
Campus de Quixadá

Este documento traz uma lista de exercícios referentes aos tópicos da SEMANA 09. É recomendado que você faça todos os exercícios e tire suas dúvidas antes das aulas da semana seguinte.

## 1 Instruções Preliminares

Obs.: "prove", "demonstre" e "mostre" são sinônimos. Nos exercícios abaixo, em cada um dos casos, você deve oferecer um demonstração (uma prova!) do que estiver sendo afirmado.

Quando a resposta envolver números, todos os cálculos para chegar a estes números devem ser apresentados. Busque fornecer respostas que deixem claro seu raciocínio, exibindo e justificando todos os passos executados. Lembre-se que a sua resposta será lida por alguém no futuro e escreva suas respostas pensando no leitor. Idealmente, as suas respostas devem permitir que qualquer colega da turma possa identificar claramente quais foram os passos que você fez e porquê.

É muito importante que você suplemente esta lista com exercícios do livro conforme sua necessidade. Se tiver facilidade com os tópicos, poucos exercícios bastarão para compreendê-los; se tiver dificuldades, o caminho será reforçar a leitura do capítulo e resolver mais exercícios.

## 2 Leitura do Livro

Leia atentamente a Seção 3.5 do Rosen e verifique a lista de exercícios do livro por complementos a estes. Conforme a sua necessidade, revise os conteúdos sobre técnicas de demonstração, divisibilidade, algoritmo da divisão e sequências.

## 3 Leitura Complementar: Provas de Teoremas com Primos e Fatoração

O objetivo desta leitura é exemplificar pequenas diferenças que observaremos ao tentar provar teoremas sobre os novos conceitos que introduzimos esta semana. O motivo é que a video-aula da semana focou bastante nos conceitos e algoritmos relacionados, mas

não trouxe exemplos de demonstrações. Observaremos que, na prática, não há muito diferença em relação aos tópicos anteriores, pois estes conceitos continuam fortemente baseados em divisibilidade.

Para guiar o começo da nossa discussão, demonstraremos o seguinte teorema:

**Teorema 1** *Para todo $n, m, k$ inteiros, se $k \mid \texttt{MDC}(n, m)$, então $k \mid n$ e $k \mid m$.*

A prova deste teorema segue quase diretamente da definição de máximo divisor comum, bastando lembrarmos de uma das principais propriedades da divisibilidade.

**Lema 1** *Para todo $n, m, k$ inteiros, se $n \mid m$ e $m \mid k$, então $n \mid k$.*

A prova deste lema foi deixada como exercício na aula que introduziu o conceito de divisibilidade. A seguir, apresentarei uma prova desta propriedade. Recomenda-se que você compare a nova prova com o exemplo que foi exibido na mesma aula.

**Prova 1 (Lema 1)** *Sejam $a, b, c$ inteiros quaisquer, suponha que $a \mid b$ e $b \mid c$. Usando a definição de divisibilidade, temos que existe um inteiro $k$ tal que $b = ak$ e que existe um inteiro $j$ tal que $c = bj$. A primeira igualdade nos permite substituir $b$ por $ak$ na segunda igualdade. Com isso, obteremos que $c = (ak).j$. Reorganizando os termos, teremos que $c = a.(kj)$. Então, como $k$ e $j$ são inteiros, $kj$ é um inteiro. Neste ponto, repare que $a$ precisa ser um número diferente de zero, pois supusemos anteiormente que $a \mid b$. Isso nos permite usar a definição de divisibilidade para concluir que $a \mid c$.*

Agora que provamos esta propriedade, podemos utilizá-la como lema na prova do teorema principal. Isto nos permitirá escrever uma prova mais curta, onde os passos acima, invés de serem repetidos, serão substituídos pela aplicação do lema.

**Prova 2 (Teorema 1)** *Sejam $a, b, c$ inteiros quaisquer. Por prova direta, suponha que $c \mid \texttt{MDC}(a, b)$. Pela definição de máximo divisor comum, $\texttt{MDC}(a, b)$ é o maior inteiro $d$ tal que $d \mid a$ e $d \mid b$. Desta forma, como $\texttt{MDC}(a, b) = d$, podemos reescrever a hipótese de forma mais simples, supondo simplesmente que $c \mid d$. Neste ponto, temos que $c \mid d$ (hipótese da prova direta) e que $d \mid a$ (pelo conceito de máximo divisor comum). O Lema 1 nos permite usar estas afirmações para concluir que $c \mid a$. Similarmente, como $c \mid d$ e $d \mid b$, podemos concluir que $c \mid b$ (pelo Lema 1).*

A prova acima foi escrita de forma a destacar os pontos importantes conceitualmente, mas também poderíamos ter escrito uma prova mais direta usando apenas as definições que temos. Isto se torna especialmente verdadeiro uma vez que você compreender que $\texttt{MDC}(a, b)$ é um número inteiro tanto quando $a$, $b$, 2 ou qualquer outro.

**Prova 3 (Teorema 1 (Alternativa))** *Sejam $a, b, c$ inteiros quaisquer, suponha que $c \mid \texttt{MDC}(a, b)$. Pela definição de divisibilidade, deve existe um inteiro $k$ tal que $\texttt{MDC}(a, b) = ck$. Além disso, pela definição de máximo divisor comum, sabemos que $\texttt{MDC}(a, b) \mid a$ e $\texttt{MDC}(a, b) \mid b$. Então, pela definição de divisibilidade, devem existir um inteiro $j$ tal que $a = \texttt{MDC}(a, b).j$ e um inteiro $l$ tal que $b = \texttt{MDC}(a, b).l$. Como $\texttt{MDC}(a, b) = ck$, podemos fazer $a = \texttt{MDC}(a, b).j = (ck).j = c.(kj)$. Repare que $kj$ é um número inteiro, visto que $k$ e $j$ foram declarados como inteiros e que $c \neq 0$, pois supusemos que $c \mid \texttt{MDC}(a, b)$. Portanto, $c \mid a$. Os passos necessários para concluir que $c \mid b$ são análogos a partir dos fatos $\texttt{MDC}(a, b) = ck$ e $b = \texttt{MDC}(a, b).l$, previamente obtidos.*

Observe que estas provas têm estrutura idêntica à de outras que temos exercitado:

- o enunciado é uma generalização de condicional
- iniciamos com a instanciação das variáveis que aparecem generalizadas no enunciado, depois iniciamos uma prova de condicional (por prova direta, neste caso)
- logo após a hipótese da prova direta, usamos uma das definições que estudamos
- o objetivo da prova direta envolve expressões de divisibilidade, o que nos pede por uma prova de existência

Neste último ponto, o obetivo da prova direta seria concluirmos que "$c \mid a$ e $c \mid b$", uma conjunção. Precisamos, portanto, de provas independentes para cada parte desta conjunção: uma prova de que "$c \mid a$" e outra de que "$c \mid b$". Em ambos os casos, devemos encontrar estas afirmações partindo da hipótese que criamos no começo da prova direta, onde propomos supor que "$c \mid \texttt{MDC}(a, b)$".

Há apenas duas diferenças principais entre estas provas e as anteriores que praticamos:

1. Às vezes trabalharemos com uma expressão longa, de múltiplos caracteres, para nos referirmos a um número inteiro. Nos exemplos acima, usamos a expressão $\texttt{MDC}(a, b)$, que refere-se ao máximo divisor comum de $a$ e $b$. Esta é uma expressão de função binária nos inteiros (dois parâmetros inteiros, um resultado inteiro) e refere-se diretamente ao resultado que deve ser retornado. Até agora nós temos usado variáveis com uma única letra para nos referir a números desconhecidos, mas nada impediria termos usado palavras em seu lugar. O único requisito para estas manipulações é uniformizarmos os nomes de cada variável, como fazemos em programação. Desta forma, a cada vez que usarmos o mesmo nome em partes diferentes do texto, estaremos nos referindo ao mesmo objeto.

2. Pode ser mais conveniente utilizarmos uma consequência direta das definições de máximo divisor comum e mínimo múltiplo comum invés do próprio texto da definição. É uma questão de preferência, que depende apenas de você. Por exemplo, a prova 2 utilizou o próprio texto da definição de máximo divisor comum. Isso nos levou a substituir "$\texttt{MDC}(a, b)$" por "$d$" daquele ponto em diante, pois uma nova variável (nomeada por um caractere) foi introduzida na prova. Já a Prova 3 utilizou apenas o fato de que $\texttt{MDC}(a, b)$ divide $a$ e divide $b$, sem levar em conta que este é o maior inteiro que satisfaz as duas condições. Isto permitiu utilizar de forma mais direta a definição de divisibilidade sobre a expresssão "$\texttt{MDC}(a, b)$", evitando a introdução de uma nova variável. Cada caminho tem suas vantagens e ambos são sempre possíveis de fazer. É uma questão de preferência.

A outra situação com que podemos precisar lidar é a de provar que um certo número é o *máximo* divisor comum ou o *mínimo* múltiplo comum de alguns números. Para guiar esta discussão, discutiremos a prova do seguinte teorema:

**Teorema 2** *Para todo $n$ inteiro positivo,* $\texttt{MDC}(n, n) = n$.

Intuitivamente, nós já sabemos que $n \mid n$ para todo inteiro $n$ diferente de zero, então com certeza isso valera para os inteiros positivos... Mas como provar que $n$ é o *maior* divisor de $n$? Tecnicamente, isso significará mostrar que

$$\textit{não existe nenhum inteiro } k > n \textit{ tal que } k \mid n.$$

Por sua vez, uma prova de não existência é idêntica a uma prova de generalização, como discutimos durante o tópico de *prova de unicidade*. No nosso exemplo, deveremos mostrar que

$$\textit{para todo inteiro } k > n\textit{, não é verdade que } k \mid n.$$

Isso significa que a prova do Teorema 2 envolverá duas partes e será muito similar às provas de unicidade.

1. devemos garantir, para todo inteiro $n$ positivo, que $n \mid n$;
2. sendo $n$ um inteiro positivo qualquer, devemos mostrar que para todo inteiro $k$, se $k > n$, então $k \nmid n$.

O motivo para essa semelhança é que o *máximo* divisor comum de dois números é sempre *único*. Na verdade, como estudaremos mais à frente no tópico "*Relações de Ordem Parcial*", os conceitos de máximo e mínimo dependem diretamente da unicidade. Desta forma, garantir que um inteiro é o *máximo* divisor comum de dois números significa garantir que ele é *o único* divisor comum dos dois números que satisfaz uma propriedade: a de ser maior que os demais.

Apesar do detalhe na discussão acima, isso não significa que a prova do Teorema 2 será longa.

**Prova 4 (Teorema 2)** *Seja $a$ um inteiro positivo qualquer, nós precisamos provar que $\texttt{MDC}(a, a) = a$. Pela definição de máximo divisor comum, $\texttt{MDC}(a, a)$ é o maior inteiro $d$ tal que $d \mid a$ (veja a observação[1] no fim da página).*

*Primeiro, mostraremos que $a \mid a$. Para tal, basta notar que $a = a.1$. Como $1$ é inteiro e $a \neq 0$ (pois é positivo), podemos usar a definição de divisibilidade para concluir que $a \mid a$. Isso garante que $a$ é um divisor de $a$.*

*Nos resta agora mostrarmos que $a$ é o* maior *divisor de $a$. Isso equivale a mostrar que todo inteiro $k > a$ não divide $a$. Faremos isso utilizando a técnica de* prova por contradição*, que envolve supor o contrário do que desejamos provar, mostrando depois que essa hipótese leva a uma contradição.*

*Desta forma, suponha que existe um inteiro $b > a$ tal que $b \mid a$. Agora considere a divisão de $a$ por $b$ no contexto do* Algoritmo da Divisão*. Visto que $0 \leq a < b$ e*

[1] A aplicação da definição nos dirá que $\texttt{MDC}(a, a)$ é o maior inteiro $d$ tal que $d \mid a$ e $d \mid a$, mas não perderemos nem ganharemos nada em afirmar a mesma coisa duas vezes. Uma das propriedades da conjunção, chamada "idempotência da conjunção" nos garante que $p \wedge p \equiv p$ para toda proposição $p$.

$a = b.0 + a$, *obtemos que* $a$ ***div*** $b = 0$ *e* $a$ ***mod*** $b = a$. *Mas como* $a$ *é positivo,* $a$ ***mod*** $b = a$ *significará que* $a$ ***mod*** $b \neq 0$. *Portanto,* $b \nmid a$, *uma contradição. Isso garante que não existe nenhum inteiro* $b > a$ *tal que* $b \mid a$. *Ou seja, garante que* $a$ *é o* maior *divisor de* $a$.

Observe que esta prova utilizou a prova por generalização em dois pontos distintos: no começo, com base no enunciado do teorema, e na segunda parte da prova de que $a$ seria o *maior* divisor de si mesmo. Além disso, tivemos uma prova construtiva de existência para garantir que $a \mid a$. Esta parte da prova junto com a segunda passagem de generalização são similares a uma prova de unicidade. Tirando isso, utilizamos somente os conceitos que temos estudados recentemente: a divisibilidade, o algoritmo da divisão, e a definição de máximo divisor comum. Provas sobre o mínimo múltiplo comum de dois números funcionarão todos de forma análoga aos exemplos desta texto, adaptando-se apenas quais variáveis farão os papéis de dividendo e divisor em cada caso e trocando "$>$" por "$<$" na última parte das provas de que um inteiro é o *mínimo* múltiplo comum de dois números.

Para finalizarmos, vou mostrar um dos casos mais simples de prova de teorema com estes conceitos. Esta será uma prova sem manipulação algébrica, que depende apenas da definição de mínimo múltiplo comum.

**Teorema 3** *Para todos* $n, m$ *inteiros, temos* $\texttt{MMC}(n, m) = \texttt{MMC}(m, n)$.

Este teorema propõe que o mínimo múltiplo comum de dois números não é influenciado pela ordem em que estes números aparecem. Repare que se você usasse a definição de mínimo múltiplo comum separadamente sobre cada uma das expressões "$\texttt{MMC}(a, b)$" e "$\texttt{MMC}(b, a)$", obterá conclusões quase idênticas. Por conta disso, podemos construir uma prova bastante simples para este teorema:

**Prova 5 (Teorema 3)** *Sejam* $a$ *e* $b$ *inteiros quaisquer. Pela definição de mínimo divisor comum,* $\texttt{MMC}(a, b)$ *é o menor inteiro positivo* $c$ *tal que* $a \mid c$ *e* $b \mid c$. *A comutatividade da conjunção nos permite reescrever esta frase para dizer que* $\texttt{MMC}(a, b)$ *é o menor inteiro positivo* $c$ *tal que* $b \mid c$ *e* $a \mid c$. *Utilizando novamente a definição de mínimo múltiplo comum, vemos que* $c$ *é o* $\texttt{MMC}(b, a)$. *Ou seja,* $\texttt{MMC}(a, b) = \texttt{MMC}(b, a)$.

Este exemplo cumpre dois papéis: garantir um exemplo que usasse a definição de mínimo múltiplo comum e mostrar que podemos utilizar manipulação lógica de forma direta nas nossas provas quando os conectivos lógicas aparecerem de forma explícita. De certa forma, é exatamente isso que fazemos a cada vez que aplicamos uma técnica de demonstração.

## 4 Exercícios

**Exercício 1.** Verifique se os números abaixo são ou não primos. Apresente sua resposta com todos os passos necessários para a conclusão, ou seja, indique quais testes de divisibilidade você fez e os restos de divisão obtidos em cada teste, justificando sua conclusão. Enuncie claramente o que você concluiu sobre o número avaliado.

| | | | |
|---|---|---|---|
| (a) 19 | (e) 79 | (i) 133 | (m) 521 |
| (b) 39 | (f) 81 | (j) 189 | (n) 595 |
| (c) 57 | (g) 91 | (k) 259 | (o) 737 |
| (d) 61 | (h) 109 | (l) 437 | (p) 839 |

**Exercício 2.** Forneça a fatoração de cada inteiro abaixo. Para mostrar que todos os passos do algoritmo foram executados, apresentes o resto de cada divisão que você realizar.

| | | | |
|---|---|---|---|
| (a) 42 | (e) 84 | (i) 245 | (m) 326 |
| (b) 55 | (f) 93 | (j) 282 | (n) 484 |
| (c) 72 | (g) 160 | (k) 290 | (o) 500 |
| (d) 80 | (h) 215 | (l) 315 | (p) 567 |

**Exercício 3.** Para cada número da questão anterior, utilize a fatoração obtida para listar todos os seus divisores positivos. Utilize o método apresentado nos slides.

**Exercício 4.** Para cada item abaixo, utilize as *fatorações individuais* dos números pedidos para calcular seu MDC e MMC usando os métodos discutidos no vídeo da semana. Métodos diferentes destes não serão aceitos.

| | | | |
|---|---|---|---|
| (a) 10, 20 | (e) 20, 90 | (i) 72, 75 | (m) 180, 515 |
| (b) 10, 25 | (f) 45, 90 | (j) 15, 75 | (n) 243, 410 |
| (c) 10, 45 | (g) 15, 25 | (k) 100, 85 | (o) 112, 208 |
| (d) 20, 45 | (h) 30, 72 | (l) 120, 244 | (p) 315, 247 |

**Exercício 5.** Prove os teoremas abaixo usando as técnicas de sua preferência:

(a) "Para todos $n$ inteiro, $1 \mid n$."

(b) "Para todos $n$ inteiro, se $n \neq 0$, então $n \mid n$."

(c) "Para todos $n$ inteiro, se $n > 1$, então existem pelo menos dois inteiros $k, j$ positivos diferentes que dividem $n$."

(d) "Para todos $j, k, n$ inteiros, sendo $j, k \neq 0$, se $j \mid k$ e $k \mid n$, então $j \mid n$."

(e) "Para todos $n, m, k$ inteiros com $k \neq 0$, se $k \mid n$ ou $k \mid m$, então $k \mid \texttt{MMC}(\texttt{n}, \texttt{m})$."

(f) "Para todos $n, m$ inteiros positivos, se $n \mid m$, então $\texttt{MDC}(n, m) = n$."

(g) "Para todos $n, m$ inteiros positivos, se $n \mid m$, então $\texttt{MMC}(n, m) = m$."

(h) "Para todos $n, m$ primos com $n \neq m$, $\texttt{MDC}(n, m) = 1$."

(i) "Para todos $n, m$ primos com $n \neq m$, $\texttt{MMC}(n, m) = nm$."

(j) "Para todos $n, m$ inteiros positivos, $\texttt{MDC}(n, m) \mid \texttt{MMC}(n, m)$."

(k) "Para todos $n, m, k$ inteiros positivos, se $\texttt{MDC}(n, m) = k$, então $\texttt{MDC}(n, k) = k$."

(l) "Para todos $n, m$ inteiros positivos, temos $\texttt{MDC}(n, m) = \texttt{MDC}(m, n)$."

(m) "Para todos $n, m$ inteiros positivos com $n > m$, $\texttt{MDC}(n, m) = \texttt{MDC}(m, n-m)$."

(n) "Para todos $n, m$ inteiros positivos com $n > m$, $\texttt{MDC}(n, m) = \texttt{MDC}(m, n \textbf{ mod } m)$."

(o) "Para todos $n, m, k$ inteiros positivos, $\texttt{MDC}(n, \texttt{MDC}(m, k)) = \texttt{MDC}(\texttt{MDC}(n, m), k)$."

(p) "Para todos $n, m, k$ inteiros positivos, $\texttt{MMC}(n, \texttt{MMC}(m, k)) = \texttt{MMC}(\texttt{MMC}(n, m), k)$."