Lista de revisão para P1
Álgebra 1 para licenciatura
MAT0120

Exercícios retirados do livro: **Números, Uma Introdução a Matemática**. Vocês não devem entregar. Os execícios marcados com * são os mais importantes e recomendo que não deixem de fazê-los para estudar.

O conteúdo da prova vai até a seção 3.3. Portanto, devem estudar o capítulo 1 (todas as seções), capítulo 2(seções 2.1, 2.3, 2.4, 2.5 e 2.6), capítulo 3(seções 3.1, 3.2 e 3.3).

A ideia dessa lista é guiar vocês durante os estudos, pontuando o que é mais importante e que vocês não devem deixar passar. Além dos exercícios essa lista contem um pequeno resumo das seções 2.5 e 2.6 que não foram tratadas em aula devido ao caos que se instaurou com a pandemia, mas que são fundamentais nesse curso.

Lembrem-se de que a prova será no dia 23/04 que poderá ser feita durante todo o dia com o auxílio dos livros que escolherem. Pedimos a honestidade de todos para que consultem apenas os livros e suas notas de aula, nada mais. Como sugestão particular minha (Jaime), aconselho a se focarem nas listas, inclusive nesta e no livro **Números, Uma Introdução a Matemática**, com isso vocês com certeza farão a prova sem muitas dificuldades.

Bons estudos!

1 Exs do capítulo 1

Exercício 1. *Provar que para todo inteiro positivo (<u>maior</u> que zero) vale:*

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(2n+1)(n+1)}{6} \tag{1}$$

Exercício 2. *(Soma dos termos de uma progressão geométrica) Sejam a e r dois números inteiros, $r \neq 1$. A sequência $a_1 = a$, $a_2 = ra, a_3 = r^2a, \cdots, a_n = r^{n-1}a, \cdots$ diz-se uma progressão geométrica de razão r. Provar que a soma dos n primeiros termos de uma progressão geométrica é*

$$S_n = \frac{r^n a - a}{r - 1} \tag{2}$$

Exercício 3. *Demonstrar que para todo inteiro positivo n vale:*

i. $1 + 2 + \cdots + 2^{n-1} = 2^n - 1$;

ii. $n < 2^n$.

Exercício 4 (*)**.** *(Desigualdade de Bernoulli) seja $x \in \mathbb{R}$ com $x > -1$. Demonstrar que*

$$(1+x)^n \geq 1 + nx, \text{ para todo } n \geq 2 \tag{3}$$

2 Exs do capítulo 2

2.1 Exs da seção 2.1

Exercício 5. *(aquecimento) Façam/leiam as demonstrações das proposições* 2.1.2, 2.1.3 *e* 2.1.4 *na seção 2.1. Tudo que está nessas proposições deve ser* <u>muito</u> *natural para vocês.*

Exercício 6 (*)**.** *Decida se as afirmações abaixo são verdadeiras ou falsas, dando a demonstração ou um contra-exemplo. Sejam a, b e c inteiros quaisquer:*

i. *Se $a|b$, então $(a+c)|(b+c)$;*

ii. *Se $a|b$, então $ac|bc$;*

iii. *Se $a|b$, então $(-b)|(-a)$;*

iv. *Se $a|(b+c)$, então $a|b$ ou $a|c$.*

Exercício 7. *Sejam a, b, c inteiros. Provar que:*

i. *Se $a|b$, então $(-a)|b$, $a|(-b)$ e $(-a)|(-b)$;*

ii. *Se $c \neq 0$, então $a|b$ se e somente se $ac|bc$.*

Exercício 8 (*)**.** *Leiam com atenção a demonstração do lema* 2.1.5 *e do teorema* 2.1.6*(Algoritmo da Divisão)*

Exercício 9 (*)**.** *Usar o algoritmo da divisão para provar que*

i. *Todo inteiro ímpar é da forma $4k+1$ ou $4k+3$.*

ii. O cubo de um número inteiro é da forma $9k$, $9k+1$ ou $9k+8$.

Exercício 10 (*). *i. Provar que o produto de três inteiros consecutivos é um múltiplo de 3;*

ii. Mais geralmente, provar que o produto de n inteiros consecutivos é múltiplo de n.

Exercício 11. *Provar que se a é um inteiro tal que 2 não divide a, então $8|(a^2-1)$.*

Exercício 12. *i. A soma dos quadrados de dois inteiros ímpares não pode ser um quadrado perfeito;*

ii. Se a é ímpar, então $24|a(a^2-1)$;

iii. Se a e b são inteiros ímpares, então $8|(a^2-b^2)$

2.2 Exs da seção 2.3

Definição 1. *Chama-se máximo divisor comum de a e b o maior de seus divisores comuns, isto é,*

$$mdc(a,b) = maxD(a,b)$$

onde $D(a,b) = \{d \in \mathbb{Z} : d|a \text{ e } d|b\}$

Exercício 13 (*). *Sejam a, be c números inteiros. Verificar se as afirmações abaixo são verdadeiras ou falsas, dando a demonstração ou um contra-exemplo:*

i. $mdc(a,b) = mdc(b,a)$;

ii. $mdc(mdc(a,b),c) = mdc(a, mdc(b,c))$;

iii. $mdc(a,1) = 1$;

iv. $mdc(a, b+c) = mdc(a,b) + mdc(a,c)$;

v $mdc(a,bc) = mdc(a,b) \cdot mdc(a,c)$;

vi. $mdc(ab,cd) = mdc(a,c) \cdot mdc(b,d)$

vii. $a|b \Leftrightarrow mdc(a,b) = |b|$;

viii. $mdc(-a,b) = mdc(a,-b) = mdc(a,b)$

Exercício 14. *Sejam a, b e d inteiros, com $d > 0$. Decidir se as afirmações abaixos são verdadeiras ou falsas, dando a demonstração ou um contra-exemplo*

i. *Se existem $r,\ s \in \mathbb{Z}$ tais que $d = ra + sb$, então $d = mdc(a,b)$;*

ii. *se existem $r, s \in \mathbb{Z}$ tal que $ra + sb = 1$, então $mdc(a,b) = 1$.*

Teorema 1. *Sejam a, b inteiros. Um inteiro positivo d é o máximo divisor comum de a e b se e somente se verifica*

i. $d|a$ *e* $d|b$.

ii. *Se* $d'|a$ *e* $d'|b$, *então* $d'|d$.

Demonstração. leiam a demonstração na página 67. □

O teorema acima nos dá uma nova caracterização para máximo divisor comum, ou seja, poderíamos, com esse teorema, dar uma nova definição para mdc.

Exercício 15. *Façam/leiam a demonstração das proposições* 2.3.6 *e* 2.3.7 *(Teorema de Euclides)*

Observação 1. *Vamos dar uma demonstração do teorema de Euclides alternativa àquela que encontrarão no livro. Observe que como $mdc(a,b) = 1$, então podemos usar o Teorema de Bezout e temos que existem $r,\ s\ \in \mathbb{Z}$ tais que*

$$ra + sb = 1 \tag{4}$$

Com efeito, multiplicando ambos os lados de 4 por c ebtemos

$$rac + sbc = c \tag{5}$$

Claramente $a|rac$ e, por hipótese como $a|bc$ então $a|sbc$. Daí, concluímos que $a|c$.

Exercício 16 (*). *Façam/leiam a demonstração da proposição* 2.3.9.*(Essa proposição mesmo que com demonstração simples tem uma importância prática bem grande nos nossos exs, provavelmente vocês já até usaram esse resultado anteriormente nos exs dessa lista)*

Exercício 17. *Sejam* a*,* b*,* c *inteiros. Provar que*

i. Se $a|b$ *e* $mdc(b,c) = 1$*, então* $mdc(a,c) = 1$*;*

ii. $mdc(a,c) = mdc(b,c) = 1$ *se e somente se* $mdc(ab,c) = 1$*.*

Exercício 18 (*)**.** *Sejam* a*,* b *inteiros tais que* $mdc(a,b) = 1$*. Provar que:*

i $mdc(a+b, a^2+ab+b^2) = 1$*;*

ii. $mdc(a+b, a^2-ab+b^2) = 1$ *ou* 3*;*

iii. $mdc(a+b, a^2+b^2) = 1$ *ou* 2*.*

iv $mdc(a,b) = mdc(a, a \pm b)$

Exercício 19. *Sejam* a*,* b *initeiros. Para* $n \geq 1$*, provar que:*

i. $mdc(a,b) = 1$ *se e somente se* $mdc(a^n, b^n) = 1$*;*

ii. $a^n|b^n$ *se e somente se* $a|b$*.*

2.3 Exs da seção 2.4

Exercício 20. *usar o Algoritmo de Euclides para obter números* r *e* s *satisfazendo:*

i. $mdc(56,72) = 56r + 72s$*;*

ii. $mdc(24,138) = 24r + 138s$*;*

iii. $mdc(119,272) = 119r + 272s$*.*

2.4 Exs da seção 2.5

Um inteiro c chama-se um múltiplo comum de a e b se $a|c$ e $b|c$. Indicaremos por $M(a,b)$ o conjunto de todos os múltiplos comuns de a e be por $M^+(a,b)$ o conjunto de todos os múltiplos comuns positivos de a e b.

Observe que $M^+(a,b) \neq 0$, pois $|a||b|$ é múltiplo positivo de a e b. Perlo princípio da Boa ordem, esse conjunto tem elemento mínimo, assim definimos:

Definição 2. *Chama-se mínimo múltiplo comum de a e b o menor dos seus múltiplos positivos comuns, isto é,*

$$mmc(a,b) = minM^+(a,b)$$

Exercício 21. *Façam/leiam o lema* 2.5.2*.*

Teorema 2. *Sejam* a, $b \in \mathbb{Z}$ *e* m *um inteiro positivo. Então,* $m = mmc(a,b)$ *se e somente se* m *verifica:*

i. $a|m$, $b|m$;

ii. Se $a|m'$ *e* $b|m'$*, então* $m|m'$.

Demonstração. Página 76. □

Bem como o teorema (1), o teorema acima dá uma nova caracterização para minímo múltiplo comum.

Exercício 22 (*)**.** *Façam/leiam a proposição* 2.5.4 *que diz:*
"Sejam a, $b \in \mathbb{Z}$, $d = mdc(a,b)$ *e* $m = mmc(a,b)$*. Então,* $md = |ab|$*."*

Com esse exercício, temos uma maneira prática para calcular o $mmc(a,b)$. Dados a, $b \in \mathbb{Z}$, podemos calcular o $mdc(a,b)$ usando o Algoritmo de Euclides e, em seguida,

$$mmc(a,b) = \frac{|ab|}{mdc(a,b)} \tag{6}$$

Exercício 23 (*)**.** *Para todo* $n \in \mathbb{Z}$, $n \neq 0, 1$, *calcular:*

i. $mmc(n, n+1)$;

ii. $mmc(2n-1, 2n+1)$;

iii. $mmc(nc, (n+1)c)$, $c \in \mathbb{Z}$, $c \neq 0$.

Exercício 24 (*)**.** *Dados os inteiros não nulos a e b, provar que:*

i. Para todo $k \in \mathbb{Z}$, $k \neq 0$, $mmc(ka, kb) = |k|mmc(a,b)$;

ii. Se $k|a$ *e* $k|b$, $mmc(\frac{a}{k}, \frac{b}{k}) = \frac{mmc(a,b)}{|k|}$

2.5 Exs da seção 2.6

Antes de tudo, assim como na seção anterior, vamos fazer um breve resumo.

Definição 3. *Um inteiro p diz-se primo se tem exatamente dois divisores positivos* 1 *e* $|p|$.

Para um número que não é primo, dizemos que ele é composto. Observe que se um número a é composto, a definição acima nos garante que esse número deve ter um divisor b diferente de 1 e $|a|$. Um divisor nessas condições chama-se divisor próprio.

Proposição 1. *Seja p um número primo, e sejam a e b inteiros.*

i. Se $p \nmid a$, então $mdc(a,p) = 1$;

ii. Se $p|ab$, então $p|a$ ou $p|b$.

Demonstração. Página 78. □

Exercício 25. *Façam/leiam o corolário* 2.6.3*, o teorema* 2.6.4 *e o lema* 2.6.5*.*

Teorema 3. *Seja $a > 1$ um inteiro. Então, existem primos positivos $p_1 \leq p_2 \leq \cdots \leq p_t$ tais que $a = p_1 p_2 \cdots p_t$, e essa decomposição é única.*

Usando o o teorema 3, conseguimos provar o Teorema Fundamental da Aritmética.

Teorema 4. *(TFA) Seja a um inteiro diferente de 0, 1 e -1. Então, existem primos positivos $p_1 < p_2 < \cdots < p_r$ e inteiros positivos $n_1, n_2, \cdots, n_r$ tais que $a = Ep_1^{n_1} \cdots p_r^{n_r}$, em que $E = \pm 1$, conforme a seja positivo ou negativo. Além disso, essa decomposição é única.*

Com o teorema fundamental da aritmética podemos encontrar outro modo de caracterizar o mdc e o mmc. Vamos primeiro prosseguir com um exemplo, considere os números 360 e 4725, a decomposição em fatores primos é

$$360 = 2^3 \cdot 3^2 \cdot 5$$

$$4725 = 3^3 \cdot 5^2 \cdot 7$$

Note que os primos que aparecem em uma decomposição podem não aparecer em outra, todavia, se escrevermos a decomposição como

$$360 = 2^3 \cdot 3^2 \cdot 5 \cdot 7^0$$

$$4725 = 2^0 \cdot 3^3 \cdot 5^2 \cdot 7$$

então temos os mesmos primos em ambas as decomposições. Esse tipo de artifício nos ajudará a trabalhar com mmc e mdc.

Lema 1. *Sejam $a = p_1^{n_1} \cdots p_t^{n_t}$ e $d = p_1^{m_1} \cdots p_t^{m_t}$ inteiros positivos, onde $p_1, \cdots p_t$ são primos positivos e n_i, m_i, $1 \leq i \leq t$ são inteiros não-negativos. Então, $d|a$ se e somente se $m_i \leq n_i$, $1 \leq i \leq t$*

(FALTA TERMINAR)

3 Exs do capítulo 3

3.1 Exs da seção 3.1

Exercício 26 (*)**.** *Resolva as seguintes equações diofantinas e determine em cada caso as soluções positivas:*

i. $2X + 3Y = 9$

ii. $3X + 5Y = 47$

iii. $8X + 7Y = 3$

iv. $47X + 29Y = 999$

3.2 Exs da seção 3.2

Exercício 27. *Determinar o resto das divisões:*

i. De 2^{50} *por* 7*;*

ii. De 41^{65} *por* 7

iii. De $1^5 + 2^5 + \cdots + 100^5$ *por* 4

Exercício 28. *Usar congruências para verificar que:*

i. $89|(2^{44} - 1)$*;*

ii. $97|(2^{48} - 1)$.

3.3 Exs da seção 3.3

Releiam o exercício 7 da lista 4