Lista de Revisão para P2
Álgebra 1 para licenciatura
MAT0120

Os exercícios desta lista não devem ser entregues, eles foram retirados do livro: **Números, Uma Introdução a Matemática**. Aqueles marcados com * são os mais importantes e recomendo que não deixem de fazê-los para estudar.

Nas palavras do professor Eduardo, a prova poderá abranger todo o conteúdo visto até o momento. Portanto, além de recordarem a matéria anterior à P1, devem estudar o capítulo 3 (seções 3.2, 3.3, 3.4, 3.5 e 3.6) e capítulo 4 (seção 4.1 e 4.2). Esta lista conterá exercícios apenas dos capítulos 3 e 4.

A ideia dessa lista é guiar vocês durante os estudos, pontuando o que é mais importante e que vocês não devem deixar passar.

Lembrem-se de que a prova será no dia 21/05 e 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 Exercícios do capítulo 3

1.1 Exs. da seção 3.2

Exercício 1. *Vocês devem ler/fazer a proposição* 3.2.2 *e* 3.2.3. *(Essas duas proposições devem ser bastante naturais para vocês).*

Exercício 2. *Leiam/façam a proposição* 3.2.4. *(Lembrem-se que essa proposição é o mais próximo que temos de uma lei cancelativa em relação a congruência).*

Exercício 3. *(*)(Ex. 5, página 111) Sejam* m_1, m_2 *inteiros relativamente primos e seja a um inteiro arbitrário. Provar que* $a \equiv 0 (mod\ m_1 \cdot m_2)$ *se e*

somente se $a \equiv 0(mod\ m_1)$ *e* $a \equiv 0(mod\ m_2)$*. Mostrar com um exemplo que a hipótese* $mdc(m_1,\ m_2) = 1$ *é essencial.*

Exercício 4. *(Ex. 6, página 111) Provar que* $n^7 \equiv n(mod\ 42)$*, para todo inteiro* n*.*

Exercício 5. *(Ex. 7, página 111) Determinar o resto das divisões:*

1. *De* 41^{65} *por* 7*;*
2. *De* $1^5 + 2^5 + \cdots + 100^5$ *por* 4*.*

Exercício 6. *(*)(Ex. 8, página 111) Usar congruências para verificar que* $23|(2^{11} - 1)$*.*

Exercício 7. *(Ex. 10, página 111) Sejam* $\{a_1, a_2, \cdots, a_n\}$ *um sistema completo de resíduos módulo* n*, e seja* a *um inteiro tal que* $mdc(a, n) = 1$*. Provar que* $\{aa_1, aa_2, \cdots, aa_n\}$ *é um sistema completo de resíduos módulo* n*.*

1.2 Exs. da seção 3.3

Exercício 8. *Leiam/façåm a demonstração das proposições* 3.3.4 *e* 3.3.9*.*

Exercício 9. *(Ex. 1(ii) - página 117) Resolva a seguinte congruência linear:* $5X \equiv 2(mod\ 26)$*.*

Exercício 10. *(*)(Ex. 2 - página 117) Usando congruências, resolva as seguintes equações diofantinas:*

1. $4X + 51Y = 9$*;*
2. $12X + 25Y = 331$*.*

Exercício 11. *(Ex. 3 - página 117) Determinar todas as soluções da congruência linear* $3X - 7Y \equiv 11(mod\ 13)$*.*

1.3 Exs. da seção 3.4

Exercício 12. *Leiam/Façam o teorema* 3.4.4*(Teorema Chinês do Resto). (Lembrem-se de que há um resumo postado no moodle que contem a demonstração com alguns detalhes a mais).*

Exercício 13. *(Ex.1 - página 124) Resolver os seguintes sistemas e congruências lineares:*

1. $X \equiv 1(mod\ 3),\ X \equiv 2(mod\ 5),\ X \equiv 3(mod\ 7)$*;*
2. $X \equiv 5(mod\ 6),\ X \equiv 4(mod\ 11),\ X \equiv 3(mod\ 7)$.

Exercício 14. *(*)(Ex.2 - página 124) Determinar o menor inteiro* $a > 100$ *tal que* $2|a,\ 3|(a+1),\ 4|(a+2),\ 5|(a+3),\ 6|(a+4)$.

Exercício 15. *(Ex.3 - página 125)*

1. *determinar três inteiros consecutivos tais que um deles seja divisível por um quadrado perfeito.*
2. *Determinar três inteiros consecutivos tais que o primeiro seja divisível por por um quadrado, os segundo por um cubo e o terceiro por uma quarta potência.*

Exercício 16. *(Ex. 4 - página 125)*

1. *Provar que as congruências* $X \equiv a(mod\ n)$ *e* $X \equiv b(mod\ m)$ *têm uma solução comum se e somente se* $mdc(m,n)|(a-b)$*. Provar que a solução é única módulo* $mmc(m,n)$.
2. *Mostrar que o sistema de congruências*
   $X \equiv 5(mod\ 6)$
   $X \equiv 7(mod\ 15)$
   não tem solução.

1.4 Exs. da seção 3.5

Exercício 17. *Leiam/façam a demonstração de* 3.5.1*(Teorema de Fermat),* 3.5.4*,* 3.5.8*(Teorema de Euler) e* 3.5.11*(Teorema de Wilson). (Lembrem-se de que há um resumo postado no moodle que contem as demonstrações de todos esses resultados.)*

Exercício 18. *(Ex. 1 - página 133) Seja a um inteiro. Provar que:*

1. $a^{21} \equiv a(mod\ 15)$, $a^7 \equiv a(mod\ 42)$*;*
2. *Se* $mdc(a,35) = 1$*, então* $a^{12} \equiv 1(mod\ 35)$*;*

3. *Se* $mdc(a, 42) = 1$, *então* $3 \cdot 7 \cdot 8 | (a^6 - 1)$.

Exercício 19. *(Ex. 3 - página 133) Sejam* p *um inteiro e* a *e* b *inteiros arbitrários. Provar que, se* $a^p \equiv b^p (mod\ p)$, *então* $a \equiv b (mod\ p)$.

Exercício 20. *(Ex. 7 - página 133)*

1. *Mostrar que* $2^8 \equiv 1 (mod\ 17)$, $2^{16} \equiv 1 (mod\ 17)$ *(consequentemente, dados um inteiro* a *e um primo* p *que não divide* a, $(p-1)$ *não é, em geral, o menor inteiro positivo tal que* $a^{p-1} \equiv 1 (mod\ p)$*). Compare com o Teorema de Fermat.*

Sejam p *um primo e* a *um inteiro tal que* pa. *Provar que:*

2. *Se* $p > 2$, $a^{\frac{p-1}{2}} \equiv 1 (mod\ p)$ *ou* $a^{\frac{p-1}{2}} \equiv -1 (mod\ p)$.
3. *O menor inteiro positivo* e *tal que* $a^e \equiv 1 (mod\ p)$ *é divisor de* $(p-1)$.
4. *Se* e *é o inteiro acima, então todo inteiro* x *tal que* $a^x \equiv 1 (mod\ p)$ *é múltiplo de* e.

Exercício 21. *(Ex. 10 - página 134) Sejam* a, n *inteiros tais que* $mdc(a, n) = mdc(a-1, n) = 1$. *Provar que* $1 + a + \cdots + a^{\phi(n)-1} \equiv 0 (mod\ n)$.

Exercício 22. *(Ex. 12 - página 134) Seja* p *um primo distinto de* 2 *e* 5. *Provar que* p *divide infinitos inteiros na sequência:* $1,\ 11,\ 111,\ 1111, \cdots$.

Exercício 23. *(Ex. 16 - página 134) Seja* p *um inteiro primo. Provar que:*

1. $(p-1)! \equiv (p-1) (mod\ 1 + 2 + \cdots + (p-1))$;
2. *para todo inteiro* a, $p | (a^p + (p-1)!a)$ *e* $p | (p-1)!a^p + a)$;
3. *Se* p *é ímpar, então* $1^2 \cdot 3^2 \cdot 5^2 \cdots (p-1)^2 \equiv (-1)^{\frac{p-1}{2}} (mod\ p)$.

1.5 Exs. da seção 3.6

Exercício 24. *Leiam/façam a demonstração dos resultados* 3.6.2 *e* 3.6.3.

Observação 1. *As propriedades de* $\mathbb{Z}_m$ *devem ser naturais para vocês. Vejam que* $\mathbb{Z}_m$ *é um anel.*

Exercício 25. *Leiam/façam a demonstração dos resultados* 3.6.8 *e* 3.6.13.

Observação 2. *Confiram que se p é primo, $\mathbb{Z}_m$ é um corpo.*

Exercício 26. *(Ex. 2 - página 143) Em $\mathbb{Z}_{20}$, determinar:*

1. *Os menores representantes positivos de $\overline{-10}$ e $\overline{-6}$.*
2. *Todos os divisores de zero*

Exercício 27. *(Ex. 6 - página 146) Provar que o número de elementos inversíveis de $\mathbb{Z}_m$ é $\phi(m)$, em que ϕ indica a função de Euler.*

Exercício 28. *Leiam/façam a demonstração dos teoremas* 3.6.16, 3.6.17 *e* 3.6.18.

Exercício 29. *(Ex. 9 - página 148) sejam p um primo positivo e $\overline{a}$ um elemento de $\mathbb{Z}_p$. Provar que $\overline{a}^p = \overline{a}$.*

Exercício 30. *(Ex. 10 - página 148) Sejam p um primo positivo e $\overline{a}$, $\overline{b}$ elementos de $\mathbb{Z}_p$. Provar que $(\overline{a} + \overline{b})^p = \overline{a}^p + \overline{b}^p$.*

Exercício 31. *(Ex. 12 - página 148) Seja p um primo positivo. Provar que, em $\mathbb{Z}_p$, tem-se que $(\overline{p-1})! = \overline{-1}$*

Exercício 32. *(Ex. 16 - página 149) Resolver as seguintes equações em $\mathbb{Z}_m$:*

1. $\overline{3}X + \overline{2} = \overline{6}X + \overline{7}$, $m = 8$;
2. $(\overline{2}X + \overline{3})^5 + (\overline{3}X + \overline{2})^5 + \overline{5}X = \overline{0}$, $m = 5$;
3. $\overline{4}X - \overline{7} + \overline{6}X + \overline{2} = \overline{3}X + \overline{5}X$, $m = 12$.

Exercício 33. *(*)(Ex. 17 - página 149) Resolver o sistema de equações abaixo em $\mathbb{Z}_{14}$:*
$\overline{2}X - \overline{3}Y = \overline{2}$
$\overline{3}X + \overline{2}Y = \overline{3}$

2 Exs.do capítulo 4

2.1 Exs. da seção 4.1

Antes de iniciarmos com os exs, vamos fazer um pequeno resumo sobre relações de equivalência.

Definição 1. *(Relação) Uma relação (binária) entre dois conjuntos A e B é um subconjunto de $A \times B$.*

Trabalharemos apenas com relações binárias em que $A = B$. Assim, dado um conjunto arbitrário A, indicaremos por R uma relação em A ($R \subset A \times A$) e, para indicar que dois elementos $a,\ b \in A$ estão R-relacionados, ou seja, $(a, b) \in R$, escreveremos aRb.

- Uma relação R tal que para todo $a \in R$ vale aRa, diz-se reflexiva;
- Uma relação tal que para todo par de elementos $a,\ b \in A$, temos que: se aRb então bRa, diz-se simétrica;
- Uma relação R em que para toda terna de elementos $a,\ b,\ c \in A$ tem-se que: se aRb e bRc então aRc, diz-se uma transitiva.

Definição 2. *Uma relação binária em um conjunto A é dita uma relação de equivalência se é simultaneamente reflexiva, simétrica e transitiva.*

É comum usarmos o símbolo $\equiv$ para nos referirmos a uma relação de equivalência. Então, usando essa notação, uma relação binária em A deve satisfazer:

1. $a \equiv a$;
2. $a \equiv b$ implica $b \equiv a$;
3. $a \equiv b$ e $b \equiv a$ implicam $a \equiv c$.

Exemplo 1. *Leiam alguns exemplos das páginas* 152 *e* 153.

Por causa da propriedade transitiva das relações de equivalência, quaisquer elementos que são congruentes a um terceiro, são congruentes entre si, portanto, é interessante tentar agrupá-los em subconjuntos do conjunto onde está definida a relação de equivalência.

Definição 3. *Sejam A um conjunto e $\equiv$ uma relação de equivalência em A. Para cada elemento $a \in A$, chama-se classe de equivalência de a o conjunto*

$$C(a) = \{x \in A : x \equiv a\} \tag{1}$$

Lembre-se de que na seção 3.6 nos já estudamos classes de equivalência quando vimos os anéis $\mathbb{Z}_m$. Note que a congruência módulo m é uma relação de equivalência e cada elemento de $\mathbb{Z}_m$ é uma classe de equivalência.

Teorema 1. *As diferentes classes de equivalência de uma relação de equivalência num conjunto A fornecem uma decomposição de A em subconjuntos mutuamente disjuntos, não-vazios, cuja a união é o conjunto todo, ou seja, as classes de equivalência formam uma partição de A.*

Reciprocamente, dada uma decomposição de A como união de subconjuntos mutuamente disjuntos, não-vazios, podemos definir uma relação de equivalência em A cujas classes sejam, precisamente, os subconjuntos dados.

Antes de fazermos a demonstração, vejamos a seguinte proposição:

Proposição 1. *Seja A um conjunto e $\equiv$ uma relação de equivalência em A. Temos que, para a, $b \in A$, $C(a) \cap C(b) = \emptyset$ se, e somente se, $C(a) \neq C(b)$.*

Demonstração. Considere que $c(a) \cap C(b) \neq \emptyset$, então existe $x \in A$ tal que $x \in C(a)$ e $x \in C(b)$, logo $x \equiv a$ e $x \equiv b$. Pela transitividade e simetria da relação de equivalência, $a \equiv b$. Não é difícil ver que $c(a) = C(B)$ (fizemos algo parecido na proposição 3.6.2).

A outra implicação é mais simples.

□

Demonstração. (Teorema 1) Inicialmente, vamos mostrar que dada uma relação de equivalência, as classes de equivalência determinam uma partição. Seja $a \in A$, veja que $a \in C(a)$, então $C(a) \neq 0$.

Observe que se $a \in A$ então como $a \in C(a)$, temos que $A \subset \bigcup_{a \in A} C(a)$. Por outro lado, se $x \in \bigcup_{a \in A} C(a)$, como $C(a) \subset A$, segue que $x \in A$ e, portanto $A = \bigcup_{a \in A} C(a)$.

Por último, vemos que as classes são disjuntas usando a proposição anterior.

Reciprocamente, consideremos $\{A_i\}_{i \in I}$ uma partição de A. Defina a relação R de modo que aRb se e somente se existe $j \in I$ tal que $a,\ b \in A_j$. Deixo a vocês a tarefa de provar que essa relação é reflexiva, simétrica e transitiva, portanto, R é uma relação de equivalência.

□

Veja que, rigorosamente, há um abuso de notação na demostração acima quando dizemos que $A = \bigcup_{a \in A} C(a)$. Na realidade queremos dizer que A é a união das classes distintas.

Definição 4. *Chamamos conjunto quociente de A por $\equiv$ o conjunto formado por todas as clsses de equivalência determinadas pela relação $\equiv$ no conjunto A. Em símbolos,*

$$A/\equiv = \{C(a) : a \in A\} \tag{2}$$

Exercício 34. *sejam A e B conjuntos e $f : A \to B$ uma função. Definimos uma relação em A da seguinte amaneira: dados a, $a' \in A$, dizemos que aRa' se e somente se $f(a) = f(a')$. Provar que R é uma relação de equivalência.*

Exercício 35. *Seja R uma relação em um conjunto M, verificando:*

1. *se aRb então bRa;*
2. *se aRb e bRc então aRc;*
3. *Para todo $a \in M$, existe $b \in M$ tal que aRb*

Provar que R é uma relação de equivalência.

3 Extra - função de Euler

Como não tive muito tempo para trabalhar com vocês sobre a função ϕ de Euler nas monitorias, deixo aqui um link onde podem encontrar algumas propriedades dessa função e alguns exs para quem se interessar. `https://www.whitman.edu/mathematics/higher_math_online/section03.08.html`.