TEORIA DOS NÚMEROS

LICENCIATURA EM MATEMÁTICA

Ministério da Educação - MEC
Coordenação de Aperfeiçoamento de Pessoal de Nível Superior
Universidade Aberta do Brasil
Instituto Federal de Educação, Ciência e Tecnologia do Ceará

MINISTÉRIO DA EDUCAÇÃO
Universidade Aberta do Brasil
Instituto Federal de Educação, Ciência e Tecnologia do Ceará
Diretoria de Educação a Distância

Licenciatura em Matemática

Teoria dos Números

Jânio Kléo de Sousa Castro

Fortaleza, CE
2010

CRÉDITOS

Presidente
Luiz Inácio Lula da Silva

Ministro da Educação
Fernando Haddad

Secretário da SEED
Carlos Eduardo Bielschowsky

Diretor de Educação a Distância
Celso Costa

Reitor do IFCE
Cláudio Ricardo Gomes de Lima

Pró-Reitor de Ensino
Gilmar Lopes Ribeiro

Diretora de EAD/IFCE e Coordenadora UAB/IFCE
Cassandra Ribeiro Joye

Vice-Coordenadora UAB
Régia Talina Silva Araújo

Coordenador do Curso de Tecnologia em Hotelaria
José Solon Sales e Silva

Coordenador do Curso de Licenciatura em Matemática
Zelalber Gondim Guimarães

Elaboração do conteúdo
Jânio Kléo de Sousa Castro

Colaborador
Lívia Maria de Lima Santiago

Equipe Pedagógica e Design Instrucional
Ana Claúdia Uchôa Araújo
Andréa Maria Rocha Rodrigues
Cristiane Borges Braga
Eliana Moreira de Oliveira
Gina Maria Porto de Aguiar Vieira
Iraci Moraes Schmidlin
Jane Fontes Guedes
Jivago Silva Araújo
Karine Nascimento Portela
Lívia Maria de Lima Santiago
Luciana Andrade Rodrigues
Maria Irene Silva de Moura
Maria Vanda Silvino da Silva
Marília Maia Moreira
Regina Santos Young

Equipe Arte, Criação e Produção Visual
Ábner Di Cavalcanti Medeiros
Benghson da Silveira Dantas
Davi Jucimon Monteiro
Diemano Bruno Lima Nóbrega
Germano José Barros Pinheiro
Gilvandenys Leite Sales Júnior
Hommel Almeida de Barros Lima
José Albério Beserra
José Stelio Sampaio Bastos Neto
Larissa Miranda Cunha
Marco Augusto M. Oliveira Júnior
Navar de Medeiros Mendonça e Nascimento
Roland Gabriel Nogueira Molina

Equipe Web
Aline Mariana Bispo de Lima
Benghson da Silveira Dantas
Fabrice Marc Joye
Igor Flávio Simões de Sousa
Luiz Bezerra de Andrade FIlho
Lucas do Amaral Saboya
Marcos do Nascimento Portela
Ricardo Werlang
Samantha Onofre Lóssio
Tibério Bezerra Soares
Thuan Saraiva Nabuco

Revisão Textual
Aurea Suely Zavam
Nukácia Meyre Araújo de Almeida

Revisão Web
Débora Liberato Arruda Hissa
Saulo Garcia

Logística
Francisco Roberto Dias de Aguiar
Virgínia Ferreira Moreira

Secretários
Breno Giovanni Silva Araújo
Francisca Venâncio da Silva

Auxiliar
Bernardo Matias de Carvalho
Carla Anaíle Moreira de Oliveira
Maria Tatiana Gomes da Silva
Wagner Souto Fernandes
Zuila Sâmea Vieira de Araújo

Catalogação na Fonte: Islânia Fernandes Araújo CRB 3/917

C355t Castro, Jânio Kléo Sousa.

Teoria dos números / Jânio Kléo Sousa de Castro; Coordenação Cassandra Ribeiro Joye - Fortaleza: UAB/IFCE, 2010.
112p. : il. ; 27cm.

ISBN 978-85-63953-22-3

1. CONGRUÊNCIA 2. DIVISIBILIDADE 3. NÚMEROS PRIMOS. I. Joye, Cassandra Ribeiro. (Coord.) II. Instituto Federal de Educação, Ciência e Tecnologia do Ceará - IFCE III. Universidade Aberta do Brasil – UAB. IV. Título.

CDD – 512.70785

SUMÁRIO

APRESENTAÇÃO

Caro (a) aluno (a), no texto que segue temos a apresentação de algumas propriedades aritméticas dos números inteiros, especialmente aquelas referentes ao algoritmo da divisão.

Como pré-requisito para a sua leitura, recomenda-se alguma familiaridade com as operações aritméticas fundamentais - adição e multiplicação.

Os dois primeiros capítulos tratam dos divisores e dos múltiplos de um número inteiro, com enfoque nos números primos, e apresentamos a noção de congruência, aprofundada no terceiro capítulo.

As funções aritméticas m, s, t e f são estudadas nos dois capítulos seguintes, nos quais há exemplos computacionais e relações entre elas.

O princípio de Dirichlet (ou das gavetas) é abordado no sexto capítulo.

No penúltimo capítulo, estudamos os resíduos quadráticos, com ênfase no uso do símbolo de Legendre e da lei da reciprocidade quadrática, com a qual encerramos a teoria contida neste material.

O último capítulo apresenta uma miscelânea de exercícios sobre os diversos assuntos abordados. De posse deste livro, este último capítulo pode (e deve) ser consultado a qualquer momento, para melhor fixação da teoria.

Desejando a todos um bom proveito na leitura e um bom aprendizado, só resta começar o trabalho.

Jânio Kléo

AULA 1

Divisores de um número

Olá, a todos.

Em nossa primeira aula de Teoria dos Números, estudaremos o processo de divisão de números inteiros, detalhando e justificando suas principais propriedades. Alguns dos assuntos são nossos conhecidos de longa data, pois trataremos do conjunto $\mathbb{Z}$ e das operações de soma e multiplicação. Além de acompanhar os exemplos fornecidos neste texto, não hesite em fazer testes para a verificação das propriedades e melhor assimilação das definições.

Objetivos

- Definir os principais termos da Teoria dos Números
- Analisar a divisão de números inteiros e os algoritmos correlatos

TÓPICO 1

Divisibilidade

OBJETIVOS

- Identificar as principais definições sobre os números inteiros e suas consequências
- Estabelecer o conceito de divisibilidade e as relações entre os divisores de um número inteiro

A Teoria dos Números, do ponto de vista clássico, trata principalmente do conjunto dos números inteiros, denotado por $\mathbb{Z}$, que compreende todos os números naturais positivos, o zero e seus simétricos.

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, 3, \ldots\}$$

Para dois números inteiros a e b, são definidas as operações de soma, representada *infixamente* por $a+b$, e de multiplicação (ou produto), representada por $a.b$ ou simplesmente ab, que satisfazem as seguintes propriedades:

1. $\forall a, b \in \mathbb{Z}$, vale $a+b=b+a$	(a soma é comutativa)
2. $\forall a, b, c \in \mathbb{Z}$, vale $(a+b)+c=a+(b+c)$	(a soma é associativa)
3. $\forall a \in \mathbb{Z}$, vale $a+0=a$	(existe um elemento neutro para a soma)
4. $\forall a \in \mathbb{Z}, \exists(-a) \in \mathbb{Z}$, tal que $a+(-a)=0$	(todo elemento possui inverso para a soma)
5. $\forall a, b \in \mathbb{Z}$, vale $ab=ba$	(a multiplicação é comutativa)
6. $\forall a, b, c \in \mathbb{Z}$, vale $(ab)c=a(bc)$	(a multiplicação é associativa)
7. $\forall a \in \mathbb{Z}$, vale $a.1=a$	(existe um elemento neutro para a multiplicação)
8. $\forall a, b, c \in \mathbb{Z}$, vale $a(b+c)=ab+ac$	(a multiplicação é distributiva em relação à soma)

Por causa da associatividade, podemos fazer a soma de qualquer quantidade finita de inteiros agrupando-os em qualquer ordem e, assim, os parênteses serão opcionais nesse caso, bem como no produto de uma sequência finita de inteiros.

Aqui temos a relação de ordem:
$\ldots < -2 < -1 < 0 < 1 < 2 < 3 < \ldots$, na qual entre dois números listados consecutivamente não há nenhum número inteiro.

É relevante observar que $\mathbb{Z}$ não é limitado superiormente, ou seja, $\mathbb{Z}$ não possui um elemento máximo, bem como não é limitado inferiormente, pois não possui um elemento mínimo.

ATENÇÃO!

Observação: A um conjunto com operações de soma e multiplicação que satisfazem as propriedades (1), (2), (3), (4), (6) e (8) damos o nome de anel; caso a propriedade (5) seja satisfeita, o anel é dito comutativo. Se (7) é satisfeita, dizemos que o anel possui identidade. O conjunto dos números inteiros é, portanto, um anel comutativo com identidade.

Além disso, se $a < b$, então $a + c < b + c, \forall c \in \mathbb{Z}$ e $ac < bc, \forall c > 0$.

EXEMPLO 1

Mostre que não existe o inverso multiplicativo do número 2.

Solução:

Suponha que exista $a \in \mathbb{Z}$ tal que $2.a = 1$. Por um lado, este número deve ser maior que 0, pois, se $a \leq 0$, teríamos $1 = 2a \leq 2.0 = 0$, ou seja, $1 \leq 0$, que é falso. Da mesma forma, se $a \geq 1$, teríamos $1 = 2a \geq 2.1 = 2$, ou seja, $1 \geq 2$, que é falso, de onde concluímos que $a < 1$. Assim, deveríamos ter $a > 0$ e $a < 1$, mas sabemos que tal inteiro não existe. Logo 2 não possui inverso multiplicativo.

O mesmo raciocínio do exemplo acima pode ser aplicado para mostrar que os únicos números inteiros que possuem inverso multiplicativo em $\mathbb{Z}$ são 1 e –1. A estes números damos o nome de unidades e denotaremos por $U(\mathbb{Z})$. Assim definimos $U(\mathbb{Z}) = \{n \in \mathbb{Z}; \exists m \in \mathbb{Z}, mn = 1\}$ e vale $U(\mathbb{Z}) = \{-1, 1\}$.

Passemos à definição central desta aula.

Definição 1: Dados os números inteiros a e b, dizemos que a divide b (representamos por $a \mid b$) se existir um inteiro n tal que $b = a.n$. Ou seja:
$a \mid b \Leftrightarrow \exists n \in \mathbb{Z}; b = an$.
Quando $a \mid b$, dizemos também que a é um *divisor* de b ou, equivalentemente, que b é um *múltiplo* de a.

EXEMPLO 2A

Como $30 = 5.6$, podemos dizer que $5 \mid 30$ e $6 \mid 30$, ou seja, 5 e 6 são divisores de 30.

ATENÇÃO!

Embora saibamos de antemão que o inverso do número 2 é o número 1/2, que não é inteiro, esse conhecimento prévio não deve ser tomado como imediato, pois envolve, na maioria dos casos, teorias mais elaboradas, como o estudo dos números racionais. Devemos, assim, tomar cuidado com o que parecer óbvio e tentar provar usando apenas as propriedades de cada objeto que estivermos analisando.

EXEMPLO 2B

Podemos usar uma ideia semelhante à do exemplo 1 para mostrar que não existe nenhum inteiro n para o qual $5n = 12$ (tente repetir o processo de modo a demonstrar isso). Assim sendo, 5 não divide 12, o que pode ser representado por $5 \nmid 12$, isto é, 12 não é um múltiplo de 5.

Proposição 1: A divisibilidade é uma relação transitiva, ou seja, se $a \mid b$ e $b \mid c$, então $a \mid c$.
Demonstração: Se $a \mid b$, então $b = an_1$. Se $b \mid c$, então $c = bn_2 = an_1n_2$, logo $a \mid c$.

Proposição 2: Se $a \mid b$ e $b \mid a$, então $a = b$ ou $a = -b$.
Demonstração: Se $a \mid b$, então $b = an_1$. Se $b \mid a$, então $a = bn_2 = an_1n_2$, logo $n_1n_2 = 1$, o que somente ocorre se $n_1 = n_2 = 1$, caso em que $a = b$, ou $n_1 = n_2 = -1$, caso em que temos $a = -b$.

Proposição 3: Se $a \mid b$ e $c \in \mathbb{Z}$, com $c \neq 0$, então $ac \mid bc$.
Demonstração: Se $a \mid b$, então $b = an$. Multiplicando esta igualdade por $c \in \mathbb{Z}$, temos $bc = acn$, logo $ac \mid bc$.

Proposição 4: Se $a \mid b$ e $a \mid c$, então $a \mid b + c$.
Demonstração: Se $a \mid b$ e $a \mid c$, então existem inteiros m e n para os quais $b = am$ e $c = an$. Assim, $b + c = am + an = a(m + n)$, logo $a \mid b + c$.

Observação 1: Como recurso extra para o entendimento da expressão $a \mid b + c$, poderíamos usar parênteses e escrever $a \mid (b + c)$, entretanto a ausência

deles não gera nenhuma ambiguidade, pois a expressão $(a \mid b) + c$ não tem sentido definido.

Observação 2: Como consequência direta das duas últimas proposições, se $a \mid b$ e $a \mid c$, então $a \mid mb + nc$ para quaisquer inteiros m e n.

A respeito dos divisores de um número, valem também as seguintes propriedades, que são consequências diretas da definição e cujas demonstrações são sugeridas como exercício.

1) $1 \mid a$, $a \mid a$ e $a \mid 0$, para qualquer inteiro a;

2) se $ab \mid ac$ e $a \neq 0$, então $b \mid c$;

3) se $a \mid b$, então $a \mid -b$, $-a \mid b$ e $-a \mid -b$;

4) se $a \mid b$ e $b \neq 0$, então $|a| \leq |b|$;

5) se $a \mid b$, então $c = \dfrac{b}{a}$ é inteiro e $c \mid b$.

Uma das implicações da propriedade 4 é que o conjunto de divisores inteiros de um número não nulo é limitado e, por isso, finito. Como resultado da propriedade 3, a quantidade de divisores inteiros de um número não nulo é sempre par, já que sempre virão aos pares cada divisor e seu simétrico. Assim, basta conhecermos apenas os divisores inteiros *positivos* de um número, pois os negativos estarão automaticamente determinados. Denotaremos, então, por $D(n)$ o conjunto de divisores inteiros positivos do número n, ou seja, $D(n) = \{m \in \mathbb{Z}_+ ; m \mid n\}$.

EXEMPLO 3

Fazendo testes com os inteiros positivos de 1 a 8, vemos que $D(8) = \{1, 2, 4, 8\}$. Assim, os divisores inteiros de 8 são ± 1, ± 2, ± 4 e ± 8.

Definição 2: O número inteiro n é *par* se $2 \mid n$ e é *ímpar*, caso contrário.

ATENÇÃO!

Pela transitividade da relação de divisibilidade, verifica-se facilmente que se $a \mid b$, então $D(a) \subset D(b)$.

Durante nossa primeira aula, estudaremos métodos que, entre outras coisas, nos fornecerão a quantidade de divisores positivos de um número inteiro. Antes disso, observe o seguinte exemplo prático de como *construir* o conjunto $D(n)$, usando principalmente a propriedade 5, indicada acima.

EXEMPLO 4A

Escreva o conjunto de divisores positivos do número 60.

Solução:

De princípio, sabemos que 1 e 60 devem entrar na lista, pois cada número inteiro tem pelo menos dois divisores positivos. Uma vez que podemos escrever 60 = 2.30, podemos afirmar que $2 \mid 60$ (60 é par) e, pelo mesmo motivo, $30 \mid 60$. Como não há nenhum inteiro entre 1 e 2, não há nenhum divisor inteiro de 60 entre 30 e 60. Assim, os demais divisores estão entre 2 e 30. Fazendo testes semelhantes aos do primeiro exemplo, concluímos que 60 = 3.20. Assim, $3 \in D(60)$ e $20 \in D(60)$, e não há números entre 20 e 30 a serem considerados. Continuando assim entre 3 e 20, o próximo divisor de 60 é o número 4, pois 60 = 4.15. Entre 4 e 15, o próximo divisor de 60 é o número 5, pois 60 = 5.12. Entre 5 e 12, o próximo divisor de 60 é 6, pois 60 = 6.10. Por fim, testando os números entre 6 e 10, não encontramos nenhum divisor de 60 e encerramos a lista. $D(60) = \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$.

EXEMPLO 4B

Realizando processo semelhante, podemos concluir que $D(28) = \{1, 2, 4, 7, 14, 28\}$ e $D(11) = \{1, 11\}$.

Observação 3: Se os números inteiros positivos a e b são tais que $a \mid b$, com $a \neq 1$ e $a \neq b$, dizemos que a é um *divisor próprio* de b. Assim, no exemplo anterior, os divisores próprios de 60 são 2, 3, 4, 5, 6, 10, 12, 15, 20 e 30, e o número 11 não tem divisores próprios.

Observação 4: Para qualquer inteiro positivo n, o teste com os divisores só é necessário para os números menores ou iguais a $\sqrt{n}$ por causa da propriedade 5.

Uma vez que sabemos construir o conjunto dos divisores inteiros positivos de um número, é ainda mais simples construir o conjunto dos divisores de um dos seus divisores. Do que obtivemos no exemplo 4a, ficaria bem simples encontrar os divisores de 30 ou de 15. Pelo resto de nossa aula, teremos a relação de divisibilidade como objeto relevante, acrescentando novas ferramentas e aprofundando com consequências interessantes.

TÓPICO 2

Números primos

Objetivos

- Definir número primo e estudar suas propriedades
- Descrever o crivo de Erastótenes

Quando analisamos os divisores de um número, encontramos maneiras de fatorá-los, ou seja, de escrevê-los como produto de outros números, por exemplo escrevemos 60 da forma 2.30. Obviamente, podemos também fazer 60 = 1.60, que pode ser chamada de fatoração trivial. Neste tópico, estudaremos especificamente os números que não podem ser fatorados de maneira não trivial que não podem ser escritos como produtos de fatores menores. Começaremos com a definição central a seguir:

Definição 3: Um número inteiro $p>1$ é dito primo se sempre que $p|ab$ obtivermos $p|a$ ou $p|b$.

Guarde bem esta definição, pois ela será revisitada em outros cursos, como o de Estruturas Algébricas, nos quais se estudam outros conjuntos dentro dos quais a ideia de elemento primo também é relevante. Para números inteiros, podemos trabalhar com uma definição equivalente, como a que segue.

Suponha que o número inteiro positivo d seja um divisor do número primo $p>1$, ou seja, que $p=dn$, para algum inteiro positivo n. Assim, os números $a=d^2$ e $b=n^2$ são tais que $ab=d^2n^2=(dn)^2=(dn)(dn)=p.p$, logo $p|ab$. Pela definição de número primo, temos $p|a$ ou $p|b$. Uma vez que $p|a$ equivale a

$p \mid d^2$, significa que $p \mid d$, mas, como $d \mid p$ e são ambos positivos, concluímos que $d = p$ e $n = 1$. A outra alternativa seria $p \mid b$, que equivale a $p \mid n^2$, logo $p \mid n$, mas, como $n \mid p$, concluímos que $n = p$ e $d = 1$. Aqui demonstramos que, se é primo, um número possui exatamente dois divisores positivos. A recíproca dessa afirmação é verdadeira e sua demonstração é deixada como exercício.

Assim, obtemos que $p > 1$ é primo se, e somente se $D(p) = \{1, p\}$, ou seja, um número maior que 1 é primo quando não possui divisores próprios ou ainda quando possui exatamente dois divisores positivos.

EXEMPLO 5

Analisando os dados do exemplo 4, vemos que 60 não é primo, pois o conjunto de seus divisores próprios é não vazio. O número 28 é múltiplo de 2, logo não é primo, enquanto 11 possui exatamente 2 divisores positivos, sendo, portanto, primo.

GUARDE BEM ISSO!

1. Se o número inteiro positivo $n > 1$ não é primo, dizemos que ele é composto, pois ele pode ser escrito como produto de dois números menores que ele.
2. Todo número composto tem pelo menos um número primo como divisor (veremos a demonstração ainda nesta aula).
3. Os números 0 e 1 não são primos nem compostos, por definição.

Os números primos funcionam como os átomos dos números inteiros positivos, pois, como veremos adiante, todo número inteiro positivo pode ser escrito como produto de números primos e, igualmente importante, essa *decomposição* é feita de maneira única.

Como a quantidade de divisores de um número inteiro positivo é finita, poderíamos nos perguntar qual o maior número primo que existe. Uma investigação mais apurada nos levaria a uma resposta interessante: não há um maior número primo! Acompanhe o seguinte raciocínio: se houvesse um maior número primo, isso significaria que a quantidade deles é finita. Seja, então, o conjunto $P = \{p_1, p_2, ..., p_k\}$ de "todos" os números primos. Dessa forma, considere o número inteiro $n = p_1 p_2 ... p_k + 1$, que é maior que qualquer elemento de P, logo $n \notin P$. Além disso, vemos que $p_i \nmid n$, para todo $i = 1, ..., k$, de onde obtemos que n não possuiria nenhum divisor primo, o que é uma contradição, visto que $n > 1$. Assim, a suposição de que há uma quantidade finita de números primos é incorreta. Podemos, então, enunciar o resultado:

Proposição 5: Existem infinitos números primos.

Se testarmos alguns dos números inteiros positivos maiores que 1 para sabermos seus divisores e determinarmos se eles são primos, podemos concluir que os primeiros cinco números primos são 2, 3, 5, 7 e 11. Já que a quantidade de números primos é infinita, poderíamos investigar como eles estão distribuídos ou quantos deles são menores que um número fixado.

Há um algoritmo, conhecido como *crivo de Eratóstenes* (matemático e geógrafo grego nascido no século III a.C.), que lista os números primos menores que n. Pelo observado anteriormente, os divisores devem ser procurados apenas até (no máximo) $\sqrt{n}$.

Observe como funciona o crivo de Erastótenes para $n = 60$. Inicialmente, vejamos que $\sqrt{60} \cong 7{,}7$. Assim, o processo de busca de divisores próprios dos números da lista será encerrado no 7. Comecemos listando os números inteiros positivos de 1 a 60, e "riscamos" o 1, que não é primo. O primeiro número não marcado é o 2, que é primo, destaquemos por colchetes.

~~1~~	[2]	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60

Em seguida, eliminamos todos os múltiplos seguintes de 2, pois eles não são primos.

~~1~~	[2]	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~
11	~~12~~	13	~~14~~	15	~~16~~	17	~~18~~	19	~~20~~
21	~~22~~	23	~~24~~	25	~~26~~	27	~~28~~	29	~~30~~
31	~~32~~	33	~~34~~	35	~~36~~	37	~~38~~	39	~~40~~
41	~~42~~	43	~~44~~	45	~~46~~	47	~~48~~	49	~~50~~
51	~~52~~	53	~~54~~	55	~~56~~	57	~~58~~	59	~~60~~

O primeiro número não marcado foi o 3 e como ele não tem divisores primos menores que ele, ele é primo. Em seguida, eliminamos os múltiplos de 3 (basta contar "de três em três").

~~1~~	[2]	[3]	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	25	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	35	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	49	~~50~~
~~51~~	~~52~~	53	~~54~~	55	~~56~~	~~57~~	~~58~~	59	~~60~~

O primeiro número não marcado foi o 5 e como ele não tem divisores primos menores que ele, ele é primo. Em seguida, eliminamos os múltiplos de 5.

~~1~~	[2]	[3]	~~4~~	[5]	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	49	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~

O primeiro número não marcado foi o 7 e como ele não tem divisores primos menores que ele, ele é primo. Em seguida, eliminamos os múltiplos de 7. E como é o último do teste, os que sobrarem sem marcação, são números primos.

~~1~~	[2]	[3]	~~4~~	[5]	~~6~~	[7]	~~8~~	~~9~~	~~10~~
[11]	~~12~~	[13]	~~14~~	~~15~~	~~16~~	[17]	~~18~~	[19]	~~20~~
~~21~~	~~22~~	[23]	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	[29]	~~30~~
[31]	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	[37]	~~38~~	~~39~~	~~40~~
[41]	~~42~~	[43]	~~44~~	~~45~~	~~46~~	[47]	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	[53]	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	[59]	~~60~~

Assim, os números primos menores que 60 são 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53 e 59.

O crivo de Eratóstenes pode ser usado para qualquer valor de n, obviamente exigindo trabalho crescente. Muitos trabalhos atuais são feitos com testes de primalidade, alguns demandando esforços computacionais muito grandes. Máquinas modernas trabalham neste intuito e o maior número primo conhecido é $2^{43112698}-1$, que em notação decimal tem quase treze mil algarismos e foi descoberto em 2008.

SAIBA MAIS!

No site http://www.ahistoria.com.br/eratostenes/ você pode conhecer um pouco mais sobre Eratóstenes e algumas de suas obras.

EXEMPLO 6

Mostre que a equação $n^3-4n^2-59=0$ não possui raízes inteiras.

Solução:

A equação dada é equivalente a $n^3-4n^2=59$, ou ainda $n^2(n-4)=59$. Assim $n^2 \mid 59$. Como 59 é primo, seus únicos divisores positivos são 1 e 59. Como $n^2 \neq 59$, para todo n inteiro, a alternativa seria $n^2=1$, que resulta em $n=\pm 1$. Entretanto, por substituição direta, vemos que nenhum desses valores é raiz da equação dada. Assim, ela não possui raízes inteiras.

Vale ressaltar que 2 é o único número primo par, pois todos os demais números pares têm pelo menos o 2 como divisor próprio. Assim, todo número primo maior que 2 é ímpar, mas nem todo número ímpar é primo, como bem ilustra o número 9.

Conhecer os números primos e suas propriedades é, de certa forma, conhecer todos os números inteiros. Dessa forma, é razoável que conheçamos pelo menos os primeiros números primos de cor. A tabela obtida no exemplo do crivo de Eratóstenes é um bom modo de fixar essas ideias. Entretanto, como parte fundamental da teoria dos números inteiros, há muito ainda o que se ver sobre os números primos, e isso se dará nos próximos tópicos.

TÓPICO 3

Divisão de inteiros e o algoritmo de Euclides

OBJETIVOS

- Definir quociente e resto na divisão de inteiros
- Destacar as propriedades do máximo divisor comum
- Estudar métodos de inferência sobre o conjunto solução das equações diofantinas

Nos tópicos anteriores, vimos como determinar se $a \mid b$, ou seja, se existe $c \in \mathbb{Z}$ tal que $b = ac$. Nesse caso dizemos que b é um múltiplo de a. Agora veremos o algoritmo da divisão, suas consequências e principais propriedades. Inicialmente, veja que, da mesma forma que definimos o conjunto dos divisores positivos de um número, podemos definir o conjunto dos *múltiplos positivos* de um número, o qual denotaremos por $M(n)$, ou seja, $M(n) = \{m \in \mathbb{Z}_+^* ; n \mid m\}$.

De imediato verificamos que os múltiplos positivos do número inteiro positivo n são $1.n$, $2.n$, $3.n$, $4.n$, ... Logo, concluímos simplesmente que são infinitos. Entretanto, fixado o número inteiro $a > 0$, o conjunto $\{m \in M(n); m \leq a\} \cup \{0\}$, dos múltiplos não-negativos de n que são menores ou iguais a a, é limitado superiormente e não-vazio, e assume, portanto, um máximo. Seja m_0 este máximo. Como m_0 é um múltiplo de n, podemos escrever $m_0 = qn$, para algum inteiro positivo q. Necessariamente é válido que $a - m_0 < n$, pois, do contrário, perderíamos a maximalidade de m_0. Se escrevermos $r = a - qn$, podemos, então, enunciar o seguinte resultado:

Dados os números inteiros positivos a e n, existem números inteiros q e r, chamados respectivamente de *quociente* e *resto* da divisão, tais que

$$a = qn + r \text{ e } 0 \leq r < n.$$

Assim, *dividir* a (chamado de dividendo) por n (o divisor) consiste em encontrar o quociente e o resto que satisfazem a propriedade desejada. Aqui usamos o artigo definido porque tanto quociente quanto resto são unicamente determinados, como provado a seguir.

Proposição 6: O quociente e o resto da divisão entre os inteiros positivos a e n são únicos.

Demonstração: Suponha que haja inteiros q_1, q_2 e r_1, r_2 tais que $a = q_1 n + r_1$ e $a = q_2 n + r_2$ e $0 \leq r_1, r_2 < n$. Dessa última desigualdade, fazemos $r_2 < n \Rightarrow r_2 - r_1 < n - r_1 \leq n$, ou seja, $r_2 - r_1 < n$. Analogamente, pode-se demonstrar que $-n < r_2 - r_1$. Das igualdades acima, podemos inferir $q_1 n + r_1 = q_2 n + r_2 \Rightarrow (q_1 - q_2)n = r_2 - r_1$, com base na qual podemos afirmar que $n \mid r_2 - r_1$. Mas como $-n < r_2 - r_1 < n$, a única possibilidade é $r_2 - r_1 = 0$, isto é, o resto é único e, assim, o quociente também é único, como se pode verificar da igualdade $(q_1 - q_2)n = r_2 - r_1 = 0$.

EXEMPLO 1A

Uma vez que podemos escrever 13 = 5.2 + 3 e 3 < 5, podemos dizer que a divisão de 13 por 5 apresenta quociente 2 e resto 3.

EXEMPLO 1B

É verdade que 27 = 4.5 + 7, mas não podemos dizer que a divisão de 27 por 4 gera quociente 5 e resto 7, pois 7 não é menor que 4. Da mesma maneira, embora 27 = 4.7 + (–1), o resto não pode por ser negativo. Na divisão de 27 por 4, o quociente vale 6 e o resto vale 3.

EXEMPLO 1C

Como 30 = 6.5, o quociente e o resto da divisão de 30 por 6 valem 5 e 0, respectivamente.

Observação: Embora a definição acima tenha sido estabelecida para números inteiros positivos, o processo pode ser, com pequenas adaptações, estendido para números inteiros quaisquer desde que o divisor seja diferente de zero. Quando o divisor for negativo, exigiremos para o resto que ele seja menor que o valor absoluto do divisor. Assim, fazendo a divisão de 33 por –5, o quociente é –7 e o resto é 2, pois 33 = (–5).(–7) + 2 e $0 \leq 2 < |-5|$.

Pelo que definimos anteriormente, é imediato que, quando $a \mid b$, o resto da divisão de b por a é 0, caso em que dizemos que a divisão é *exata*.

Definição 4: Dados os números inteiros positivos a e b, dizemos que o número $d \in \mathbb{Z}_+$ é o *máximo divisor comum* entre a e b, e escrevemos $d = (a,b)$, quando:

(i) $d \mid a$ e $d \mid b$, ou seja, $d \in D(a) \cap D(b)$;

(ii) se $d_1 \mid a$ e $d_1 \mid b$, então $d_1 \mid d$, ou seja, d é o maior número com a propriedade (i).

Quando $(a,b) = 1$, dizemos que a e b são *relativamente primos* ou *primos entre si*.

EXEMPLO 2A

Como $D(60) = \{1,2,3,4,5,6,10,12,15,20,30,60\}$ e $D(28) = \{1,2,4,7,14,28\}$, temos $D(60) \cap D(28) = \{1,2,4\}$ e, assim, $(60,28) = 4$.

EXEMPLO 2B

Como $D(16) = \{1,2,4,8,16\}$ e $D(27) = \{1,3,9,27\}$, temos $(16,27) = 1$ e, assim, 16 e 27 são relativamente primos, embora nenhum deles seja um número primo.

Vale ressaltar que, como o número 1 é divisor de qualquer inteiro, o conjunto dos divisores comuns a dois inteiros positivos nunca é vazio e é limitado por a e b, logo possui um elemento máximo. Podemos, assim, concluir que sempre existe (a,b). Vejamos, então, como determinar o máximo divisor comum entre dois números inteiros sem ter que listar todos os divisores de ambos.

Decorre diretamente da definição que se $a \mid b$, então $(a,b) = a$ e não há o que fazer. Caso isso não aconteça, considere $a > b$, divida a por b e obtenha um resto r.

Proposição 7: Se r é o resto da divisão de a por b, então $(a,b) = (b,r)$.

Demonstração: Fazendo $d = (a,b)$, temos que d é divisor de a e de b,

logo podemos escrever $a = dq_1$ e $b = dq_2$. Como r é o resto da divisão de a por b, podemos escrever $a = bq + r$, ou seja, $r = a - bq = dq_1 - dq_2q = d(q_1 - qq_2)$. Desse modo, temos que d é um divisor de r.

Agora considere $d_0 = (b,r)$. Como d é divisor de b e de r, temos, pela condição (ii) da definição, que d é divisor de d_0. Se mostrarmos que que d_0 é divisor de d, teremos a igualdade que completa a prova.

Como d_0 é divisor de b e de r, podemos escrever $b = d_0q_3$ e $r = d_0q_4$ e, fazendo as devidas substituições, temos: $a = bq + r = d_0q_3q + d_0q_4 = d_0(q_3q + q_4)$. Assim, d_0 é divisor de a e, como já era divisor de b, temos que d_0 é divisor de d. Dessa forma, d é divisor de d_0, e d_0 é divisor de d. Chegamos, então, à conclusão de que são iguais, ou seja $(a,b) = (b,r)$.

A proposição anterior apenas transfere o problema de determinar o máximo divisor comum entre os números a e b para encontrar o máximo divisor comum entre b e r, o resto da divisão de a por b, mas com a vantagem de que os números envolvidos são menores. Se $r \mid b$, vale dizer que $(b,r) = r$, e o processo, então, se encerra. Caso contrário, repetimos este passo: se r_2 for o resto da divisão de b por r, temos $(b,r) = (r,r_2)$, e assim sucessivamente até que encontremos uma divisão exata, caso em que o divisor será o máximo divisor comum entre os números iniciais.

O processo descrito é conhecido como *Algoritmo de Euclides*.

EXEMPLO 3A

Determine o máximo divisor entre 60 e 28.

Solução:

Comecemos dividindo 60 por 28; obtemos quociente 2 e resto 4. Assim $(60,28) = (28,4)$ e como $4 \mid 28$, vale $(28,4) = 4$, ou seja $(60,28) = 4$.

EXEMPLO 3B

Determine o máximo divisor comum entre 129 e 45.

Solução:

Observe que 129 = 45.2 + 39, assim transferimos o problema para os números 45 e 39. Mas 45 = 39.1 + 6, e o problema passa para 39 e 6. Temos 39 = 6.6 + 3. Por fim, o problema de encontrar o máximo divisor comum entre 3 e 6 resolve-se diretamente do fato de 3 ser um divisor de 6, de modo que 3 é o máximo divisor

comum entre 3 e 6 e, logo, entre 129 e 45.

EXEMPLO 3C

Determine o máximo divisor comum entre 400 e 148.

Solução:

400 = 2.148 + 104	(400, 148) = (148, 104)
148 = 1.104 + 44	(148, 104) = (104, 44)
104 = 2.44 + 16	(104, 44) = (44, 16)
44 = 2.16 + 12	(44, 16) = (16, 12)
16 = 1.12 + 4	(16, 12) = (12, 4)
12 = 3.4 + 0.	(12, 4) = 4

Assim, (400, 148) = 4.

Decorre também do algoritmo de Euclides que, se $d = (a,b)$, então existem $m,n \in \mathbb{Z}$, tais que $d = ma + nb$. Adiante será provado que d é o menor inteiro positivo que pode ser escrito dessa forma. Assim, por exemplo, a equação $30m + 15n = 1$ não tem raízes inteiras porque 30 e 15 não são relativamente primos. Podemos dizer que 1 não pode ser escrito como *combinação linear* de 30 e 15.

EXEMPLO 4A

Encontre $m,n \in \mathbb{Z}$ tais que $129m + 45n = 3$.

Solução:

Uma vez que (129, 45) = 3, o problema é possível. Pelo algoritmo de Euclides, podemos proceder:

129 = 2.45 + 39, daqui podemos dizer que 39 = 129 − 2.45

45 = 1.39 + 6, assim 6 = 45 − 39 = 45 − (129 − 2.45) = 3.45 − 129

39 = 6.6 + 3.

Logo

3 = 39 − 6.6 = (129 − 2.45) − 6.(3.45 − 129) = 129 − 2.45 − 18.45 + 6.129 = 7.129 − 20.45. Assim, os valores $m = 7$ e $n = -20$ satisfazem a relação $129m + 45n = 3$.

Observe que podemos encontrar soluções inteiras para $129m + 45n = d$ para qualquer inteiro d múltiplo de 3, bastando para isso multiplicar as soluções da equação original.

EXEMPLO 4B

Encontre dois números inteiros a, b tais que $60a + 25b = 30$.

Solução:

Para que o algoritmo de Euclides forneça uma solução para o problema, é necessário que 30 seja múltiplo do máximo divisor comum entre 60 e 25. Comecemos determinando (60, 25).

60 = 2.25 + 10

25 = 2.10 + 5

20 = 4.5.

Assim, encontramos (60, 25) = 5 e, aplicando o método descrito no exemplo anterior, podemos encontrar 5 como combinação linear de 60 e 25. O processo leva à igualdade

5 = (−2).60 + 5.25

Como 30 = 6.5, basta multiplicar a última igualdade por 6 para obter:

6.5 = 6.(−2).60 + 6.5.25

E assim concluímos que 30 = (−12).60 + 30.25, ou seja, os valores $a = -12$ e $b = 30$ satisfazem a relação $60a + 25b = 30$.

Definição 5: Dados os números inteiros a, b, c, a equação $ax + by = c$ com incógnitas x e y é chamada de *equação diofantina linear* (em referência a Diofante, matemático e geógrafo considerado por muitos o maior algebrista grego, o qual tem para a Aritmética a importância que Euclides tem para a Geometria).

Proposição 8: A equação diofantina linear de duas incógnitas x e y dada por $ax + by = c$ admite solução se, e somente se, $(a, b) \mid c$.

Demonstração: Suponha que a equação $ax + by = c$ tenha uma solução, ou seja, que existam inteiros x_1 e y_1 tais que $ax_1 + by_1 = c$. Sendo $d = (a, b)$, podemos escrever $a = dq_1$ e $b = dq_2$, para inteiros apropriados. Assim $c = dq_1x_1 + dq_2y_1 = d(q_1x_1 + q_2y_1)$. Concluímos, então, que $d \mid c$.

Pelo algoritmo de Euclides, podemos escrever $d = ax_1 + by_1$ para inteiros apropriados, mas, se supusermos que $d \mid c$, poderemos escrever $c = dq$, onde q é seria um inteiro. Assim $c = dq = q(ax_1 + by_1) = (qx_1)a + (qy_1)b$. Logo, obtemos que os inteiros $x = qx_1$ e $y = qy_1$ satisfazem a relação $ax + by = c$ e, assim, a equação tem solução inteira, o que completa a prova.

O algoritmo de Euclides para a determinação do máximo divisor comum

entre dois números fornece, como visto, uma maneira de resolver as equações diofantinas. Verifique nos exemplos que antecedem a definição de equação diofantina que poderíamos ter feito um teste com o máximo divisor comum entre os coeficientes para determinar se a equação era possível. Revise os conceitos da aula e faça testes com dois números a quaisquer para treinar a técnica. Em seguida, podemos passar ao próximo tópico, que trata do Teorema Fundamental da Aritmética e de suas implicações.

TÓPICO 4

O Teorema Fundamental da Aritmética

OBJETIVOS

- Enunciar e demonstrar um teorema central para o curso
- Observar as principais consequências do teorema e suas aplicações

Vimos que um número primo possui exatamente dois divisores positivos e, portanto, não pode ser escrito como produto de dois números menores que ele. Assim, como 29 é um número primo, a única forma de escrevê-lo como produto de dois números inteiros positivos é $29 = 1.29$.

Os números compostos possuem divisores triviais, podendo ser *fatorados* como produto de números menores. Por exemplo, 30 é composto e pode ser escrito como $30 = 6.5 = 2.15 = 3.10$. Algo a se observar aqui é que nenhuma dessas maneiras de escrever o número 30 envolve apenas primos. De fato, a única maneira (a menos da ordem dos números) de escrever 30 como produto de números primos é $30 = 2.3.5$. A seguir, veremos que podemos fazer isso com qualquer número inteiro maior que 1.

Comecemos por um resultado simples que servirá para, de certa forma, tornar a demonstração do teorema mais clara.

Lema: Se a é um número composto, então o menor divisor próprio de n é primo.

Demonstração: Seja d o menor divisor próprio de n. Por definição, $d \neq 1$. Se d fosse composto, ele possuiria um divisor próprio, digamos d_0. Mas $d_0 | d$ e $d | n$ implicam que $d_0 | n$ e, como $d_0 < d$, haveria um divisor próprio de n menor que d, contrariando a sua minimalidade.

Teorema (Fundamental da Aritmética): Todo número inteiro maior que 1 pode ser escrito como produto de números primos. Em outros termos: dado qualquer número inteiro $a>1$, existem primos $p_1,...,p_k$ distintos, e inteiros positivos $\alpha_1,...,\alpha_k$ tais que $n=p_1^{\alpha_1}...p_k^{\alpha_k}$. Além disso, a menos da ordem dos números, essa *decomposição* é feita de maneira única.

Demonstração: Se n é primo, o resultado vale imediatamente. Seja, então, n composto. Pelo lema anterior, o menor divisor próprio de n é primo. Vamos chamá-lo de p_1. Podemos, então, escrever $n=p_1n_1$. Se n_1 é primo, o resultado vale imediatamente. Caso contrário, seja, então, n_1 composto. Da mesma forma, o menor divisor próprio de n_1 é primo. Vamos chamá-lo de p_2. Assim, podemos escrever $n=p_1n_1=p_1p_2n_2$. O processo pode ser repetido, e como, a cada passo, $n_i<n_{i-1}$, ou seja, forma-se uma sequência decrescente de inteiros positivos e maiores que 1, haverá um momento no qual teremos $n_m=p_m$ primo e, assim, $n=p_1...p_m$. Como os primos obtidos não são necessariamente distintos, podemos contar a quantidade de vezes que cada primo p_i aparece. Vamos chamar essa quantidade de α_i e concluir que $n=p_1^{\alpha_1}...p_k^{\alpha_k}$.

Quanto à unicidade, suponha que $n=p_1^{\alpha_1}...p_k^{\alpha_k}$ e $n=q_1^{\beta_1}...q_r^{\beta_r}$ sejam duas decomposições em números primos do número n. Como p_1 é primo e divide $n=q_1^{\beta_1}...q_r^{\beta_r}$, pela definição de número primo, temos $p_1 \mid q_i$ para algum i e, como eles são primos, devem ser iguais, assim, podemos reordenar os primos da segunda decomposição para que $p_1=q_1$. Usando um argumento semelhante, podemos concluir que os expoentes devem ser iguais também. Da igualdade $p_1^{\alpha_1}...p_k^{\alpha_k}=q_1^{\beta_1}...q_r^{\beta_r}$, e uma vez que $p_1=q_1$ e $\alpha_1=\beta_1$, podemos concluir que $p_2^{\alpha_2}...p_k^{\alpha_k}=q_2^{\beta_2}...q_r^{\beta_r}$. Daí, basta repetir a ideia de reordenamento para provar que $p_2=q_2$ e $\alpha_2=\beta_2$. O raciocínio é repetido k vezes, quando se esgotam os primos p_i o mesmo tendo que acontecer com os q_i. Dessa forma, a quantidade de primos distintos nas duas decomposições é a mesma e, a menos de ordem dos números, elas possuem os mesmos fatores com os mesmos expoentes, o que conclui a demonstração.

Não é sem motivo que o teorema acima recebe o nome de *fundamental*, pois muitos outros resultados seguem diretamente dele, além da simplificação de uma série de outros problemas.

EXEMPLO 1A

A decomposição em fatores primos do número 72 é $2^3.3^2$. Dessa maneira, se $d \mid 72$, nenhum primo diferente de 2 e 3 pode dividir d, ou seja, podemos

escrever $d = 2^{\alpha}3^{\beta}$, com $\alpha \in \{0,1,2,3\}$ e $\beta \in \{0,1,2\}$. Assim, temos 4 possibilidades para o valor de α e 3 para β. Pelo Princípio Fundamental da Contagem, podemos concluir, então, que 72 possui 4.3 = 12 divisores inteiros positivos.

EXEMPLO 1B

Como $100 = 2^2.5^2$, os divisores positivos de 100 são da forma $d = 2^{\alpha}5^{\beta}$, com $\alpha, \beta \in \{0,1,2\}$. Assim, 100 possui 3.3 = 9 divisores positivos.

O número $3^2.5^4.7$ possui 3.5.2 = 30 divisores positivos.

EXEMPLO 1C

Para determinar a quantidade de divisores positivos do número $m = 4^3.12^2.15^3$, devemos obter sua fatoração em primos: $4^3.12^2.15^3 = (2^2)^3.(2^2.3)^2.(3.5)^3 = 2^6.2^4.3^2.3^3.5^3 = 2^{10}.3^5.5^3$. Dessa forma, m possui 11.6.4 = 264 divisores positivos.

Como visto nos exemplos, podemos determinar a quantidade de divisores positivos de um número inteiro de maneira prática a partir da sua decomposição em números primos. Outra utilidade dessa maneira de escrever os inteiros positivos é a determinação do máximo divisor comum.

ATENÇÃO!

Se n<-1, então -n é um inteiro maior que 1 e, assim, possui decomposição em números primos, de modo que npode ser escrito como produto de números primos vezes –1.

Se a e b são inteiros positivos e $d = (a,b)$, é claro que $d \mid a$. Assim a decomposição de d possui apenas primos constantes na fatoração de a, não podendo exceder os expoentes dessa fatoração. O mesmo deve acontecer em relação a b, de modo que a fatoração de d em primos contém exatamente os primos comuns às fatorações de a e de b com o menor expoente que aparecer.

EXEMPLO 2A

Como $108 = 2^2.3^3$ e $120 = 2^3.3.5$, o máximo divisor comum entre 108 e 120 tem em sua fatoração apenas os primos 2 e 3, que são os fatores comuns a ambos. Além disso, se o expoente do 2 fosse maior que 2, o resultado não seria divisor do 108. O expoente para 3 será 1, que é o máximo possível para ser divisor de 120. Dessa forma, temos $(108,120) = 2^2.3 = 12$.

EXEMPLO 2B

Como $72 = 2^3.3^2$ e $35 = 7.5$, temos $(72,35) = 1$.

Se pusermos os números primos em ordem crescente e escrevermos $p_1 = 2$, $p_2 = 3$, $p_3 = 5$ e assim sucessivamente, podemos dizer que todo número possui uma decomposição única da forma $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots = \prod_{k=1}^{\infty} p_k^{\alpha_k}$, onde α_k é diferente de 0 se $p_k \mid n$, e igual a 0, caso contrário.

Dessa forma, se $a = \prod_{k=1}^{\infty} p_k^{\alpha_k}$ e $b = \prod_{k=1}^{\infty} p_k^{\beta_k}$, vale dizer que $(a,b) = \prod_{k=1}^{\infty} p_k^{\gamma_k}$, onde γ_k é o mínimo entre α_k e β_k.

É claro que muito mais se pode extrair da relação de divisibilidade e da decomposição em números primos. Continuaremos com esse assunto, dando-lhe mais profundidade, vendo novos conceitos e revisitando outros. Por ora, encerramos essa primeira aula. Até breve.

AULA 2 | Múltiplos

Olá a todos,

Continuamos nosso estudo de Teoria dos Números. Na aula 1, demos ênfase aos divisores de um número inteiro. Nesta aula 2, continuamos com o assunto, abordando também os seus múltiplos. Veremos alguns critérios de divisibilidade e como representar números em bases diferentes da base 10.

Objetivos

- Dar prosseguimento ao estudo da divisibilidade
- Relacionar propriedades de divisibilidade e sistema decimal

TÓPICO 1

Mínimo Múltiplo Comum

Objetivos

- Definir e verificar as principais propriedades do mínimo múltiplo comum entre dois números
- Relacionar Mínimo Múltiplo Comum e Máximo Divisor Comum

Para os números inteiros positivos a e b, vimos que $a \mid b$ quando $b = aq$ para algum inteiro q, caso em que dizemos que a é um divisor de b, e b é um múltiplo de a. O conjunto de múltiplos inteiros positivos do número a é denotado por $M(a)$ e é sempre ilimitado superiormente.

Consequentemente podemos verificar, pela transitividade da relação de divisibilidade, que $a \mid b$ se, e somente se, $M(b) \subset M(a)$. Dessa relação, obtemos que se $c \in M(a) \cap M(b)$, então $M(c) \subset M(a) \cap M(b)$.

Definição 1: Dados os números inteiros positivos a e b, dizemos que o número $m \in \mathbb{Z}_+^*$ é o *mínimo múltiplo comum* e escrevemos $m = [a,b]$ quando:
(i) $a \mid m$ e $b \mid m$, ou seja, $m \in M(a) \cap M(b)$;
(ii) se $a \mid m_1$ e $b \mid m_1$, então $m \mid m_1$, ou seja, m é o menor número positivo com a propriedade (i).

EXEMPLO 1A:

Como $M(2) = \{2,4,6,8,10,...\}$ e $M(5) = \{5,10,15,20,25,....\}$, vale [2, 5] = 10.

EXEMPLO 1B:

Observando que $7 \mid 721$, podemos dizer que [721, 7] = 721.

Uma vez que para os inteiros positivos a e b é sempre verdade que $ab \in M(a) \cap M(b)$, o conjunto dos múltiplos comuns a dois inteiros positivos nunca

é vazio e, como possui apenas números positivos, possui sempre um elemento mínimo, de onde podemos concluir que sempre existe $[a,b]$.

Considerando os primos listados em ordem crescente (como no final da aula 1) e as decomposições $a=\prod_{k=1}^{\infty} p_k^{\alpha_k}$ e $b=\prod_{k=1}^{\infty} p_k^{\beta_k}$, vale $[a,b]=\prod_{k=1}^{\infty} p_k^{\omega_k}$, onde ω_k é o máximo entre α_k e β_k. De fato, se $m=\prod_{k=1}^{\infty} p_k^{\omega_k}$, vale $a \mid m$ e $b \mid m$. Além disso, qualquer múltiplo simultâneo de a e b deve conter todos os fatores primos das suas decomposições, fazendo com que o valor de m seja o menor possível.

EXEMPLO 2A:

Como $36=2^2 3^2$ e $40=2^3 5$, vale $[36,40]=2^3 3^2 5=360$.

EXEMPLO 2B:

Quando dois números são primos entre si, eles não possuem fatores primos em comum. Assim sendo, seu mínimo múltiplo comum é igual ao produto dos dois. Por exemplo, $[16,27]=16.27=432$.

Uma vez que para quaisquer números reais α e β vale mín $\{\alpha,\beta\}$ + máx $\{\alpha,\beta\} = \alpha+\beta$, é simples verificar que $(a,b).[a,b]=a.b$, para quaisquer inteiros positivos a e b. Assim, o algoritmo de Euclides fornece, também, uma maneira de encontrar o mínimo múltiplo comum entre dois números, como vemos a seguir.

EXEMPLO 3:

Podemos determinar (60, 36) de acordo com o esquema:

60 = 36 + 24	(60, 36) = (36, 24)
36 = 24 + 12	(36, 24) = (24, 12)
24 = 2.12	(24, 12) = 12

Assim, (60, 36) = 12, mas como $(60,36).[60,36]=60.36$, podemos escrever $[60,36]=\frac{60.36}{12}=180$.

TÓPICO 2

Outras bases

Objetivo

- Escrever números inteiros em diversas bases

Observe que, ao escrevermos, por exemplo, o número 3272, estamos usando a base 10, o que significa que podemos representá-lo da seguinte forma:

$$3272 = 3.10^3 + 2.10^2 + 7.10^1 + 2.10^0 .$$

Desde cedo aprendemos esse tipo de notação. Uma das consequências dessa notação é a propriedade que assegura que, para se multiplicar um número inteiro por 10, basta acresentar um 0 à direita do número. Neste tópico, veremos que é possível fazer o mesmo para qualquer base.

Teorema: Seja $B > 1$ um número inteiro. Todo número inteiro positivo a pode ser expresso, de maneira única, na forma $a = r_n B^n + \ldots + r_1 B + r_0$, com $0 \leq r_k < B$, para qualquer $0 \leq k < n$.

Demonstração: Comecemos dividindo a por B, obtendo quociente q_0 e resto r_0. Assim, vale dizer que:

$a = Bq_0 + r_0$, com $0 \leq r_0 < B$.

Dividindo, então, q_0 por B, obtemos quociente q_1 e resto r_1. Assim, vale dizer também que:

$q_0 = Bq_1 + r_1$, com $0 \leq r_1 < B$.

Note que $q_0 > q_1$. Repetindo o processo, podemos dividir q_1 por B, obtendo quociente q_2 e resto r_2, onde $q_1 > q_2$.

$q_1 = Bq_2 + r_2$, com $0 \leq r_2 < B$.

Repetimos o processo até que $q_n = 0$, o que fatalmente acontecerá,

uma vez que a sequência de quocientes é decrescente e formada apenas por números não negativos.

Neste caso, teremos os dois últimos passos:

$q_{n-2} = Bq_{n-1} + r_{n-1}$, com $0 \leq r_{n-1} < B$.

$q_{n-1} = Bq_n + r_n = B.0 + r_n = r_n$, com $0 \leq r_n < B$.

Por retrossubstituição, podemos fazer:

$q_{n-2} = Bq_{n-1} + r_{n-1} = Br_n + r_{n-1}$

$q_{n-3} = Bq_{n-2} + r_{n-1} = B(Br_n + r_{n-1}) + r_{n-2} = B^2 r_n + Br_{n-1} + r_{n-2}$

$q_{n-4} = Bq_{n-3} + r_{n-3} = B(B^2 r_n + Br_{n-1} + r_{n-2}) + r_{n-3} = B^3 r_n + B^2 r_{n-1} + Br_{n-2} + r_{n-3}$

e assim sucessivamente até

$q_0 = Bq_1 + r_1 = B(B^{n-2} r_n + B^{n-3} r_{n-1} + ... + Br_3 + r_2) + r_1$

$= B^{n-1} r_n + B^{n-2} r_{n-1} + ... + B^2 r_3 + Br_2 + r_1$

E, por fim:

$a = Bq_0 + r_0 = B(B^{n-1} r_n + B^{n-2} r_{n-1} + ... + Br_2 + r_1) + r_0$

$= B^n r_n + B^{n-1} r_{n-1} + ... + B^2 r_2 + Br_1 + r_0$

Assim, demonstramos a existência de tais coeficientes.

Observe agora que r_0 é o resto da divisão de a por B, sendo, portanto, unicamente determinado. Além disso, $Br_1 + r_0$ é o resto da divisão de a por B^2, fazendo com que r_1 seja unicamente determinado. Uma repetição desse argumento nos levará à unicidade da representação.

Por simplicidade, escrevemos $a = r_n B^n + ... + r_1 B + r_0 = (r_n ... r_1 r_0)_B$ e, como de costume, quando a base é omitida, é porque estamos usando 10.

EXEMPLO 1A:

Escreva 185 na base 7.

Solução:

Fazendo divisões sucessivas:

185 = 7.26 + 3

26 = 7.3 + 5.

Assim, temos 187 = 7.(7.3 + 5) + 3 = $3.7^2 + 5.7 + 3 = (353)_7$

EXEMPLO 1B:

Escreva 2185 na base 5.

2185 = 437.5 + 0

437 = 87.5 + 2

87 = 17.5 + 2

$17 = 3.5 + 2$

$3 = 0.5 + 3$

Por substituição, temos:

$$87 = 17.5 + 2 = (3.5 + 2).5 + 2 = 3.5^2 + 2.5 + 2$$

$$437 = 87.5 + 2 = (3.5^2 + 2.5 + 2).5 + 2 = 3.5^3 + 2.5^2 + 2.5 + 2$$

$$2185 = 437.5 + 0 = (3.5^3 + 2.5^2 + 2.5 + 2).5 + 0 = 3.5^4 + 2.5^3 + 2.5^2 + 2.5 + 0 = (32220)_5$$

ATENÇÃO!

Em outras palavras, o teorema acima pode ser expresso por:

Para cada par de números $a, B \in \mathbb{Z}$, com $B > 1$, existe um único polinômio $p \in \mathbb{Z}[x]$, com coeficientes menores que B e não negativos tais que $a = p(B)$.

EXEMPLO 1C:

Passe 217 para a base 6

$217 = 6.36 + 1$

$36 = 6.6 + 0$

$6 = 1.6 + 0$

$1 = 0.6 + 1$

Logo $217 = (1001)_6$.

Também podemos fazer o processo inverso, ou seja, transformar um número em uma base qualquer para a decimal, processo este que é feito de maneira ainda mais simples.

EXEMPLO 2:

Passe o número $(432)_8$ para a base 10.

Solução:

Vemos, pela definição, que

$$(432)_8 = 4.8^2 + 3.8 + 2 = 4.64 + 24 + 2 = 292.$$

EXEMPLO 3:

Independentemente da base $B > 2$, o número $(121)_B$ é um quadrado perfeito, pois $(121)_B = 1.B^2 + 2.B + 1 = B^2 + 2.B.1 + 1^2 = (B + 1)^2$, ou seja, o quadrado de um inteiro.

TÓPICO 3

Congruência

Objetivos

- Estabelecer a notação de congruência
- Verificar as principais propriedades de congruência

Neste tópico, veremos uma maneira interessante de escrever o resto da divisão entre dois números. A notação que estabeleceremos será muito útil.

Definição 2: Dado o número inteiro positivo n, dizemos que os inteiros a e b são *congruentes módulo* n, e representamos por $a \equiv b (\mathrm{mod}\, n)$, quando $a-b$ é um múltiplo de n, ou seja:

$$a \equiv b (\mathrm{mod}\, n) \Leftrightarrow n \mid a-b$$

EXEMPLO 1:

Uma vez que 47 − 3 = 44, que é um múltiplo de 4, podemos escrever $44 \equiv 3 (\mathrm{mod}\, 4)$. Podemos verificar também que $25 \equiv 10 (\mathrm{mod}\, 5)$, $49 \equiv 0 (\mathrm{mod}\, 7)$ e $50 \equiv 2 (\mathrm{mod}\, 6)$.

Proposição 1: Se $a \equiv b (\mathrm{mod}\, n)$, então a e b deixam o mesmo resto na divisão por n.

Demonstração: Escrevendo $a = nq_1 + r_1$ e $b = nq_2 + r_2$, com $0 \leq r_1, r_2 < n$ e usando a definição, temos $a \equiv b (\mathrm{mod}\, n) \Leftrightarrow n \mid a-b \Leftrightarrow \exists q; a-b = nq$. Assim, por substituição, obtemos $(nq_1 + r_1) - (nq_2 + r_2) = nq$, ou seja, $r_1 - r_2 = nq - nq_1 + nq_2 = n(q - q_1 + q_2)$, de onde concluímos que $n \mid r_1 - r_2$, e, como $0 \leq r_1, r_2 < n$, obtemos $r_1 - r_2 = 0$, isto é, os restos são iguais. Ressalta-se aqui que a recíproca dessa proposição também é válida.

Relembramos que a divisão do inteiro a pelo inteiro positivo n deixa resto não negativo e sempre menor que n. Dessa forma, se r é tal resto, necessariamente $0 \leq r < n$. Podemos, então, resumir essa informação em notação: $\forall a \in \mathbb{Z}, \exists m \in \{0,1,\ldots,n-1\}; a \equiv m (\mathrm{mod}\, n)$.

Teorema: Dado o inteiro positivo n, a relação de congruência módulo n satisfaz as seguintes propriedades:
(i) $a \equiv a (\mathrm{mod}\, n)$, para qualquer inteiro a, ou seja, é uma relação *reflexiva*;
(ii) se $a \equiv b (\mathrm{mod}\, n)$, então $b \equiv a (\mathrm{mod}\, n)$, para quaisquer inteiros a e b, ou seja, é uma relação *simétrica*;
(iii) se $a \equiv b (\mathrm{mod}\, n)$ e $b \equiv c (\mathrm{mod}\, n)$, então $a \equiv c (\mathrm{mod}\, n)$, para quaisquer inteiros a, b e c, ou seja, é uma relação *transitiva*;

GUARDE BEM ISSO!

Uma relação reflexiva, simétrica e transitiva é chamada de relação de equivalência.

A demonstração deste teorema é imediata, uma vez que, como provado anteriormente, dois números são congruentes módulo n quando deixam o mesmo resto na divisão por n.

Vejamos agora que a relação de congruência é preservada por somas e produtos.

Proposição 2: Se $a \equiv b (\mathrm{mod}\, n)$ e $c \equiv d (\mathrm{mod}\, n)$, então $a + c \equiv b + d (\mathrm{mod}\, n)$ e $ac \equiv bd (\mathrm{mod}\, n)$.

Demonstração: Por definição $a \equiv b (\mathrm{mod}\, n) \Rightarrow n \mid a - b$. Analogamente $c \equiv d (\mathrm{mod}\, n) \Rightarrow n \mid c - d$. Sabemos que a soma de dois múltiplos de n é também um múltiplo de n, ou seja, $a - b + c - d$ é um múltiplo de n, isto é, $n \mid (a + c) - (b + d)$ e, assim, $a + c \equiv b + d (\mathrm{mod}\, n)$.
Se $n \mid a - b$, ocorre também que $n \mid (a - b)c$. Da mesma forma, se $n \mid c - d$, $n \mid (c - d)b$. Usando argumento semelhante, concluímos que, se $n \mid a - b$, vale dizer também que $(a - b)c + (c - d)b$ é um múltiplo de n, mas $(a - b)c + (c - d)b = ac - bc + bc - bd = ac - bd$, ou seja, $n \mid ac - bd$, de onde obtemos $ac \equiv bd (\mathrm{mod}\, n)$.

Como conclusão da proposição acima, podemos afirmar que a congruência não apenas é uma maneira simplificada de dizer que dois números possuem o mesmo resto na divisão por outro (e assim também uma maneira alernativa de dizer que

um número é múltiplo do outro), mas também que é uma relação compatível com as operações de adição e de multiplicação. Obviamente, como $a-b=a+(-1)b$, concluímos que, também com a subtração, podemos operar com números congruentes sem alterar essa propriedade. Além disso, como a potência com expoente natural consiste de produto com fatores repetidos, podemos afirmar que se $a\equiv b(\mathrm{mod}\, n)$, então $a^k\equiv b^k(\mathrm{mod}\, n)$. Vejamos agora alguns exemplos de como essa propriedade pode ser aplicada para simplificar vários problemas.

EXEMPLO 2A:

Se o resto da divisão do número k por 5 é 2, qual o resto da divisão de $4k+13$ por 5?

Solução:

Observe que a condição inicial é equivalente a $k\equiv 2(\mathrm{mod}\, 5)$ e, como $4\equiv 4(\mathrm{mod}\, 5)$, podemos, pela conservação do resto na multiplicação, afirmar que $4k\equiv 8(\mathrm{mod}\, 5)$. Por fim, como $13\equiv 3(\mathrm{mod}\, 5)$, somamos para obter $4k+13\equiv 11(\mathrm{mod}\, 5)$. Assim, o resto da divisão de $4k+13$ por 5 é o mesmo que o de 11 por 5. A resposta é, portanto, 1.

EXEMPLO 2B:

Mostre que não existe inteiro a tal que $a^2\equiv 2(\mathrm{mod}\, 3)$.

Solução:

Em relação à congruência módulo 3, temos três possibilidades:

• se $a\equiv 0(\mathrm{mod}\, 3)$, então $a^2\equiv 0^2(\mathrm{mod}\, 3)$, ou seja, $a^2\equiv 0(\mathrm{mod}\, 3)$ e, claro, $a\not\equiv 2(\mathrm{mod}\, 3)$;

• se $a\equiv 1(\mathrm{mod}\, 3)$, então $a^2\equiv 1^2(\mathrm{mod}\, 3)$, ou seja, $a^2\equiv 1(\mathrm{mod}\, 3)$ e, claro, $a\not\equiv 2(\mathrm{mod}\, 3)$;

• por fim, se $a\equiv 2(\mathrm{mod}\, 3)$, então $a^2\equiv 2^2(\mathrm{mod}\, 3)$, ou seja, $a^2\equiv 1(\mathrm{mod}\, 3)$ e, claro, $a\not\equiv 2(\mathrm{mod}\, 3)$;

Assim, esgotam-se todas as possibilidade, e podemos afirmar que a equação $a^2\equiv 2(\mathrm{mod}\, 3)$ não possui soluções em $\mathbb{Z}$.

EXEMPLO 2C:

Uma vez que $6\equiv 1(\mathrm{mod}\, 5)$, podemos dizer que $6^{40}\equiv 1(\mathrm{mod}\, 5)$. Geralmente, $6^k\equiv 1(\mathrm{mod}\, 5)$, para qualquer inteiro positivo k.

EXEMPLO 3:

Determine o algarismo das unidades de 14^{14}.

Solução:

Podemos perceber diretamente que o algarismo das unidades de um número, na representação decimal, é o resto da divisão deste número por 10. Inicialmente, observamos que $14 \equiv 4(\mathrm{mod}10)$. Assim, $14^{14} \equiv 4^{14}(\mathrm{mod}10)$, mas $4^2 = 16 \equiv 6(\mathrm{mod}10)$ e $4^3 = 4^2.4 \equiv 6.4(\mathrm{mod}10)$, ou seja, $4^3 \equiv 4(\mathrm{mod}10)$. Geramos, então, uma sequência periódica, sendo $4^n \equiv 4(\mathrm{mod}10)$ se n é ímpar, e $4^n \equiv 6(\mathrm{mod}10)$ se n é par. Desta feita, obtemos $4^{14} \equiv 6(\mathrm{mod}10)$ e, consequentemente, o algarismo das unidades de 14^{14} é 6.

Outras informações a respeito de congruência serão discutidas nas próximas aulas, nas quais enunciaremos resultados importantes e suas respectivas aplicações.

TÓPICO 4

Critérios de divisibilidade

Objetivo

- Analisar critérios segundo os quais um número divide o outro, sem apelar para a divisão direta

Usando a base 10, agora veremos como reconhecer múltiplos de alguns números sem ter que recorrer à divisão. Revisitaremos, então, algumas regras, justificando-as.

Divisibilidade por 2: Um número é divisível por 2 se, e somente se, quando escrito na base 10, terminar em um algarismo par, ou seja, em 0, 2, 4, 6 ou 8.
Demonstração: Dado o número a, podemos escrevê-lo na base 10 da forma $a = r_n ... r_1 r_0$, significando $a = r_n.10^n + ... + r_1.10 + r_0 = 10(r_n.10^{n-1} + ... + r_1) + r_0$. Fazendo $k = r_n.10^{n-1} + ... + r_1$, temos, então $a = 10k + r_0 = 2.5k + r_0$. Assim, a e r_0 deixam o mesmo resto na divisão por 2.

EXEMPLO 1:

Os números 23472 e 8008 são divisíveis por 2, enquanto 98221 e 507 não são.

Observação:

É importante ressaltar que os critérios descritos neste tópico estão sendo enunciados tomando a representação do número na base 10; quando a base for diferente, devem-se fazer os devidos ajustes. O número $(324)_5$, por exemplo, é ímpar, enquanto o número $(11)_7$ é par. (Verifique).

Divisibilidade por 3: Um número é divisível por 3 se, e somente se, a soma dos seus algarismos na representação em base 10 for divisível por 3.

Demonstração: Observe inicialmente que $10 \equiv 1 (\mathrm{mod}\, 3)$, de onde podemos concluir que $10^k \equiv 1 (\mathrm{mod}\, 3)$ para qualquer natural k, de onde também obtemos $r.10^k \equiv r (\mathrm{mod}\, 3)$. Dado o número a, podemos escrevê-lo na base 10 da forma $a = r_n \ldots r_1 r_0$, significando $a = r_n.10^n + \ldots + r_1.10 + r_0$. Pelas propriedades da congruência, temos $a \equiv r_n + \ldots + r_1 + r_0 (\mathrm{mod}\, 3)$. Assim, a e $r_n + \ldots + r_1 + r_0$ deixam o mesmo resto na divisão por 3.

ATENÇÃO!

Como $10 \equiv 1 (\mathrm{mod}\, 9)$, o critério de divisibilidade por 3, descrito acima, também é válido para divisibilidade por 9, ou seja, para verificarmos se um número é múltiplo de 9, testamos a soma dos seus algarismos. Assim, por exemplo, podemos afirmar que 61758423 é múltiplo de 9, porque a soma de seus algarismos é um múltiplo de 9.

EXEMPLO 2:

Para saber se o número 276534 é divisível por 3, podemos somar os algarismos que o compõem: 2 + 7 + 6 + 5 + 3 + 4 = 27. Como 27 é múltiplo de 3, concluímos que 276543 também é múltiplo de 3. Realizando teste semelhante, podemos afirmar que 89332 não é múltiplo de 3.

Divisibilidade por 4: Um número é divisível por 4 se, e somente se, os dois últimos algarismos da sua representação na base 10 formarem, na ordem em que aparecerem, um número divisível por 4.

Demonstração: Dado o número a, podemos escrevê-lo na base 10 da forma $a = r_n \ldots r_1 r_0$, significando $a = r_n.10^n + \ldots + r_1.10 + r_0 = 100(r_n.10^{n-2} + \ldots + r_2) + 10r_1 + r_0$.

Como 100 é divisível por 4, e fazendo $k = r_n.10^{n-2} + \ldots + r_2$, temos $a = 100k + r_0 = 4.25k + 10r_1 + r_0$. Assim, a e $10r_1 + r_0$ deixam o mesmo resto na divisão por 4.

EXEMPLO 3:

Uma vez que 32 é múltiplo de 4, podemos dizer que 399287532 é múltiplo de 4.

Observação:

Como 1000 = 8.125, podemos proceder de maneira análoga ao visto acima para afirmar que um número é divisível por 8 quando o número formado pelos três últimos algarismos de sua representação decimal for um múltiplo de 8.

Divisibilidade por 5: Um número é divisível por 5 se, e somente se, quando escrito na base 10 terminar em 0 ou 5.

Demonstração: Dado o número a, podemos escrevê-lo na base 10 da forma $a = r_n...r_1r_0$, significando $a = r_n.10^n + ... + r_1.10 + r_0 = 10(r_n.10^{n-1} + ... + r_1) + r_0$. Fazendo $k = r_n.10^{n-1} + ... + r_1$, temos, então, $a = 10k + r_0 = 5.2k + r_0$. Assim, a e r_0 deixam o mesmo resto na divisão por 5.

EXEMPLO 4:

Os números 9355 e 7530 são múltiplos de 5, enquanto 49873 e 541 não são.

Observação:

Os critérios acima podem ser combinados para se verificar se um número é múltiplo de 6, de 10 ou de 15. Por exemplo, como 15 = 3.5, um número será divisível por 15 se, e somente se, for divisível por 3 e por 5. Além disso, verifica-se facilmente que 660 é divisível por 2, por 3 e por 5, sendo, portanto, um múltiplo de 30.

Há critérios semelhantes aos apresentados até aqui que podem ser aplicados para se testar se um número é múltiplo de 7, de 11 ou de outros primos. Em seguida, apresentaremos um exemplo de como podemos verificar se um número é múltiplo de 7, entretanto, como se verá, a divisão direta pode ser meio mais prático para essa verificação.

SAIBA MAIS!

No site http://www.somatematica.com.br/fundam/critdiv.php, você poderá rever os critérios de divisibilidade apontados e conhecer ainda outros, sobre os quais falaremos a seguir. Bom estudo!

EXEMPLO 5:

Como $10 \equiv 3 (\mathrm{mod}\, 7)$, podemos, multiplicando por 3 e observando o resto na divisão por 7, escrever a sequência:

$10^2 \equiv 2 (\mathrm{mod}\, 7)$;

$10^3 \equiv 6 (\mathrm{mod}\, 7)$;

$10^4 \equiv 4 (\mathrm{mod}\, 7)$;

$10^5 \equiv 5(\mathrm{mod}\,7)$, e assim sucessivamente. Usando esses resultados, podemos verificar se 3801 é divisível por 7. Façamos $3801 = 3.10^3 + 8.10^2 + 1$. Assim, $3801 \equiv 3.6 + 8.2 + 1(\mathrm{mod}\,7)$, e como 3.6 + 8.2 + 1 = 35, que é um múltiplo de 7, podemos dizer que 3801 também é um múltiplo de 7. Pode-se repetir o processo e verificar que o resto da divisão de 4986 por 7 é 2.

EXEMPLO 6:

Observando inicialmente que 1001 = 7.11.13, temos $1001 \equiv 0(\mathrm{mod}\,7)$, ou seja, $1000 \equiv -1(\mathrm{mod}\,7)$. Podemos verificar se um número é divisível por 7, 11 ou 13 através de um teste que será descrito aqui com o número 124397. Uma vez que $124397 = 124.1000 + 397$, temos $124397 \equiv 124.(-1) + 397(\mathrm{mod}\,7)$. Agora, como 397 − 124 = 273, que é um múltiplo de 7, afirmamos que 124397 é múltiplo de 7. Como $11 \not| 273$, podemos dizer, pela mesma ideia, que 124397 não é múltiplo de 11.

AULA 3

Alguns teoremas sobre congruência

Olá aluno(a),

Nesta nossa terceira aula, estudaremos detalhadamente a congruência de números inteiros, tratando, por meio de enunciado, demonstração e consequências, de três importantes resultados, os conhecidos teoremas de Wilson, Fermat e Euler.

Objetivo

- Complementar o estudo de congruência, dando-lhe mais aprofundamento

TÓPICO 1

Teorema de Wilson

Objetivos

- Apreender os conceitos de cultura nacional e cultura organizacional
- Entender os planos ou níveis da cultura organizacional
- Conhecer técnicas de desenvolvimento organizacional

Na última aula, estabelecemos que a notação $a \equiv b (\mathrm{mod}\, n)$ para os inteiros a, b e n indica que a e b deixam o mesmo resto na divisão por n. Por exemplo, é verdade que $25 \equiv 1 (\mathrm{mod}\, 4)$ e $19 \equiv 4 (\mathrm{mod}\, 5)$, enquanto $a \equiv 0 (\mathrm{mod}\, n)$ é equivalente a $n \mid a$.

Neste primeiro tópico, discutiremos algumas propriedades sobre congruência e enunciaremos alguns resultados relevantes.

Comecemos com algumas definições simples.

Definição 1: O conjunto $S = \{r_0, r_1, \ldots, r_k\}$ é um *sistema completo de resíduos* módulo n se

(i) $r_i \equiv r_j (\mathrm{mod}\, n) \Leftrightarrow i = j$, ou seja, dois elementos distintos de S deixam restos distintos na divisão por n;

(ii) para todo inteiro a, tivermos $a \equiv r_i (\mathrm{mod}\, n)$ para algum $r_i \in S$.

EXEMPLO 1A:

O conjunto {5, 11, 22, 33, 44} é um sistema completo de resíduos módulo 5.

EXEMPLO1B:

Para qualquer inteiro $n > 1$, o conjunto $\{0, 1, \ldots, n-1\}$ é um sistema completo de resíduos módulo n.

Algo que podemos verificar é que qualquer sistema completo de resíduos módulo n possui exatamente n elementos. De fato, se $S=\{r_0,r_1,...,r_k\}$ é um sistema completo de resíduos módulo n, cada um dos números do conjunto $\{0,1,...,n-1\}$ é congruente a um dos $r_i \in S$. Logo, $k \leq n$. Reciprocamente, cada elemento de S é congruente a um número de $\{0,1,...,n-1\}$, que é, também, um sistema completo de resíduos módulo n, de onde obtemos que $n \leq k$, o que resulta em $k=n$.

Definição 2: Dado o número inteiro a, dizemos que $a^{-1} \in \mathbb{Z}$ é um *inverso* de a módulo n se $a.a^{-1} \equiv 1 (\mathrm{mod}\, n)$.

EXEMPLO 2A:

Como 7.3 = 21 e 21 deixa resto 1 na divisão por 5, vale $7.3 \equiv 1 (\mathrm{mod}\, 5)$, e podemos dizer que 3 é um inverso de 7 módulo 5.

EXEMPLO 2A:

Como 40 é múltiplo de 8, vale $40.b \equiv 0 (\mathrm{mod}\, 8)$, para qualquer inteiro b, de onde concluímos que 40 não possui inverso módulo 8. Mais geralmente, nenhum múltiplo de n possui inverso módulo n.

ATENÇÃO!

Na definição 2, usamos o artigo indefinido, pois, caso exista, o inverso módulo n de um número não é único, por exemplo, $7.3 \equiv 1 (\mathrm{mod}\, 5)$ e $7.8 \equiv 1 (\mathrm{mod}\, 5)$, de onde podemos dizer que 8 também é um inverso de 7 módulo 5. Entretanto, como veremos adiante, os inversos módulo n de um mesmo número são congruentes módulo n.

Podemos investigar a existência de inversos módulo n de acordo com o que segue.

Proposição 1: O número a possui inverso módulo n se, e somente se, $(a,n)=1$.

Demonstração: O inverso módulo n é uma solução para a equação $ax \equiv 1 (\mathrm{mod}\, n)$. Supondo que exista tal solução, deve haver um inteiro y tal que $ax-1=ny$, ou seja, $ax-ny=1$, que é uma equação diofantina linear nas variáveis x e y, que, de acordo com o exposto na aula 1 (tópico 3), possui solução se, e somente se, $(a,n) \mid 1$, o que vale apenas quando $(a,n)=1$.

EXEMPLO 3A:

Os números 2, 4, 5, 6, 8 e 10 não possuem inverso módulo 10.

EXEMPLO 3B:

Os números 1, 3, 7 e 9 são inversos módulo 10 de 1, 7, 3 e 9, respectivamente.

Exemplo 3c:

Para o número primo p, todos os números 1, 2, 3, $p-1$ possuem inverso módulo p.

Proposição 2: Se b e c são inversos de a módulo n, então $b \equiv c(\mathrm{mod}\, n)$.

Demonstração: Pela definição, a hipótese diz que $ab \equiv 1(\mathrm{mod}\, n)$ e $ac \equiv 1(\mathrm{mod}\, n)$. Subtraindo essas duas congruências, obtemos $a(b-c) \equiv 0(\mathrm{mod}\, n)$, ou seja, $n \mid a(b-c)$, mas, como $(a,n)=1$ é condição necessária para existir o inverso de a módulo n, obtemos $n \mid b-c$, que conclui a demonstração.

Assim, quando um número a possuir inverso módulo n, a quantidade de inversos é infinita, contudo, dentro de um sistema completo de resíduos módulo n, esse inverso é único.

Especificamente, se p é um número primo, então a será seu próprio inverso módulo p se, e somente se, $a \equiv 1(\mathrm{mod}\, p)$ ou $a \equiv -1(\mathrm{mod}\, p)$, pois, se $a^2 \equiv 1(\mathrm{mod}\, p)$, então vale $p \mid a^2 - 1 = (a+1).(a-1)$, ou seja, $p \mid a+1$ ou $p \mid a-1$, casos que implicam $a \equiv -1(\mathrm{mod}\, p)$ e $a \equiv 1(\mathrm{mod}\, p)$, respectivamente. A recíproca é imediata.

EXEMPLO 4:

Sabemos que o conjunto $S = \{0,1,...,10\}$ é um sistema completo de resíduos módulo 11. O número 0, obviamente, não possui inverso módulo 11. Como 11 é primo, todos os outros possuem inverso módulo 11, único no conjunto, e apenas 1 e 10 são seus próprios inversos. Assim, 2 e 6 são inversos módulo 11, o mesmo acontecendo com os pares 3 e 4; 5 e 9; e 7 e 8.

SAIBA MAIS!

No site http://www.dec.ufcg.edu.br/biografias/JohnWiso.html, você pode obter mais informações sobre o matemático John Wilson. Confira!

Podemos, agora, enunciar e ter uma demonstração simples de um teorema que leva o nome do matemático inglês John Wilson (1741 – 1793).

Teorema de Wilson 1: Se p é primo, então $(p-1)! \equiv -1 (\mathrm{mod}\, p)$.

Demonstração: O caso $p = 2$ é de imediata verificação. Entre os números $1, 2, ..., p-1$, apenas 1 e $p-1$ são seus próprios inversos módulo p. Os demais, $2, ..., p-2$, podem ser agrupados em pares cujo produto é congruente a 1 módulo p. Isso se deve ao fato de que eles possuem inverso módulo p, diferente de si mesmo e pertencente ao conjunto, ou seja, se $a \in \{2, ..., p-2\}$, existe $b \in \{2, ..., p-2\}$, com $b \neq a$, tal que $ab \equiv 1 (\mathrm{mod}\, p)$. Se multiplicarmos todas essas congruências sem repetir os números, obteremos $2.3.....(p-2) \equiv 1 (\mathrm{mod}\, p)$. Se multiplicarmos esta última congruência pela imediata $p-1 \equiv -1 (\mathrm{mod}\, p)$, obteremos $2.3.....(p-2).(p-1) \equiv -1 (\mathrm{mod}\, p)$, isto é, $(p-1)! \equiv -1 (\mathrm{mod}\, p)$.

Teorema de Wilson 2: Se $(n-1)! \equiv -1 (\mathrm{mod}\, n)$, então n é primo.

Demonstração: Vamos supor que $(n-1)! \equiv -1 (\mathrm{mod}\, n)$. Se $a < n$, aparece a no cálculo de $(n-1)!$, de onde concluímos que $(n-1)! \equiv 0 (\mathrm{mod}\, a)$. Se tivermos $a \mid n$, da hipótese $n \mid (n-1)!+1$ e da transitividade da divisibilidade, $a \mid (n-1)!+1$, ou seja, $(n-1)!+1 \equiv 0 (\mathrm{mod}\, a)$. Subtraindo $(n-1)!+1 \equiv 0 (\mathrm{mod}\, a)$ e $(n-1)! \equiv 0 (\mathrm{mod}\, a)$, obtemos $1 \equiv 0 (\mathrm{mod}\, a)$, mas isso somente é possível se $a = 1$. Assim, 1 é o único inteiro positivo menor que n que é divisor de n, de onde concluímos que n é primo.

Poderíamos ter enunciado que "$(n-1)! \equiv -1 (\mathrm{mod}\, n)$ se, e somente se, n é primo". A fragmentação foi feita apenas por caráter didático. Com isso, obtemos um não muito objetivo teste de primalidade.

EXEMPLO 5A:

Mostre que, se n é um múltiplo de 5, o resto da divisão de $(n+1)(n+2)(n+3)(n+4)$ por 5 é 4.

Solução:

Como $n \equiv 0 (\mathrm{mod}\, 5)$, então $n+1 \equiv 1 (\mathrm{mod}\, 5)$, $n+2 \equiv 2 (\mathrm{mod}\, 5)$, $n+3 \equiv 3 (\mathrm{mod}\, 5)$ e $n+4 \equiv 4 (\mathrm{mod}\, 5)$. Multiplicando as quatro congruências, obtemos $(n+1)(n+2)(n+3)(n+4) \equiv 1.2.3.4 (\mathrm{mod}\, 5)$, isto é, $(n+1)(n+2)(n+3)(n+4) \equiv 4! (\mathrm{mod}\, 5)$, mas, como 5 é primo, temos, pelo teorema de Wilson, $(5-1)! \equiv -1 (\mathrm{mod}\, 5)$. Como o resto deve ser um número positivo e $-1 \equiv 4 (\mathrm{mod}\, 5)$, obtemos que o resto da divisão de $(n+1)(n+2)(n+3)(n+4)$ por 5 é 4.

EXEMPLO 5B:

O produto de uma sequência de 16 números inteiros consecutivos pode ou não possuir um múltiplo de 17. Caso possua, o produto de todos eles deixará resto 0 na divisão por 17. Do contrário, teremos um sistema completo de resíduos módulo 17, e, se multiplicarmos todos eles, obteremos um número que, quando dividido por 17, deixa o mesmo resto que $16! = (17-1)!$, mas, pelo teorema de Wilson, esse resto é congruente a -1. Assim, o produto de dezesseis números inteiros consecutivos deixa resto 0 ou 16 na divisão por 17, de modo que a equação $n(n+1)(n+2)...(n+15) \equiv 10 (\mathrm{mod} 17)$ não possui solução.

EXEMPLO 6:

Como resultado embutido na demonstração do teorema de Wilson, podemos afirmar que, se p é primo, então $(p-2)! \equiv 1 (\mathrm{mod}\, p)$, de modo que $(11-2)! = 9!$ deixa resto 1 na divisão por 11. Nesses termos, concluímos que $9!-1$ é um múltiplo de 11. Analogamente $23 \mid 21!-1$.

TÓPICO 2

Teorema de Fermat

Objetivos

- Complementar o estudo sobre resíduos
- Enunciar e estudar as consequências do Pequeno Teorema de Fermat

Vamos aqui nos aproveitar dos resultados obtidos no tópico anterior para provar um resultado que leva o nome do matemático francês Pierre de Fermat (1601 – 1665). Um resultado forte que Fermat

Teorema de Fermat: Se p é um primo que não divide a, então $a^{p-1} \equiv 1 (\text{mod } p)$.

Demonstração: Para começar, $S = \{0, a, 2a, 3a, ..., (p-1)a\}$ é um sistema completo de resíduos módulo p. De fato, $ab \equiv ac (\text{mod } p)$ e $(a, p) = 1$ conduzem a $b \equiv c (\text{mod } p)$, mas $b, c \in \{0, 1, 2, ..., (p-1)\}$, que é um sistema completo de resíduos módulo p, logo $b = c$. Assim, os números $a, 2a, 3a, ..., (p-1)a$ deixam restos $1, 2, ..., (p-1)$ na divisão por p, não necessariamente nessa ordem. Temos, então, a congruência:

$a.2a.3a.....(p-1)a \equiv 1.2.....(p-1) (\text{mod } p)$, que pode ser simplificada por $a^{p-1}.(p-1)! \equiv (p-1)! (\text{mod } p)$.

Mas p não divide $(p-1)!$, de onde concluímos que $(p, (p-1)!) = 1$ e os fatores $(p-1)!$ podem ser "cancelados" da última congruência, de onde obtemos a conclusão:

$a^{p-1} \equiv 1 (\text{mod } p)$.

Com a hipótese de que p não é um divisor de a, temos, então, $a^{p-1} \equiv 1 (\text{mod } p)$. Se multiplicarmos a congruência pela imediata $a \equiv a (\text{mod } p)$, obteremos $a^p \equiv a (\text{mod } p)$. Agora, se $p \mid a$, então $p \mid a.(a^{p-1} - 1)$, ou seja, $p \mid a^p - a$, e obtemos o mesmo resultado $a^p \equiv a (\text{mod } p)$. Assim, podemos enunciar o seguinte resultado,

sem hipóteses de divisibilidade:

Proposição: Se p é primo e a é um inteiro positivo qualquer, então $a^p \equiv a(\text{mod}\, p)$.

EXEMPLO 1A:

Encontre o resto da divisão de 2^{120} por 13.

Solução:

Já que 13 é primo e não é um divisor de 2, podemos usar o Teorema de Fermat para concluir que $2^{13-1} \equiv 1(\text{mod}13)$, ou seja, $2^{12} \equiv 1(\text{mod}13)$. Daí obtemos $\left(2^{12}\right)^{10} \equiv 1^{10}(\text{mod}13)$, isto é, $2^{120} \equiv 1(\text{mod}13)$ e, assim, o resto procurado é 1.

EXEMPLO 1B:

Encontre o resto da divisão de 5^{110} por 19.

Solução:

Observe que não podemos usar exatamente o mesmo raciocínio do exemplo 1a, pois 18 não é um divisor de 110, mas podemos escrever 110 = 18.6 + 2 e, assim, $5^{110} = \left(5^{18}\right)^6 .5^2$. Já que 19 é primo e não é um divisor de 5, podemos usar o Teorema de Fermat para concluir que $5^{19-1} \equiv 1(\text{mod}19)$, ou seja, $5^{18} \equiv 1(\text{mod}19)$. Daí obtemos $\left(5^{18}\right)^6 \equiv 1^6(\text{mod}19)$, isto é, $5^{108} \equiv 1(\text{mod}19)$. Alie-se a isso a congruência facilmente verificável $5^2 \equiv 6(\text{mod}19)$ e concluímos $5^{110} \equiv 6(\text{mod}19)$. O resto procurado é, portanto, 6.

TÓPICO 3

Teorema de Euler

Objetivos

- Definir a função totiente de Euler e estudar suas características
- Generalizar o teorema de Fermat para todos os inteiros

O objeto principal deste tópico é um resultado devido ao matemático suíço Leonhard Euler (1707 – 1783) e trata de uma generalização do teorema de Fermat apresentado anteriormente. Antes de enunciá-lo, definiremos uma função especial. A primeira de uma série de funções – as funções aritméticas – que serão estudadas em uma aula posterior

Definição 2: A função ϕ, chamada de *totiente de Euler*, associa a cada número inteiro positivo n a quantidade de inteiros positivos relativamente primos com n. Mais precisamente, $\phi : \{1,2,...\} \to \{1,2,...\}$, definida por $\phi(n)$, é a quantidade de elementos do conjunto $\{m \in \mathbb{Z}; 0 < m \leq n \text{ e } (m,n) = 1\}$.

EXEMPLO 1A:

Como os números inteiros positivos que são menores que 12 e relativamente primos com 12 são 1, 5, 7 e 11, vale $\phi(12) = 4$. Analogamente, os números inteiros positivos que são relativamente primos com 15 são 1, 2, 4, 6, 7, 8, 11, 13 e 14, de modo que $\phi(15) = 9$.

EXEMPLO 1B:

Para qualquer primo p, todos os inteiros positivos menores que p são relativamente primos com p. Assim, vale $\phi(p) = p - 1$.

EXEMPLO 1C:

A equação $\phi(n) = n$ possui apenas a solução $n = 1$, pois, do contrário, $\phi(n) < n$.

EXEMPLO 1D:

Podemos determinar $\phi(100)$ por meio de um crivo semelhante ao de Erastótenes. Para tanto, da lista dos números menores que 100, riscamos todos aqueles que sejam múltiplos dos mesmos divisores primos de 100, a saber: 2 e 5. Se listarmos os inteiros positivos de 1 a 100 e eliminarmos os múltiplos de 2, sobram apenas 50 números. Nesse primeiro passo, já foram eliminados os múltiplos de 5 que terminam em 0, ficando para serem eliminados, no segundo passo, apenas os que terminam em 5. São eles: 5, 15, 25, ..., 95, num total de 10. Assim, riscando esses 10 números dos 50 que haviam restado ao final do primeiro passo, sobram 40, que é o valor de $\phi(100)$.

ATENÇÃO!

Vimos, no tópico 1, que um número possui inverso módulo n se, e somente se, ele e n forem relativamente primos. Podemos usar essa propriedade para definir, de forma equivalente, que $\phi(n)$ é a quantidade de inteiros positivos menores que n que possuem inverso módulo n.

Um raciocínio semelhante ao empregado no exemplo 1d pode ser usado para determinar o valor de $\phi(n)$, entretanto esse procedimento pode ser bem trabalhoso. Quando estudarmos as funções aritméticas, aprenderemos um método mais rápido para essa determinação. Por ora, ficamos com o que pode ser obtido diretamente da definição.

Definição 3: Dado o inteiro positivo n, o conjunto $S = \{r_1, ..., r_{\phi(n)}\}$ é um *sistema reduzido de resíduos* módulo n se os elementos forem dois a dois incongruentes módulo n e forem todos relativamente primos a com n. Mais formalmente, $S = \{r_1, ..., r_{\phi(n)}\}$ é um sistema reduzido de resíduos módulo n quando:

(i) $(r_i, n) = 1, \forall i$;

(ii) $r_i \equiv r_j \pmod{n} \Rightarrow i = j$.

Assim, uma maneira de obter um sistema reduzido de resíduos módulo n é retirar de um sistema completo de resíduos todos aqueles que não forem relativamente primos com n. De modo a abranger todas as possibilidades, da maneira como foi definido, um sistema reduzido de resíduos módulo n deve ter $\phi(n)$ elementos.

EXEMPLO 2A:

O conjunto $S = \{1,5,7,11\}$ é um sistema reduzido de resíduos módulo 12.

EXEMPLO 2B:

Para qualquer primo p, o conjunto $\{1,2,...,p-1\}$ é um sistema reduzido de resíduos módulo p.

Agora vamos ao objetivo principal do tópico.

Teorema de Euler: Para os inteiros relativamente primos a e n, vale $a^{\phi(n)} \equiv 1 (\mathrm{mod}\, n)$.

Demonstração: Essencialmente, a prova é a mesma que a feita do Teorema de Fermat. Aqui apenas ajustaremos para um sistema reduzido de resíduos. Comecemos verificando que, se $S = \{r_1,...,r_{\phi(n)}\}$ é um sistema reduzido de resíduos módulo n, o conjunto $S' = \{a.r_1,...,a.r_{\phi(n)}\}$ também o é. Para tal, basta observar que, sendo todos os r_i relativamente primos com n e o mesmo acontecendo com a, então $(a.r_i, n) = 1$. Além disso, se $a.r_i \equiv a.r_j (\mathrm{mod}\, n)$, mais uma vez apelando para $(a,n) = 1$, obtemos $r_i \equiv r_j (\mathrm{mod}\, n)$. Entretanto, dentro de um sistema de resíduos, isso somente ocorre quando $r_i = r_j$. Observado isso, fica claro que o produto dos elementos de S deixa o mesmo resto da divisão por n que o produto dos elementos de S', ou seja, $a.r_1.a.r_2.....a.r_{\phi(n)} \equiv r_1.....r_{\phi(n)} (\mathrm{mod}\, n)$, que é o mesmo que:

$$a^{\phi(n)}.r_1.r_2.....r_{\phi(n)} \equiv r_1.....r_{\phi(n)} (\mathrm{mod}\, n)$$

E como $(n, r_1.....r_{\phi(n)}) = 1$, o fator $r_1.....r_{\phi(n)}$ pode ser "cancelado" na congruência para obtermos $a^{\phi(n)} \equiv 1 (\mathrm{mod}\, n)$, que é o resultado desejado.

Bastar fazer n primo e observar o exemplo 1b para obter o Teorema de Fermat como um corolário do Teorema de Euler.

EXEMPLO 3A:

Encontre o algarismo das unidades de 7^{100}, quando representado na base 10.

Solução:

O algarismo das unidades, no sistema decimal, nada mais é que o resto da divisão do número por 10. Observe que $\phi(10)=4$ e $(7,10)=1$, daí, pelo Teorema de Euler, $7^4 \equiv 1(\mathrm{mod}10)$, de onde concluímos que $7^{100}=\left(7^4\right)^{25} \equiv 1^{25}(\mathrm{mod}10)$. Assim, a representação decimal de 7^{100} termina em 1.

EXEMPLO 3B

Podemos, também usando o Teorema de Euler, determinar o algarismo das dezenas de 21^{42}, já que os dois algarismos mais à direita na representação decimal de um número formam o resto da divisão do número por 100. Vimos que $\phi(100)=40$ e, além disso, $(100,21)=1$. Logo $21^{40} \equiv 1(\mathrm{mod}100)$. Multiplicando essa congruência por 21^2, obtemos $21^{42} \equiv 21^2(\mathrm{mod}100)$. Mas $21^2=441$. Assim, $21^{42} \equiv 41(\mathrm{mod}100)$ e o algarismo das dezenas é 4.

AULA 4

Funções aritméticas - parte I

Caro(a) aluno(a),

Nesta nossa quarta aula, daremos continuidade ao estudo de funções especiais que expressam alguma propriedade aritmética do número e cujo domínio é o conjunto dos inteiros positivos. De destaque, temos a função ϕ de Euler, a qual já começamos a estudar na aula 3, a função μ de Möbius, e as funções τ e σ.

No decorrer desta aula, apresentaremos as funções e algumas de suas principais propriedades, ilustraremos com exemplos e estabeleceremos relações entre elas. Na aula 5, daremos continuidade a esse estudo.

Objetivos

- Conhecer as funções aritméticas mais importantes
- Obter meios diretos de determinação de imagem por essas funções

TÓPICO 1

As funções τ e σ

OBJETIVOS

- Reconhecer as funções aritméticas τ e σ
- Definir função multiplicativa

Começaremos o nosso estudo de funções aritméticas apresentando a função que associa a cada número inteiro positivo a quantidade dos seus divisores inteiros positivos. Uma maneira de contar elementos de um conjunto é somar 1 para cada vez que esse elemento aparecer. Assim, podemos enunciar:

Definição 1: Denotaremos pela letra grega τ (tau) a função que, para cada inteiro positivo n, associa o valor $\tau(n)=\sum_{d|n}1$. Equivalentemente, podemos colocar $\tau(n)=\#D(n)$, onde # representa a quantidade de elementos do conjunto.

ATENÇÃO!

De acordo com o que estudamos no começo da primeira aula, os divisores inteiros de um números sempre vêm aos pares. Desse modo, basta estudar os divisores positivos, pois, se 3 é divisor de um número, "ganhamos" automaticamente o -3. Uma formulação mais precisa da definição ao lado seria $\tau(n)=\sum_{\substack{d|n\\ d>0}}1$. Por simplicidade (para evitar excesso de notação), consideraremos a partir daqui apenas os divisores positivos.

EXEMPLO 1A:

Como os divisores de 20 são 1, 2, 4, 5, 10 e 20, vale que $\tau(20)=6$.

EXEMPLO 1B:

Decorre diretamente da definição de número primo que $\tau(p)=2$, para qualquer primo p.

EXEMPLO 1C:

A tabela abaixo lista os valores de $\tau(n)$ para os 12 primeiros inteiros positivos.

n	1	2	3	4	5	6	7	8	9	10	11	12
$\tau(n)$	1	2	2	3	2	4	2	4	3	4	2	6

Do Teorema Fundamental da Aritmética, todo número inteiro positivo maior que 1 pode ser escrito de forma única como produto de primos. Seja, então, $n = p_1^{\alpha_1}.p_2^{\alpha_2}.....p_k^{\alpha_k}$. Pela transitividade da divisibilidade, um divisor de n tem fatoração em primos que aparecem na fatoração de n, de modo que podemos listar todos os divisores de um número pela escolha dos expoentes. Para cada p_i, o expoente pode variar de 0 até α_i, sendo, ao todo, $\alpha_i + 1$ possibilidades. Pelo Princípio Fundamental da Contagem (conforme estudado em Matemática Básica II), a quantidade de divisores de n será, então, $\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1)...(\alpha_k + 1)$.

GUARDE BEM ISSO!

Como os divisores de um número nunca são maiores que o próprio número, a quantidade de divisores também não passa desse número. Assim, vale $\tau(n) \leq n$ e a igualdade somente ocorre para os números 1 e 2.

EXEMPLO 2A:

Se p é primo, vale $\tau(p^k) = k + 1$, para qualquer inteiro positivo k.

EXEMPLO 2B:

Determine o menor número inteiro positivo n para o qual se tenha $\tau(n) = 5$.

Solução:

Se $n = p_1^{\alpha_1}.p_2^{\alpha_2}.....p_k^{\alpha_k}$, a equação $\tau(n) = 5$ é equivalente a $(\alpha_1 + 1)(\alpha_2 + 1)...(\alpha_k + 1) = 5$. Mas como 5 é primo, o produto do primeiro membro tem um fator igual a 5 e os outros iguais a 1, de modo que, assim, $\alpha_1 = 4$ e todos os outros expoentes são nulos, ou seja, $n = p_1^4$ para algum primo p. De modo a minimizar o valor de n, consideramos o menor primo. Dessa forma, o menor número inteiro positivo n para o qual se tenha $\tau(n) = 5$ é $n = 2^4 = 16$.

Outra função aritmética interessante que está relacionada com os divisores de um número é aquela que associa a cada inteiro positivo a soma dos seus divisores.

Definição 2: Denotaremos pela letra grega σ (sigma) a função que, para cada inteiro positivo n, associa o valor $\sigma(n) = \sum_{d|n} d$.

EXEMPLO 3A:

Como os divisores positivos de 10 são 1, 2, 5 e 10, é verdadeiro que $\sigma(10) = 18$.

EXEMPLO 3B:

Se p é um número primo, seus únicos divisores positivos são 1 e p. Dessa forma, para qualquer número primo p vale $\sigma(p) = p + 1$.

EXEMPLO 3C:

A tabela abaixo lista os valores de $\sigma(n)$ para os 12 primeiros inteiros positivos.

n	1	2	3	4	5	6	7	8	9	10	11	12
$\sigma(n)$	1	3	4	7	6	12	8	15	13	18	12	28

Se um número é da forma p^k, com p primo e k inteiro positivo, seus únicos divisores são $1, p, p^2, ..., p^k$. Assim, $\sigma(p^k) = 1 + p + p^2 + ... + p^k$. Temos aqui a soma dos $k+1$ primeiros termos de uma progressão geométrica de razão p e primeiro termo igual a 1. Considerando que a soma dos n primeiros termos de uma progressão geométrica com primeiro termo a_1 e razão $q \neq 1$ vale $S_n = \frac{a_1(q^n - 1)}{q - 1}$, podemos concluir que $\sigma(p^k) = \frac{p^{k+1} - 1}{p - 1}$.

EXEMPLO 4:

Uma vez que $512 = 2^9$ e com base no exposto acima, podemos calcular $\sigma(512) = \sigma(2^9) = \frac{2^{10} - 1}{2 - 1} = 1023$.

Antes de tratarmos de outras propriedades interessantes das funções σ e τ, vejamos o caso geral das funções multiplicativas.

Definição 3: A função f, cujo domínio é o conjunto dos inteiros positivos, é dita multiplicativa quando $f(m.n) = f(m).f(n)$ sempre que $(m,n) = 1$, ou seja, m e n são relativamente primos. Quando a propriedade $f(m.n) = f(m).f(n)$ for válida sempre, a função é dita completamente multiplicativa.

EXEMPLO 5A:

Como 1 é o elemento neutro para o produto, a função (constante) $f(n)=1$ para qualquer n é completamente multiplicativa.

EXEMPLO 5B:

A função identidade $f(n)=n$ é completamente multiplicativa.

Proposição 1: A função τ é multiplicativa.

Demonstração: Considere os números inteiros positivos m e n, com fatorações em primos $m=p_1^{\alpha_1}.p_2^{\alpha_2}.....p_k^{\alpha_k}$ e $n=q_1^{\beta_1}.q_2^{\beta_2}.....q_r^{\beta_r}$. Nessas condições, temos $\tau(m)=(\alpha_1+1)(\alpha_2+1)...(\alpha_k+1)$ e $\tau(n)=(\beta_1+1)(\beta_2+1)...(\beta_r+1)$. Se m e n forem relativamente primos, os primos de uma e de outra decomposição são distintos, de modo que $m.n=p_1^{\alpha_1}.p_2^{\alpha_2}.....p_k^{\alpha_k}.q_1^{\beta_1}.q_2^{\beta_2}.....q_r^{\beta_r}$ e não há simplificações nessa fatoração. Assim, temos:

$$\begin{aligned}\tau(mn) &= (\alpha_1+1)(\alpha_2+1)...(\alpha_k+1)(\beta_1+1)(\beta_2+1)...(\beta_r+1)= \\ &= \tau(m)\tau(n).\end{aligned}$$

Uma maneira alternativa de obter esse mesmo resultado é pela verificação de que, quando números são relativamente primos, os divisores do produto podem ser obtidos pela multiplicação dos divisores dos dois números, e, novamente pelo Princípio Fundamental da Contagem, a quantidade de divisores de mn será $\tau(m)\tau(n)$.

Observação: Como $\tau(1)=1$, o caso em que um dos números envolvidos no produto é 1, não analisado na demonstração acima, se torna óbvio, pois $\tau(1.m)=\tau(m)=1.\tau(m)=\tau(1)\tau(m)$. Dessa forma, omitiremos este caso também nas demonstrações sobre a multiplicabilidade das demais funções estudadas nesta aula.

Proposição 2: A função σ é multiplicativa.

Demonstração: Consideremos m e n números inteiros relativamente primos. Pela definição, temos $\sigma(mn)=\sum_{d|mn} d$. Entretanto, uma vez que os números são relativamente primos, cada divisor de mn pode ser escrito como produto de um divisor de m por um divisor de n. Assim, podemos escrever:

$$\sigma(mn)=\sum_{d|mn} d=\sum_{\substack{d_1|m \\ d_2|n}} d_1d_2=\sum_{d_1|m}\sum_{d_2|n} d_1d_2=\sum_{d_1|m} d_1.\sum_{d_2|n} d_2=\sigma(m)\sigma(n).$$

Assim, obtemos que σ é multiplicativa.

EXEMPLO 6:

Como $(9,10)=1$, valem

$\tau(90)=\tau(9.10)=\tau(9)\tau(10)=3.4=12$

e $\sigma(90)=\sigma(9.10)=\sigma(9)\sigma(10)=13.18=234$.

Observação: As funções τ e σ são multiplicativas, mas não são completamente multiplicativas. Veja, por exemplo, que $\tau(12)=6$, enquanto $\tau(2).\tau(6)=2.4=8$.

Como consequência da multiplicatividade da função σ, se $n=p_1^{\alpha_1}.p_2^{\alpha_2}.....p_k^{\alpha_k}$ é a decomposição em primos do inteiro positivo n, temos

$$\begin{aligned}\sigma(n) &= \sigma(p_1^{\alpha_1}.p_2^{\alpha_2}.....p_k^{\alpha_k})= \\ &= \sigma(p_1^{\alpha_1}).\sigma(p_2^{\alpha_2}).....\sigma(p_k^{\alpha_k}).\end{aligned}$$

Em seguida, pela expressão $\sigma(p^k)=\dfrac{p^{k+1}-1}{p-1}$ obtida antes do exemplo 4, conseguimos uma fórmula para calcular o valor de $\sigma(n)$. Temos, então:

$$\sigma(n)=\frac{p_1^{\alpha_1+1}-1}{p_1-1}.\frac{p_2^{\alpha_2+1}-1}{p_2-1}.....\frac{p_1^{\alpha_k+1}-1}{p_k-1}.$$

EXEMPLO 7:

Determine o valor de $\sigma(72)$.

Solução:

Pelo uso da fatoração $72=2^3.3^2$. De acordo com a fórmula anterior, obtemos:

$$\begin{aligned}\sigma(72) &= \sigma(2^3.3^2)=\sigma(2^3).\sigma(3^2)= \\ &= \frac{2^{3+1}-1}{2-1}.\frac{3^{2+1}-1}{3-1}=\frac{2^4-1}{1}.\frac{3^3-1}{2}= \\ &= 16-1.\frac{27-1}{2}=15.13=195.\end{aligned}$$

Outra maneira, talvez mais trabalhosa, seria listar todos os divisores de 72 e fazer sua soma, ou seja, $1+2+3+4+6+8+9+12+18+24+36+72=195$.

Com esse estudo das funções τ e σ, encerramos o tópico. No próximo, voltaremos a estudar a função ϕ definida na aula 3.

TÓPICO 2

A função ϕ de Euler

Objetivos

- Definir a função totiente de Euler e estudar suas características
- Generalizar o teorema de Fermat para todos os inteiros

Na aula 3, apresentamos a função que associa a cada número inteiro positivo a quantidade de inteiros positivos menores ou iguais a ele com os quais ele é relativamente primo. Recapitulando esta definição:

Definição: Denotaremos pela letra grega ϕ (phi) a função que, para cada inteiro positivo n, associa o valor $\phi(n) = \#\{k \in \mathbb{Z}; 0 < k < n \text{ e } (k,n) = 1\}$.

EXEMPLO 1A:

A tabela abaixo lista os valores de $\phi(n)$ para os 12 primeiros inteiros positivos.

n	1	2	3	4	5	6	7	8	9	10	11	12
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4

EXEMPLO 1B:

Para qualquer número primo p, vale $\phi(p) = p - 1$.

Pelo que vimos no tópico anterior, se uma função aritmética é multiplicativa, basta que saibamos como ela age nos números primos e nas potências de primos. Antes de verificar que ϕ é uma função multiplicativa, vejamos como encontrar o valor de $\phi(n)$, no caso de n ser potência de um primo, digamos $n = p^k$. Como o único divisor primo de p^k é p, para que $(m,n) = 1$, não deve aparecer o primo p na fatoração de m, ou seja, não pode ser um múltiplo de p, mas os múltiplos de p que são menores ou iguais a p^k são $p, 2p, 3p, \ldots, p^k = p^{k-1}p$, no total, portanto, de p^{k-1}. Assim, concluímos que $\phi(p^k) = p^k - p^{k-1}$.

Proposição 3: A função ϕ é multiplicativa.

Demonstração: Considere os inteiros positivos m e n, relativamente primos. Por definição, $\phi(mn)$ é a quantidade de números menores que mn e que lhe são relativamente primos. Comecemos por separar os elementos de $A = \{1, 2, \ldots, mn\}$ em suas *classes de congruência* módulo m, isto é, agruparemos em

$A_1 = \{a; 0 < a \leq mn \text{ e } a \equiv 1 (\text{mod } m)\}$;

$A_2 = \{a; 0 < a \leq mn \text{ e } a \equiv 2 (\text{mod } m)\}$;

...

$A_m = \{a; 0 < a \leq mn \text{ e } a \equiv m (\text{mod } m)\}$.

Uma vez que $\{1, 2, \ldots, m\}$ é um sistema completo de resíduos módulo m, todos os conjuntos descritos acima são disjuntos e a união de todos eles é o próprio $A = \{1, 2, \ldots, mn\}$. Para cada $r = 1, 2, \ldots m$, veja que, se m e r não forem relativamente primos, nenhum dos elementos de A_r será relativamente primo com mn, pois se m e r possuírem um divisor comum diferente de 1, então os números da forma $km + r$, que são os elementos de A_r, serão divisíveis por esse divisor comum, logo serão divisíveis por m e, pela transitividade da divisibilidade, serão também divisíveis por mn. Assim, A_r só conterá algum número relativamente primo com mn se $(m,r) = 1$. Mas de 1 a m, sabemos que há $\phi(m)$ destes números, pela definição da função totiente.

Estudemos agora dentro de cada um dos $\phi(m)$ conjuntos A_r destacados na primeira etapa quantos elementos são relativamente primos com mn. Observe que os elementos de cada A_r são da forma $km + r$. Como m e n são relativamente primos, cada conjunto A_r é um sistema completo de resíduos módulo n,

havendo, portanto, $\phi(n)$ elementos que são relativamente primos com n e, assim, com mn.

Dessa forma, temos $\phi(m)$ conjuntos e em cada um deles há $\phi(n)$ elementos relativamente primos com mn. Assim, no total, temos $\phi(m)\phi(n)$ elementos do conjunto $A=\{1,2,...,mn\}$, que são relativamente primos com mn. Mas esta é exatamente a definição de $\phi(mn)$ e por ela concluímos que $\phi(mn)=\phi(m)\phi(n)$.

EXEMPLO 2:

Como $81=3^4$, podemos escrever $\phi(81)=\phi(3^4)=3^4-3^3=81-27=54$.

EXEMPLO 3:

Como $(9,10)=1$, vale $\phi(90)=\phi(9.10)=\phi(9).\phi(10)=6.4=24$.

Agora que sabemos que a função ϕ é multiplicativa e sabemos calcular os seus valores para qualquer potência de primo, podemos usar o Teorema Fundamental da Aritmética para estabelecer uma fórmula geral para $\phi(n)$.

Observe, inicialmente, que, para p primo, obtivemos anteriormente $\phi(p^k)=p^k-p^{k-1}$, que pode ser reescrito como $\phi(p^k)=p^k\left(1-\frac{1}{p}\right)$. Considere, então, a fatoração em primos $n=p_1^{\alpha_1}.p_2^{\alpha_2}.....p_k^{\alpha_k}$. Usando a multiplicabilidade da função ϕ, podemos fazer:

$$\begin{aligned}
\phi(n) &= \phi(p_1^{\alpha_1}.p_2^{\alpha_2}.....p_k^{\alpha_k})= \\
&= \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2})...\phi(p_k^{\alpha_k})= \\
&= p_1^{\alpha_1}\left(1-\frac{1}{p_1}\right)p_2^{\alpha_2}\left(1-\frac{1}{p_2}\right)...p_k^{\alpha_k}\left(1-\frac{1}{p_k}\right)= \\
&= p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}.\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)...\left(1-\frac{1}{p_k}\right)= \\
&= n.\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)...\left(1-\frac{1}{p_k}\right).
\end{aligned}$$

Assim, para encontrarmos o valor de $\phi(n)$, basta que multipliquemos n pela expressão $\left(1-\frac{1}{p_k}\right)$ para cada um dos fatores primos p_k de sua decomposição.

EXEMPLO 4A:

Como 2 e 5 são os únicos primos na fatoração de 100, podemos fazer $\phi(100) = 100.\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 100.\frac{1}{2}.\frac{4}{5} = 40$.

EXEMPLO 4B:

Pela fatoração $72 = 2^3.3^2$, obtemos: $\phi(72) \quad = 72.\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) = 72.\frac{1}{2}.\frac{2}{3} = 24$.

As informações contidas neste tópico são, obviamente, apenas uma introdução às principais propriedades da função ϕ. No próximo tópico, estudaremos a função μ de Möbius.

TÓPICO 3

A função μ de Möbius

OBJETIVOS

- Reconhecer a função μ e algumas de suas propriedades
- Definir quando um número é livre de quadrados

O matemático e astrônomo alemão August Ferdinand Möbius (1790 – 1868) desenvolveu um trabalho de grande relevância na Matemática, especialmente no campo da Geometria, com a famosa faixa (ou fita) de Möbius, e nas Variáveis Complexas, com as transformações de Möbius. Na Teoria dos Números, deve-se a ele o estudo sobre a função que recebeu o seu nome e que apresentamos a seguir.

A função de Möbius (lê-se, aproximadamente, Mêbius) é alterada pela quantidade de primos que aparecem na fatoração de um número, mas, ao

Definição 5: Denotaremos pela letra grega μ (mi) a função que, para cada número inteiro positivo $n>1$, com fatoração em primos $n=p_1^{\alpha_1}.p_2^{\alpha_2}.....p_k^{\alpha_k}$, associa o número

$$\mu(n)=\begin{cases}(-1)^k, \text{ se } \alpha_1=\alpha_2=...=\alpha_k=1\\ 0, \text{ caso contrário}\end{cases}.$$

De modo a tornar μ definida para todos os inteiros positivos e não alterar a sua multiplicabilidade (ainda a ser demonstrada), definimos convenientemente $\mu(1)=1$.

Assim, a função $\mu(n)$ vale 0 sempre que n possuir, em sua fatoração em

primos, um expoente maior ou igual a 2. Neste caso, n é divisível pelo quadrado de algum primo. Mas para que seja divisível pelo quadrado de um inteiro maior que 1, um número deve também ser divisível pelo quadrado de um primo. Assim, quando $\mu(n) \neq 0$, dizemos que o inteiro n é *livre de quadrados*.

EXEMPLO 1A:

Como $30 = 2.3.5$, vale $\mu(30) = (-1)^3 = -1$, pois 30 tem 3 primos distintos em sua fatoração e nenhum dos expoentes é maior que 1. Analogamente, a fatoração $10 = 2.5$ leva a $\mu(10) = (-1)^2 = 1$.

EXEMPLO 1B:

Para qualquer primo p, tem-se $\mu(p) = -1$.

EXEMPLO 1C:

A tabela abaixo lista os valores de $\mu(n)$ para os 12 primeiros inteiros positivos.

n	1	2	3	4	5	6	7	8	9	10	11	12
$\mu(n)$	1	–1	–1	0	–1	1	–1	0	0	1	–1	0

Proposição 4: A função μ é multiplicativa.

Demonstração: Para os números inteiros positivos e relativamente primos m e n, temos duas possibilidades a considerar. Se m e n forem livres de quadrados, podemos escrever $m = p_1 p_2 \ldots p_k$ e $n = q_1 q_2 \ldots q_t$, onde os primos envolvidos são todos distintos, de modo que mn também será livre de quadrados. Daí, temos $mn = p_1 p_2 \ldots p_k q_1 q_2 \ldots q_k$ e, portanto,

$$\mu(mn) = (-1)^{k+t} = (-1)^k (-1)^t = \mu(m)\mu(n).$$

Se para algum primo p, tivermos $p^2 \mid mn$, isto é, mn não for livre de quadrados, o mesmo deve acontecer com m ou n, já que eles são relativamente primos. Assim, $\mu(m) = 0$ ou $\mu(n) = 0$, daí $\mu(mn) = 0 = \mu(m)\mu(n)$ e obtemos o mesmo resultado.

Nos tópicos anteriores, verificamos a multiplicabilidade de algumas funções de modo a obter uma expressão simplificada para o cálculo das imagens dessas funções quando sabemos a fatoração em primos do número. Com tal fatoração, o valor obtido na função μ é encontrado diretamente, de modo que a proposição

acima não será usada para a determinação de μ, mas como resultado auxiliar para outros fatos, como o que segue.

Proposição 5: Para qualquer número inteiro positivo $n>1$, vale $\sum_{d|n}\mu(d)=0$.

Demonstração: Comecemos com o caso $n=p^k$ para algum primo p. Os divisores de p^k são $1, p, p^2, ..., p^k$, logo:

$$\sum_{d|p^k}\mu(d)=\mu(1)+\mu(p)+\mu(p^2)+...+\mu(p^k)=$$
$$=1+(-1)+0+...+0=0.$$

Observe agora que, para m e n relativamente primos, procedemos de maneira semelhante ao que fizemos para provar que σ é multiplicativa. Acompanhe o raciocínio, no qual empregamos o fato de μ ser multiplicativa.

$$\sum_{d|mn}\mu(d)=\sum_{\substack{d_1|m\\ d_2|n}}\mu(d_1d_2)=\sum_{d_1|m}\sum_{d_2|n}\mu(d_1)\mu(d_2)=\sum_{d_1|m}\mu(d_1).\sum_{d_2|n}\mu(d_2).$$

Dessa feita, para $n=p_1^{\alpha_1}.p_2^{\alpha_2}.....p_k^{\alpha_k}$, vale

$\sum_{d|n}\mu(d)=\sum_{d_1|p^{\alpha_1}}\mu(d_1).\sum_{d_2|p^{\alpha_2}}\mu(d_2).....\sum_{d_k|p^{\alpha_k}}\mu(d_k)$. Mas cada um destes fatores é nulo, de onde temos o resultado válido para qualquer $n>1$.

Com esta propriedade, encerramos o estudo inicial das propriedades da função μ. Além de outros fatos interessantes sobre cada uma das funções estudadas nesta aula, há uma série de relações relevantes entre elas. Tais relações serão o foco de nossa próxima aula.

AULA 5

Funções aritméticas - parte II

Caro(a) aluno(a),

Na quinta aula de nosso curso de Teoria dos Números, daremos prosseguimento ao estudo das funções aritméticas, apresentando outras propriedades e, especialmente, algumas relações entre as funções aritméticas estudadas na aula 4, além de apresentar uma função especial, com domínio real, mas que desempenha papel relevante na análise dos números inteiros, tanto no estudo das funções aritméticas quanto no princípio das gavetas de Dirichlet, que será tema da aula 6.

Objetivos

- Prosseguir com o estudo das funções aritméticas
- Apresentar a função maior inteiro e algumas de suas propriedades

TÓPICO 1

Outras propriedades das funções aritméticas

OBJETIVO

- Apresentar algumas propriedades sobre as funções aritméticas

Neste tópico, continuaremos o estudo iniciado na aula 4, na qual associamos, para cada inteiro positivo n, os seguintes valores:

• $\tau(n)$, que é a quantidade de divisores positivos de n, por exemplo, $\tau(15)=4$. Assim,

$$\tau(n)=\#\{d\in\mathbb{Z}_+;d\,|\,n\}=\sum_{d|n}1$$

• $\sigma(n)$, que é a soma dos divisores positivos de n, por exemplo, $\sigma(15)=24$. Assim,

$$\sigma(n)=\sum_{d|n}d$$

ATENÇÃO!

Observação 1: Na fatoração do número 1 não aparece nenhum primo. Assim, podemos usar a definição ao lado também para o número 1, fazendo, portanto, $k=0$.

Observação 2: A quantidade de elementos do conjunto A pode ser representada por $\#A$, mas também há as notações $n(A)$, $|A|$ ou $card(A)$.

• $\phi(n)$, que é a quantidade de inteiros positivos menores que n e relativamente primos com n, por exemplo, $\phi(15)=8$. Assim,

$$\phi(n)=\#\{m\in\mathbb{Z}_+;m<n \text{ e } (m,n)=1\}$$

• $\mu(n)$, que é 0, se n não for livre de quadrados, e $(-1)^k$, se k for a quantidade de primos distintos que aparecem na fatoração de n, por exemplo, $\mu(15)=1$. Assim:

$$\mu(n)=\begin{cases}(-1)^k, \text{ se } n=p_1p_2\ldots p_k\\ 0, \text{ caso contrário}\end{cases}$$

Vimos que todas essas funções são multiplicativas, em particular $\tau(1)=\sigma(1)=\phi(1)=\mu(1)=1$. Vejamos agora outras propriedades interessantes sobre as funções aritméticas, que serão demonstradas tomando em conta o fato de que se $d\,|\,n$, então $a=\dfrac{n}{d}$ é inteiro e $a\,|\,n$.

Proposição 1: Para qualquer inteiro positivo n, vale $\prod_{d|n} d = n^{\tau(n)/2}$

Demonstração: Aqui basta verificar que sempre que $d\,|\,n$, então $a=\dfrac{n}{d}$ é inteiro e $a\,|\,n$. Assim, se

$Q=\prod_{d|n} d$, vale, igualmente, $Q=\prod_{d|n} \dfrac{n}{d}$. Daí, multiplicando as duas igualdades, temos $Q^2=\prod_{d|n} d\dfrac{n}{d}=\prod_{d|n} n$. No segundo membro, temos fatores todos iguais a n e tantos quantos forem os divisores de n, ou seja, há $\tau(n)$ fatores. Assim, $Q^2=n^{\tau(n)}$, e como $Q>0$, basta extrair a raiz quadrada nos dois membros da igualdade para obter o resultado.

Na expressão acima, poderíamos pensar que o resultado do segundo membro resultaria em um número não inteiro, caso $\tau(n)$ fosse ímpar. Mas $\tau(n)$ é obtido pelo produto dos consecutivos dos expoentes da fatoração em primos de n, de modo que somente resultará $\tau(n)$ ímpar se todos os expoentes da fatoração forem pares e, assim, n é quadrado perfeito e $n^{\tau(n)/2}$ é inteiro.

Proposição 2: Para todo inteiro positivo n, vale $\sum_{d|n} \phi(d)=n$.

Demonstração: Comecemos separando os números do conjunto $A=\{1,2,\ldots,n\}$ em subconjuntos de acordo com o segue:

$A_1=\{m\in A;(m,n)=1\}$;

$A_2=\{m\in A;(m,n)=2\}$;

...

$A_n=\{m\in A;(m,n)=n\}$.

Observe que no conjunto $A_k=\{m\in A;(m,n)=k\}$ será vazio se k não for um divisor de n. Assim, teremos $\tau(n)$ conjuntos não vazios e $A_n=\{n\}$. Agora analisemos a quantidade de elementos de A_d para cada divisor de n. Ora, para que $m\in A_d$ é necessário que $(m,n)=d$, mas isto significa que $\dfrac{m}{d}$ e $\dfrac{n}{d}$ são

inteiros sem divisores próprios comuns, ou seja, $(\frac{m}{d},\frac{n}{d})=1$. Dessa forma, cada conjunto A_d possui $\phi\left(\frac{m}{d}\right)$ elementos. Como os subconjuntos A_d assim formados são disjuntos, a quantidade de elementos da união de todos vale $\#\bigcup_{d|n} A_d = \sum_{d|n} \phi(n/d)$. Mas $\bigcup_{d|n} A_d = A$, que possui n elementos, de modo que temos a igualdade $\sum_{d|n} \phi(n/d) = n$. Mas, de novo usando o argumento de que quando d percorre os divisores de n, os valores de n/d também percorrem esses mesmos divisores, sem repetição, de modo que $\sum_{d|n} \phi(n/d) = \sum_{d|n} \phi(d)$, daí vale $\sum_{d|n} \phi(d) = n$.

Antes de prosseguir com outras propriedades das funções aritméticas, vamos estudar a função maior inteiro, que, embora não seja uma função com domínio no conjunto dos números inteiros, tem significativa importância na Teoria dos Números, como veremos a seguir.

TÓPICO 2

A função maior inteiro

OBJETIVO

- Apresentar a função maior inteiro

No estudo das funções aritméticas, uma nova função surge para desempenhar papel relevante, ainda que não seja, ela própria, aritmética no sentido de ter domínio no conjunto dos inteiros positivos. Com os conhecimentos elementares sobre o conjunto dos números reais, podemos trabalhar com a seguinte definição, que será fundamentada no seguinte argumento

Definição 1: Dado o número real x, representamos por $\lfloor x \rfloor$ o maior inteiro que é menor ou igual a x, equivalentemente, escrevemos: $\lfloor x \rfloor = \max\{n \in \mathbb{Z}; n \leq x\}$. A função $f : \mathbb{R} \to \mathbb{Z}$ dada por $f(x) = \lfloor x \rfloor$ é chamada de **função maior inteiro**. O valor $\lfloor x \rfloor$ também pode ser chamado de parte inteira de x.

EXEMPLO 1A:

Para qualquer número inteiro n , vale diretamente da definição que $\lfloor n \rfloor = n$, de modo que podemos concluir daqui que a função maior inteiro é sobrejetiva.

EXEMPLO 1B:

Valem as igualdades $\left\lfloor \sqrt{2} \right\rfloor = 1$, $\lfloor \pi \rfloor = 3$, $\lfloor e \rfloor = 2$ e $\lfloor -2,34 \rfloor = -3$.

EXEMPLO 1C:

A solução (real) da equação $\lfloor x \rfloor = 4$ é o intervalo $[4;5)$, de modo que podemos concluir daqui que a função maior inteiro não é injetiva, pois $\lfloor 4 \rfloor = \lfloor 4,1 \rfloor$.

EXEMPLO 1D:

Suponha que o número inteiro positivo M, quando escrito na base decimal, tenha a forma $M = (a_k \ldots a_1 a_0)_{10} = a_k.10^k + \ldots + a_1.10 + a_0$, com $a_k \neq 0$, ou seja, tenha $k+1$ algarismos. Temos aqui as desigualdades $10^k \leq M < 10^{k+1}$. Aplicando o logaritmo decimal, obtemos $k \leq \log M < k+1$, daí $\lfloor \log M \rfloor = k$ e, assim, a quantidade de algarismos de M na base decimal é $\lfloor \log M \rfloor + 1$. Mais geralmente, podemos verificar que a quantidade de algarismos usados para representar o número inteiro positivo M na base $B > 1$ será igual a $\lfloor \log_B M \rfloor + 1$.

EXEMPLO 1E:

Dados os inteiros positivos a e b, podemos, pelo algoritmo da divisão, encontrar inteiros q e r tais que $a = bq + r$, com $0 \leq r < b$. Assim, temos:

$\frac{a}{b} = \frac{bq}{b} + \frac{r}{b} = q + \frac{r}{b}$, de concluímos $\left\lfloor \frac{a}{b} \right\rfloor = \left\lfloor q + \frac{r}{b} \right\rfloor = q$, pois $0 \leq \frac{r}{b} < 1$.

Veja que para cada número inteiro n, a função maior inteiro é constante e vale n dentro do intervalo $[n;n+1)$. Assim, o gráfico da função maior inteiro é formado de segmentos de reta horizontais, de comprimento 1, de acordo com o que segue:

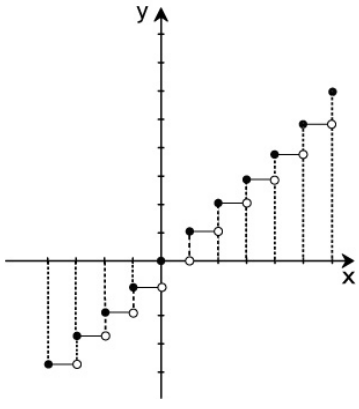

Figura 1: Representação da função maior inteiro

A respeito da função maior inteiro, valem as seguintes propriedades, cujas demonstrações são deixadas como exercício.

(1) $\lfloor x+n\rfloor=\lfloor x\rfloor+n$, para qualquer real x e qualquer inteiro positivo n.

(2) $x-1<\lfloor x\rfloor\leq x$, para qualquer real x.

(3) Se x não é um número inteiro, então $\lfloor -x\rfloor=-\lfloor x\rfloor-1$.

(4) $\lfloor\lfloor x\rfloor\rfloor=\lfloor x\rfloor$, para qualquer real x.

(5) Se $x<y$, então $\lfloor x\rfloor\leq\lfloor y\rfloor$.

(6) $\lfloor x\rfloor+\lfloor y\rfloor\leq\lfloor x+y\rfloor\leq\lfloor x\rfloor+\lfloor y\rfloor+1$, para quaisquer reais x e y.

Observação 1: A propriedade (4) pode ser reescrita nos seguintes termos: se $f(x)=\lfloor x\rfloor$, então $f(f(x))=f(x)$. Uma função que satisfaz a propriedade $f(f(x))=f(x)$ para qualquer elemento do domínio é dita *idempotente*.

Observação 2: A propriedade (5) pode ser reescrita nos seguintes termos: se $f(x)=\lfloor x\rfloor$, então $x<y\Rightarrow f(x)\leq f(y)$. Uma função que satisfaz a propriedade $x<y\Rightarrow f(x)\leq f(y)$ para quaisquer elementos do domínio é dita *monótona não decrescente*. Se $x<y\Rightarrow f(x)\geq f(y)$, então f é *monótona não crescente*.

EXEMPLO 2A:

Sabendo que $\lfloor x\rfloor=4$, determine os possíveis valores de $\lfloor 3x\rfloor$.

Solução:

Observe que $\lfloor x\rfloor=4$ se verifica para todos os valores $x\in[4;5)$, isto é, $\lfloor x\rfloor=4\Leftrightarrow 4\leq x<5$, de onde obtemos que $12\leq 3x<15$, daí os possíveis valores para $\lfloor 3x\rfloor$ são 12, 13 e 14.

GUARDE BEM ISSO!

Podemos usar a função maior inteiro para estender as funções aritméticas estudadas na aula 4 para todos os números reais, definindo, por exemplo, $\phi(x)=\phi(\lfloor x\rfloor)$ para qualquer número real, embora esta extensão não acrescente fatos significativos à nossa teoria.

EXEMPLO 2B:

Se a e b são números reais tais que $\lfloor a\rfloor=6$ e $\lfloor b\rfloor=-3$, encontre o menor valor possível para $\lfloor 2a+3b\rfloor$.

Solução:

Inicialmente temos que $\lfloor a\rfloor=6\Leftrightarrow 6\leq a<7$ e $\lfloor b\rfloor=-3\Leftrightarrow -3\leq b<-2$. Daí, multiplicando por 2 e 3, respectivamente, obtemos $12\leq 2a<14$ e $-9\leq 3b<-6$ e somando estes resultados, concluímos que $3\leq 2a+3b<8$. Assim, o menor valor possível para $\lfloor 2a+3b\rfloor$ é 3 e o maior valor possível é 7.

Também é interessante perceber que, dados os inteiros positivos a e b, a quantidade de números menores ou iguais a a que são divisíveis por b é $\left\lfloor \frac{a}{b} \right\rfloor$.

Vistas as propriedades iniciais a respeito da função maior inteiro, vamos voltar às funções aritméticas e mais algumas relações entre elas.

TÓPICO 3

Outras relações

OBJETIVOS

- Estudar outras relações entre as funções aritméticas
- Relacionar as funções aritméticas e a função maior inteiro

Vejamos agora algumas outras relações entre a Teoria dos Números e a função maior inteiro.

Proposição 3: Se n é um número inteiro positivo e p é primo, então $p^{\alpha} \mid n!$ se, e somente se, $\alpha \leq \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + ... + \left\lfloor \frac{n}{p^k} \right\rfloor$, onde k é o maior inteiro para o qual $p^k \leq n$. Alternativamente, a maior potência de p que divide $n!$ é $\alpha = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + ... + \left\lfloor \frac{n}{p^k} \right\rfloor$.

Demonstração: Observe inicialmente que poderíamos ter acrescentado qualquer potência de p à soma $\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + ... + \left\lfloor \frac{n}{p^k} \right\rfloor$, pois se $p^k > n$, vale $\left\lfloor \frac{n}{p^k} \right\rfloor = 0$. Denote por a_i a quantidade de números menores ou iguais a n que são divisíveis por p^i.

Como $n! = 1.2.....n$, então teremos que $\alpha = a_1 + a_2 + ... + a_k$, mas os números naturais que são divisíveis por p^i são $p^i, 2.p^i, 3.p^i, ..., \left\lfloor \frac{n}{p^i} \right\rfloor .p^i$. Assim, $a_i = \left\lfloor \frac{n}{p^i} \right\rfloor$ e $\alpha = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + ... + \left\lfloor \frac{n}{p^k} \right\rfloor$, como desejado.

EXEMPLO 1A:

Se quisermos saber qual a maior potência de 2 que divide 21! fazemos

$$\alpha = \left\lfloor \frac{21}{2} \right\rfloor + \left\lfloor \frac{21}{4} \right\rfloor + \left\lfloor \frac{21}{8} \right\rfloor + \left\lfloor \frac{21}{16} \right\rfloor = \\ = 10 + 5 + 2 + 1 = 18.$$

Assim, $2^{18} \mid 21!$ e, logo, $2^k \mid 21!$, para qualquer $k = 0,1,...,18$.

ATENÇÃO!

A proposição 3 apenas conta quantos números de 1 a n são divisíveis por p, depois conta quantos são divisíveis por p^2 e assim sucessivamente.

EXEMPLO 1B:

A maior potência de 5 que divide 19! é $\left\lfloor \frac{19}{5} \right\rfloor = 3$. De fato, dos números inteiros de 1 a 19, apenas 5, 10 e 15 são múltiplos de 5, e nenhum deles é múltiplo de 25.

Adiante, veremos uma relação entre as funções ϕ e μ.

Proposição 4: Para qualquer inteiro positivo n, vale $\phi(n) = \sum_{d \mid n} \mu(d).\frac{n}{d}$.

Demonstração: Veja que para $m \in \{1,2,...,n\}$, temos $\left\lfloor \frac{1}{(m,n)} \right\rfloor = 1$, se m e n forem relativamente primos e $\left\lfloor \frac{1}{(m,n)} \right\rfloor = 0$, caso contrário. Assim, obtemos uma nova maneira de obter o valor $\phi(n)$, através da igualdade $\phi(n) = \sum_{k=1}^{n} \left\lfloor \frac{1}{(k,n)} \right\rfloor$.

Vimos no final da aula 4 que $\sum_{d \mid n} \mu(d) = 0$ para qualquer inteiro positivo $n > 1$.

Uma vez que $\sum_{d \mid 1} \mu(d) = 1$, podemos sintetizar as duas informações com a igualdade $\sum_{d \mid n} \mu(d) = \left\lfloor \frac{1}{n} \right\rfloor$, válida para qualquer inteiro positivo n. Logo $\sum_{d \mid (k,n)} \mu(d) = \left\lfloor \frac{1}{(k,n)} \right\rfloor$.

Fazendo uso dessa última igualdade em $\phi(n) = \sum_{k=1}^{n} \left\lfloor \frac{1}{(k,n)} \right\rfloor$, obtemos:

$\phi(n) = \sum_{k=1}^{n} \sum_{d \mid (k,n)} \mu(d)$.

Agora, se $d \mid (n,k)$, é verdade também que $d \mid n$ e $d \mid k$, de modo que podemos ainda escrever:

$$\phi(n)=\sum_{k=1}^{n}\sum_{\substack{d|k\\ d|n}}\mu(d)\,.$$

Sabemos que $d\,|\,k$ equivale a existir um inteiro q tal que $k=qd$, mas para $1\le k\le n$, temos $1\le q\le\frac{n}{d}$. Daí, obtemos:

$\phi(n)=\sum_{d|n}\sum_{q=1}^{n/d}\mu(d)=\sum_{d|n}\left(\mu(d).\sum_{q=1}^{n/d}1\right)=\sum_{d|n}\left(\mu(d).\frac{n}{d}\right)$, o que completa a demonstração.

EXEMPLO 2:

Com a expressão obtida anteriormente, podemos encontrar $\phi(n)$ de outra maneira. Veja que $\phi(20)=\sum_{d|n}\mu(d).\frac{20}{d}$. Como os divisores inteiros positivos de 20 são 1, 2, 4, 5, 10 e 20, podemos fazer:

$$\phi(20)=\mu(1).\frac{20}{1}+\mu(2).\frac{20}{2}+\mu(4).\frac{20}{4}+\mu(5).\frac{20}{5}+\mu(10).\frac{20}{10}+\mu(20).\frac{20}{20}$$

Mas 4 e 20 não são livres de quadrados, logo $\mu(4)=\mu(20)=0$. Além disso, 2 e 5 são primos, de onde temos $\mu(2)=\mu(5)=-1$ e, pela definição, temos $\mu(1)=\mu(10)=1$. Assim:

$$\begin{aligned}\phi(20) \quad &=1.\frac{20}{1}+(-1).\frac{20}{2}+0.\frac{20}{4}+(-1).\frac{20}{5}+1.\frac{20}{10}+0.\frac{20}{20}=\\ &=20-10+0-4+2+0=8.\end{aligned}$$

Com este tópico, encerramos nossa aula. Para melhor compreensão das ideias sobre as funções aritméticas e da função maior inteiro, recomenda-se uma recapitulação dos exemplos, com a troca dos números para melhor fixação dos conceitos e relações.

Como peças fundamentais da nossa teoria, vez por outra, revisitaremos as funções aritméticas, nesta ou em outras disciplinas. Na próxima aula, também voltaremos a aplicar a função maior inteiro.

AULA 6

O princípio das gavetas

Caro(a) aluno(a),

Em nossa quarta aula, estudaremos o princípio das gavetas, o qual afirma que, se você tiver $n+1$ objetos em n gavetas, pelo menos uma dela conterá mais de um objeto. É uma afirmação simples e pode até ser considerada óbvia, mas traz consequências de grande relevância.

Objetivos

- Apresentar o Princípio de Dirichlet e problemas nos quais o princípio pode ser aplicado
- Destacar resultados do Princípio de Dirichlet na Teoria dos Números

TÓPICO 1

Introdução

Objetivos

- Apresentar exemplos iniciais
- Enunciar formalmente o princípio

O matemático Johann Dirichlet (1805 - 1859) provou um caso particular ($n=5$) do teorema de Fermat (veja comentário no início do tópico 2 da aula 3). Com seus estudos, ele proporcionou outras inúmeras contribuições para a Matemática e a Estatística, dentre elas o princípio que norteará nossa aula – o qual pode ser colocado nos seguintes termos: se $n+1$ pombos forem colocados em n gaiolas, pelo menos uma das gaiolas conterá pelo menos dois pombos. Obviamente o resultado continua valendo para qualquer quantidade de pombos que seja superior à quantidade de gaiolas. Descrevendo mais tecnicamente, podemos enunciar da seguinte forma:

Princípio de Dirichlet: Se A e B são conjuntos finitos e A tem mais elementos que B, então não pode haver uma função injetiva $f: A \to B$, isto é, haverá elementos distintos $x, y \in A$ tais que $f(x) = f(y)$.

Observe que, se P for o conjunto de $n+1$ pombos e G o conjunto de n gaiolas, a função que associa cada pombo à sua gaiola não pode ser injetiva, de onde obtemos, naturalmente, o mesmo resultado, isto é, que dois pombos (pelo menos) devem ocupar a mesma gaiola.

EXEMPLO 1A:

Em uma turma de 13 pessoas, necessariamente duas delas fazem aniversário no mesmo mês. Para verificar isso, podemos pensar nas pessoas como os "objetos" e os meses como as "gavetas". Ao distribuir 13 pessoas nos doze meses do ano, necessariamente um dos meses deveria "conter" pelo menos duas pessoas.

EXEMPLO 1B:

Em uma lista de 6 números inteiros quaisquer, pelo menos dois deles deixam o mesmo resto na divisão por 5, pois os restos possíveis são 0, 1, 2, 3 ou 4. Nesse caso, temos seis números para "distribuir" em 5 possíveis restos. Usando a notação de função, basta considerar a função que associa cada um dos seis números dados ao seu resto na divisão por 5.

EXEMPLO 1C:

Em um parágrafo com 27 palavras, pelo menos duas delas começaram com a mesma letra.

EXEMPLO 1D:

No interior de um quadrado de lado 2m, são marcados cinco pontos. Se dividirmos o quadrado em quatro quadrados menores de lado 1m – e consequentemente de diagonal $\sqrt{2} \cong 1,41$ m – podemos associar cada ponto ao quadrado menor que o contém. Pelo princípio de Dirichlet, haverá pelo menos dois pontos no mesmo quadrado, mas a distância máxima entre dois pontos de um quadrado é a medida da sua diagonal, assim haverá pelo menos dois pontos que estarão a uma distância inferior a $\sqrt{2}$ m.

É com a ideia do princípio de Dirichlet e com algumas generalizações que vamos trabalhar do decorrer desta aula. A obviedade do princípio indica a simplicidade das demonstrações, sendo que a parte difícil (que deixa de ser difícil com um pouco de prática) é identificar, dentro do problema dado, o que são os "objetos" e as "gavetas" ou, equivalentemente, entre quais conjuntos vamos definir a função que não será injetiva.

EXEMPLO 2A:

Mostre que há um múltiplo de 19 cuja representação decimal contenha apenas algarismos 0 e 1.

Solução:

Considere a sequência dos números formados apenas por algarismos 1:

1, 11, 111, ...

Se da lista considerarmos os 20 primeiros números, necessariamente dois deles deverão deixar o mesmo resto na divisão por 19. Para tanto, basta considerar a função que associa cada número ao resto da sua divisão por 19, que são apenas 19 possibilidades. Sabemos que, se dois números deixam o mesmo resto na divisão por 19, então a subtração entre eles deixa resto 0, ou seja, é múltiplo de 19 (lembre que $a \equiv b(\text{mod}19)$ equivale a $19 \mid a-b$). Mas a subtração de dois dos números considerados gera um número formado apenas pelos algarismos 1 e 0, como desejado.

EXEMPLO 2B:

Mais geralmente, dado o inteiro positivo n e um algarismo $\alpha \in \{1,2,...,9\}$, podemos encontrar um múltiplo de n cuja representação decimal contenha apenas os algarismos 0 e α. Para tanto, basta considerar os $n+1$ primeiros termos da sequência dos números formados pela justaposição de algarismos α, isto é, $\alpha, \alpha\alpha, ..., \alpha\alpha...\alpha$, com o último número tendo $n+1$ algarismos todos iguais a α e aplicar o raciocínio descrito anteriormente.

Alternativamente, podemos exprimir a ideia contida no princípio das gavetas também dizendo que, se tivermos n gavetas, a quantidade mínima de objetos a serem postos nas gavetas de modo a assegurar que haja pelo menos uma gaveta com pelo menos dois objetos é $n+1$.

EXEMPLO 3A:

Em uma urna, há 7 bolas pretas, 5 bolas brancas e 10 bolas azuis. Qual a quantidade mínima de bolas que devem ser retiradas às cegas para se garantir que há duas bolas da mesma cor?

Solução:

Aqui temos o conjunto das bolas retiradas e para cada uma delas podemos associar uma cor. Como há três cores possíveis, devemos tirar 4 bolas para garantir que essa função não seja injetiva, ou seja, para termos certeza de que duas bolas tenham a mesma cor.

EXEMPLO 3B:

O conjunto S é formado por todos os inteiros que são relativamente primos com 18. Determine a quantidade mínima de elementos de S que devem ser tomados para que haja dois deles cuja diferença é divisível por 18.

Solução:

Para que a diferença entre dois números seja um múltiplo de 18, eles devem deixar o mesmo resto na divisão por 18 e os restos possíveis nessa divisão são 0, 1, 2, ..., 17, de onde poderíamos pensar que a resposta seria "no mínimo 19 números". Entretanto devemos atentar para o fato de que não estamos considerando números inteiros quaisquer, mas apenas aqueles que são relativamente primos com 18, de modo que o conjunto de "gavetas" não contém todos os resíduos possíveis (não é um sistema completo), mas apenas aqueles que são primos com 18 (um sistema reduzido). Assim, temos $\phi(18)$ possibilidades para esses resíduos. Como $\phi(18) = 6$, a quantidade mínima de elementos de S que devem ser tomados para que se tenha a certeza de haver dois cuja diferença seja um múltiplo de 18 é 7.

Seguindo as ideias contidas nos exemplos deste tópico, podemos construir uma série de outros. Um exercício interessante é colecionar esses exemplos e discutir como o princípio de Dirichlet pode ser aplicado. Adiante, discutiremos como podemos generalizar os raciocínios envolvidos.

TÓPICO 2

Generalização do princípio das gavetas

OBJETIVOS

- Estudar situações generalizadas do problema das gavetas
- Aplicar a função maior inteiro nas soluções

Continuando com o princípio discutido no tópico anterior, podemos pensar que se $nk+1$ objetos forem colocados em n gavetas, então pelo menos uma das gavetas conterá $k+1$ objetos. Esse fato pode ser demonstrado se agruparmos os $nk+1$ em n grupos de k objetos e mais um objeto avulso. Temos aí $n+1$ grupos de objetos para serem colocados em n gavetas, de onde pelo menos uma gaveta deverá conter pelo menos dois desses grupos, ou seja, no mínimo $k+1$ objetos.

Princípio de Dirichlet (generalização) Se A e B são conjuntos com $nk+1$ (ou qualquer quantidade superior a nk) e n elementos, respectivamente, e $f: A \to B$ é uma função, então haverá um elemento de B que é imagem de pelo menos $k+1$ elementos de A.

EXEMPLO 1A:

Em um grupo de 36 pessoas, há pelo menos seis delas que fazem aniversário no mesmo dia da semana em 2010. Para tanto, basta verificar que os dias da semana (as gavetas) são 7 e as pessoas (objetos) são 36 = 5.7 + 1, de modo que o princípio pode ser aplicado e haverá pelo menos um dia correspondente a 6 pessoas.

EXEMPLO 1B:

Mostre que de um conjunto de 41 números distintos, podemos escolher cinco cuja soma é um múltiplo de 5.

Solução:

Se somarmos cinco números congruentes módulo 5, teremos necessariamente um múltiplo de 5 como resultado. Observe que, se $a_i \equiv k(\text{mod}\,5)$ para qualquer elemento do conjunto $\{a_1, a_2, ...a_5\}$, então a soma das congruências levará a $a_1 + a_2 + ... + a_5 \equiv 5k(\text{mod}\,5)$, mas $5k$ é um múltiplo de 5, daí $a_1 + a_2 + ... + a_5 \equiv 0(\text{mod}\,5)$, sendo a soma também um múltiplo de 5. Agora temos que garantir a existência de pelo menos cinco números que deixam o mesmo resto na divisão por 5. Os restos possíveis são 5 (as gavetas) e os números (objetos) são 21 = 4.5 + 1. Usando o princípio para $n = 5$ e $k = 4$, garantimos que há pelo menos 5 números que deixam o mesmo resto na divisão por 5. Analogamente, podemos estabelecer a função que associa cada número ao resto na divisão por 5 e usar a formulação em termos de função para o princípio de Dirichlet e obter o mesmo resultado.

Assim como feito no tópico anterior, também podemos obter a quantidade mínima de objetos a serem considerados para que tenhamos pelo menos uma gaveta com uma quantidade pré-estabelecida de objetos, depois da distribuição.

EXEMPLO 2A:

Cada um dos dez alunos de uma turma recebe uma cartela com quatro números inteiros positivos, distintos e menores ou iguais a 40, de modo que cada número aparece em apenas uma cartela. Serão sorteados sucessivamente os números de uma urna, um por um, até que um dos alunos preencha sua cartela, caso em que será determinado vencedor. Qual a quantidade máxima de números sorteados nessa atividade?

Solução:

Obviamente, pode acontecer de os quatro primeiros números sorteados estarem na cartela de apenas um aluno, mas o sorteio pode continuar. Aqui queremos saber a quantidade mínima de números que devem ser sorteados para que se tenha certeza de que pelo menos um deles tenha 4 números. Se pensarmos nos números como os objetos e nas cartelas como as gavetas, queremos que cada uma delas tenha 4, ou seja, 3 + 1 objetos. Como são 10 cartelas ao todo, podemos fazer $n = 10$ e $k = 3$, assim com a quantidade de $nk + 1 = 31$ números sorteados, teremos certeza de ter um aluno vencedor, então não chegaremos a sortear o 32º número.

EXEMPLO 2B:

Determine a quantidade mínima de pessoas que devem ser tomadas para que se possa formar um grupo de cinco pessoas com aniversário no mesmo mês.

Solução:

Aqui podemos pensar em $n=12$ (os meses como as gavetas) e $k+1=7$ (a quantidade mínima de objetos que queremos garantir em pelo menos uma das gavetas). Assim, para $k=6, n=12$, temos que em um grupo de $nk+1=73$ pessoas, há necessariamente um grupo de cinco com aniversário no mesmo mês.

Para o que segue da nossa teoria, faremos uso da função maior inteiro e de suas propriedades estudadas na aula 5. Lembremos que, dado o número real x, representamos por $\lfloor x \rfloor$ o maior inteiro que é menor ou igual a x. Por exemplo: $\lfloor 3,78 \rfloor = 3$.

A proposição a seguir é uma reformulação do princípio de Dirichlet, versão generalizada, acompanhada de uma demonstração.

Proposição 1: Se colocarmos k objetos em n gavetas, então pelo menos uma gaveta conterá pelo menos $\left\lfloor \frac{k-1}{n} \right\rfloor + 1$ objetos.

Demonstração: Da definição da função maior inteiro, vale $\lfloor x \rfloor \leq x$, para qualquer x real, logo

$$\left\lfloor \frac{k-1}{n} \right\rfloor \leq \frac{k-1}{n}$$

Supondo que cada gaveta contenha no máximo $\left\lfloor \frac{k-1}{n} \right\rfloor$ objetos. Assim, teremos, no máximo, $n.\left\lfloor \frac{k-1}{n} \right\rfloor$ objetos. Então:

$$n.\left\lfloor \frac{k-1}{n} \right\rfloor \leq n.\frac{k-1}{n} = k-1 < k$$

Assim, a quantidade de objetos nunca chegaria a k, o que é uma contradição.

EXEMPLO 3A:

Se observarmos os meses de nascimento de um grupo de 50 pessoas, temos $k=50$ e $n=12$, assim podemos garantir que haverá pelo menos um mês com $\left\lfloor \frac{50-1}{12} \right\rfloor + 1 = 4+1 = 5$ pessoas, ou seja, podemos concluir que, de um grupo de

50 pessoas, poderemos certamente escolher cinco que fazem aniversário no mesmo mês.

EXEMPLO 3B:

De um conjunto de 100 números, podemos garantir que há pelo menos 8 números que deixam o mesmo resto na divisão por 13. Basta usar aqui $k = 100$ e $n = 13$.

Com essa formulação geral do princípio de Dirichlet, encerramos este tópico. No próximo, veremos como aplicá-lo de outras maneiras também interessantes.

TÓPICO 3

Exemplos gerais

Objetivos

- Estudar situações generalizadas do problema das gavetas
- Aplicar a função maior inteiro nas soluções

Para finalizar nossa aula, vejamos como princípio de Dirichlet pode ser aplicado em outras situações.

EXEMPLO 1:

Se o plano for pintado de verde e azul, prove que haverá dois pontos de mesma cor cuja distância é exatamente 1 metro.

Solução:

Basta construir um triângulo equilátero de lado 1 m. Os vértices do triângulo (3) são em quantidade maior que o de cores possíveis (2), logo haverá dois vértices de mesma cor.

EXEMPLO 2:

Os números inteiros de 1 a 10 são escritos em um círculo, em qualquer ordem. Mostre que há três números adjacentes cuja soma é maior ou igual a 17.

Solução:

Podemos formar 10 sequências diferentes de três números adjacentes, de modo que, se somarmos todas as sequências possíveis, cada números aparecerá 3 vezes. A soma total será, portanto, $3.(1 + 2 + ... + 10) = 3.55 = 165$. Se todas as somas de três números adjacentes forem menores que 17, a soma total seria, no máximo, $10.16 = 160$, o que não é verdade. Logo uma das sequências, pelo menos, deve ter soma maior ou igual a 17.

EXEMPLO 3:

Prove que há duas potências de 3, distintas, cuja diferença é divisível por 2011.

Solução:

Considere o conjunto formado pelas 2012 primeiras potências de 3, isto é:

$$3^1, 3^2, 3^3, \ldots, 3^{2012}.$$

Como o número de elementos do conjunto é maior que a quantidade de possíveis restos na divisão por 2011, haverá dois deles congruentes módulo 2011, ou seja, dois deles deixam mesmo resto na divisão por 2011. Isto é, há inteiros positivos m, n distintos tais que $3^m \equiv 3^n \pmod{2011}$, ou seja, $2011 \mid 3^m - 3^n$.

EXEMPLO 4:

Qual a quantidade mínima de brasileiros que devemos escolher para garantir que se possa formar um grupo com 6 pessoas que nasceram na mesma unidade da federação (total de 27)?

Solução:

Aqui usamos a formulação geral do princípio de Dirichlet, para $n = 27$ e $k = 5$, de modo que o mínimo de pessoas a serem selecionada para se ter certeza da propriedade desejada é $27.5 + 1 = 136$.

Com essas ideias, encerramos a nossa aula. A sugestão é sempre buscar novos exemplos para complementar a teoria, bem como novos problemas que possam ser resolvidos como princípio apresentado aqui, sempre com o cuidado de identificar os "objetos" (ou pombos) e as "gavetas" (ou casas).

AULA 7

Resíduos quadráticos

Caro(a) aluno(a),

Dando prosseguimento ao estudo da Teoria dos Números, em nossa sétima aula, continuaremos analisando as propriedades das congruências e verificando as condições que assegurem a existência de soluções para equações de tipo específico.

Objetivos

- Estudar os resíduos quadráticos e o símbolo de Legendre
- Apresentar a lei da reciprocidade quadrática

TÓPICO 1

Resíduos quadráticos

Objetivos

- Definir os resíduos quadráticos
- Obter a quantidade de resíduos quadráticos

Aqui serão estudadas as equações do tipo $x^2 \equiv a(\mathrm{mod}\, n)$, o que pode ser interpretado como o problema de encontrar raízes quadradas módulo n de um número inteiro positivo a. Pelo que sabemos sobre sistemas completos de resíduos, as soluções da equação dada só precisam ser procuradas no conjunto $\{0,1,2,\ldots,n-1\}$.

EXEMPLO 1:

Encontre todas as soluções da equação $x^2 \equiv 1(\mathrm{mod}\, 5)$.

Solução:

Analisemos os casos:

$\rightarrow$ se $x \equiv 0(\mathrm{mod}\, 5)$, então $x^2 \equiv 0(\mathrm{mod}\, 5)$ e, assim, $x^2 \not\equiv 1(\mathrm{mod}\, 5)$

$\rightarrow$ se $x \equiv 1(\mathrm{mod}\, 5)$, então $x^2 \equiv 1(\mathrm{mod}\, 5)$ e, assim, os números da forma $x \equiv 5k+1$, com k inteiro são soluções para o problema

$\rightarrow$ se $x \equiv 2(\mathrm{mod}\, 5)$, então $x^2 \equiv 4(\mathrm{mod}\, 5)$ e, assim, $x^2 \not\equiv 1(\mathrm{mod}\, 5)$

$\rightarrow$ se $x \equiv 3(\mathrm{mod}\, 5)$, então $x^2 \equiv 4(\mathrm{mod}\, 5)$ e, assim, $x^2 \not\equiv 1(\mathrm{mod}\, 5)$

$\rightarrow$ se $x \equiv 4(\mathrm{mod}\, 5)$, então $x^2 \equiv 1(\mathrm{mod}\, 5)$ e, assim, os números da forma $x \equiv 5k+4$, com k inteiro são soluções para o problema.

Portanto, as soluções para a equação dada são os números da forma $x \equiv 5k+1$ ou $x \equiv 5k+4$, com k inteiro. Uma vez que $4 \equiv -1 (\mathrm{mod}\, 5)$, podemos escrever a solução geral $x = 5k \pm 1$.

Pelo que foi visto no exemplo anterior, para qualquer número inteiro n, vale $n^2 \equiv 0 (\mathrm{mod}\, 5)$, $n^2 \equiv 1 (\mathrm{mod}\, 5)$ ou $n^2 \equiv 4 (\mathrm{mod}\, 5)$ e as equações $x^2 \equiv 2 (\mathrm{mod}\, 5)$ e $x^2 \equiv 3 (\mathrm{mod}\, 5)$ não possuem soluções. Motivados por essa situação, daremos, em relação ao conjunto dos possíveis restos na divisão por 5, um destaque aos números 1 e 4, que serão chamados de resíduos quadráticos módulo 5.

Definição 1: Dados os números inteiros positivos a e n, relativamente primos, dizemos que a é um *resíduo quadrático módulo* n se a equação $x^2 \equiv a (\mathrm{mod}\, n)$ possuir soluções.

EXEMPLO 2A:

Os números 1 e 4 são resíduos quadráticos módulo 5. Também 21 é resíduo quadrático módulo 5.

EXEMPLO 2B:

Veja inicialmente que

$$x \equiv 0 (\mathrm{mod}\, 6) \Rightarrow x^2 \equiv 0 (\mathrm{mod}\, 6)$$
$$x \equiv 1 (\mathrm{mod}\, 6) \Rightarrow x^2 \equiv 1 (\mathrm{mod}\, 6)$$
$$x \equiv 2 (\mathrm{mod}\, 6) \Rightarrow x^2 \equiv 4 (\mathrm{mod}\, 6)$$
$$x \equiv 3 (\mathrm{mod}\, 6) \Rightarrow x^2 \equiv 3 (\mathrm{mod}\, 6)$$
$$x \equiv 4 (\mathrm{mod}\, 6) \Rightarrow x^2 \equiv 4 (\mathrm{mod}\, 6)$$
$$x \equiv 5 (\mathrm{mod}\, 6) \Rightarrow x^2 \equiv 1 (\mathrm{mod}\, 6)$$

Assim, somente para $a = 0, 1, 3, 4$ a equação $x^2 \equiv a (\mathrm{mod}\, 6)$ possui solução inteira, mas 3 e 4 não são relativamente primos com 6, e 0 não é positivo, de modo que 1 é o único resíduo quadrático módulo 6 (a menos de congruência módulo 6).

Proposição 1: Se a é um resíduo quadrático módulo m, e b é um resíduo quadrático módulo n, com m, n relativamente primos, então a equação $z^2 \equiv ab (\mathrm{mod}\, mn)$ possui solução.

Demonstração: Pela definição, temos que existem inteiros x, y tais que

$$x^2 \equiv a(\text{mod}\, m) \text{ e } y^2 \equiv b(\text{mod}\, n)$$

Uma vez que $(m,n)=1$, vale $x^2y^2 \equiv ab(\text{mod}\, mn)$, ou seja, a equação $z^2 \equiv ab(\text{mod}\, mn)$ possui, pelo menos, a solução xy.

Pelo exposto na proposição acima, podemos procurar os resíduos quadráticos módulo n, procurando os resíduos quadráticos referentes aos divisores de n. Assim, se n for composto, podemos reduzir o problema para os seus divisores primos. Portanto, a partir de agora, consideraremos apenas as equações $x^2 \equiv a(\text{mod}\, p)$, com p primo, caso em que também não nos ateremos à condição de serem relativamente primos, pois todos os números inteiros positivos menores que p, primo, são-lhe relativamente primos.

Além disso, o caso $p=2$ é resolvido diretamente, com todo número ímpar sendo um resíduo quadrático módulo 2. Então, por toda esta aula, p denotará um primo ímpar.

EXEMPLO 3:

Encontre todos os resíduos quadráticos módulo 7.

Solução:

Um sistema completo de resíduos módulo 7 é {0, 1, 2, 3, 4, 5, 6} e podemos analisar os valores dos restos da divisão de x^2 por 7 em cada caso. Mais simplesmente, podemos considerar o sistema completo $\{0, \pm 1, \pm 2, \pm 3\}$.

- $\rightarrow$ se $x \equiv \pm 1(\text{mod}\, 7)$, então $x^2 \equiv 1(\text{mod}\, 7)$, ou seja, 1 é um resíduo quadrático módulo 7
- $\rightarrow$ se $x \equiv \pm 2(\text{mod}\, 7)$, então $x^2 \equiv 4(\text{mod}\, 7)$, ou seja, 4 é um resíduo quadrático módulo 7
- $\rightarrow$ se $x \equiv \pm 3(\text{mod}\, 7)$, então $x^2 \equiv 2(\text{mod}\, 7)$, ou seja, 2 é um resíduo quadrático módulo 7

Logo, os resíduos quadráticos módulo 7 (menores que 7) são 1, 2 e 4, e os resíduos não quadráticos são 3, 5 e 6.

Para finalizar o tópico, vamos a duas proposições que levam à determinação da quantidade de resíduos quadráticos de um determinado número primo, motivado pelo que se pode observar nos exemplos dados e no fato de que $\{0, \pm 1, \pm 2, \pm \frac{p-1}{2}\}$ é um sistema completo de resíduos módulo p, quando p é ímpar.

Lema: Se p é primo ímpar e a é um inteiro positivo tal que a é um resíduo quadrático módulo p, então a equação $x^2 \equiv a(\text{mod}\, p)$ possui exatamente duas soluções incongruentes módulo p.

Demonstração: Primeiramente, veja que se x é solução para a equação dada, então $p-x$ também é solução, pois $(p-x)^2 = p^2 - 2px + x^2$ e como $p^2 - 2px$ é um múltiplo de p, temos $(p-x)^2 \equiv x^2(\text{mod}\, a)$. Além disso, x e $p-x$ são incongruentes módulo p, porque, se valesse $x \equiv p-x(\text{mod}\, p)$, teríamos $2x \equiv p(\text{mod}\, p)$, ou seja, $p \mid 2x$, o que levaria a $p \mid x$ e, consequentemente, $x^2 \equiv 0(\text{mod}\, p)$, o que não acontece. Com isso, obtemos que a equação possui pelo menos duas soluções incongruentes módulo p. Devemos mostrar também que qualquer outra solução para o problema é congruente a x ou a $p-x$. Seja então y tal que $y^2 \equiv a(\text{mod}\, p)$, isto é, $y^2 \equiv x^2(\text{mod}\, p)$. Daqui concluímos que $y^2 - x^2 \equiv 0(\text{mod}\, p)$, isto é, $(x+y)(x-y) \equiv 0(\text{mod}\, p)$. Como p é primo, temos que $y+x \equiv 0(\text{mod}\, p)$ ou $y-x \equiv 0(\text{mod}\, p)$, o que é equivalente a $y \equiv -x(\text{mod}\, p)$ ou $y \equiv x(\text{mod}\, p)$, mas como $-x \equiv p-x(\text{mod}\, p)$, obtemos que ou $y \equiv p-x(\text{mod}\, p)$ ou $y \equiv x(\text{mod}\, p)$, e terminamos a demonstração.

EXEMPLO 4A:

Uma vez que $5^2 \equiv 3(\text{mod}\, 11)$, temos que 3 é um resíduo quadrático módulo 11 e as únicas soluções (a menos de congruência módulo 11) para a equação $x^2 \equiv 3(\text{mod}\, 11)$ são 5 e 6 (pois 6 = 11 – 5)

Demonstração: Como $\{0,1,\ldots,p-1\}$ é um sistema completo de resíduos módulo p, os resíduos quadráticos módulo p são gerados se obtivermos os restos de x^2 por p, para $x = 1,2,\ldots,p-1$. Observe, porém, como visto no lema, que x^2 e $(p-x)^2$ deixam o mesmo resto na divisão por p, logo todos os resíduos quadráticos módulo de p são os restos na divisão de $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$. Assim há, no máximo, $\frac{p-1}{2}$ resíduos quadráticos módulo p incongruentes módulo p. Resta ser mostrado que os números $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ são incongruentes módulo p. Se $m,n \in \{1,2,\ldots,\frac{p-1}{2}\}$ são tais que $m^2 \equiv n^2(\text{mod}\, p)$, então $m^2 - n^2 \equiv 0(\text{mod}\, p)$, assim temos $(m-n)(m+n) \equiv 0(\text{mod}\, p)$, de onde concluímos $m+n \equiv 0(\text{mod}\, p)$ ou $m-n \equiv 0(\text{mod}\, p)$. Uma vez que $0 < m \leq \frac{p-1}{2}$ e $0 < n \leq \frac{p-1}{2}$, vale $0 < m+n \leq \frac{2p-2}{2} = p-1$, isto é, não há como $m+n$ ser um múltiplo de p.

Logo obtemos $m-n\equiv 0(\mathrm{mod}\, p)$ e assim $m\equiv n(\mathrm{mod}\, p)$. Porém, como m e n fazem parte de um sistema completo de resíduos módulo p, concluímos que $m=n$. Assim, $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ são números incongruentes módulo p, de onde obtemos o resultado desejado.

EXEMPLO 4B:

Para p primo ímpar, as únicas soluções para a equação $p^2\equiv 1(\mathrm{mod}\, p)$ são 1 e $p-1$.

EXEMPLO 5A:

A menos de congruência módulo 11, há exatamente 5 resíduos quadráticos módulo 11.

EXEMPLO 5B:

A menos de congruência módulo 47, há exatamente 23 resíduos quadráticos módulo 47.

No tópico seguinte, continuaremos analisando as equações do tipo $x^2\equiv a(\mathrm{mod}\, p)$, para p primo e veremos como determinar se um número é resíduo quadrático módulo p.

TÓPICO 2

O Símbolo de legendre

Objetivos

- Apresentar o símbolo de Legendre
- Relacionar o símbolo de Legendre com resíduos simples

O matemático francês Adrien-Marie Legendre (1752 - 1833) contribuiu com estudos significativos na Estatística, na Álgebra Abstrata, na solução de Equações Diferenciais e na Teoria dos Números. A seguir, definiremos o símbolo de Legendre, uma maneira simplificada de dizer se um número é resíduo quadrático módulo p.

http://en.wikipedia.org/wiki/File:Legendre.jpg

Figura 1: Adrien-Marie Legendre

Definição 1: Dado o primo ímpar p e o inteiro positivo a, não múltiplo de p. O símbolo de Legendre de a por p, denotado por $\left(\frac{a}{p}\right)$ é igual a 1, se a equação $x^2 \equiv a(\text{mod}\, p)$ possui solução, e vale -1, caso contrário. Ou seja:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, \text{ se } a \text{ é um resíduo quadrático módulo } p \\ -1, \text{ se } a \text{ não é um resíduo quadrático módulo } p \end{cases}.$$

EXEMPLO 1A:

Como visto no tópico anterior, 1 e 4 são resíduos quadráticos módulo 5, então $\left(\frac{1}{5}\right)=1$ e $\left(\frac{4}{5}\right)=1$. Uma vez que 2 e 3 não são resíduos quadráticos módulo 5, tem-se $\left(\frac{2}{5}\right)=-1$ e $\left(\frac{3}{5}\right)=-1$.

EXEMPLO 1B:

Vale dizer que $\left(\frac{1}{7}\right)=\left(\frac{2}{7}\right)=\left(\frac{4}{7}\right)=1$ e $\left(\frac{3}{7}\right)=\left(\frac{5}{7}\right)=\left(\frac{6}{7}\right)=-1$

ATENÇÃO!

Apesar da semelhança, não devemos confundir o símbolo de Legendre com uma fração simplesmente nem com o número binomial.

EXEMPLO 1C:

Para qualquer primo ímpar p, vale $\left(\frac{1}{p}\right)=1$.

A seguir, veremos algumas propriedades do símbolo de Legendre.

GUARDE BEM ISSO!

O símbolo de Legendre $\left(\frac{a}{p}\right)$ não é definido se $p \mid a$, entretanto alguns autores estendem a definição acima para $\left(\frac{a}{p}\right)=0$ se $p \mid a$. Assim, por exemplo, podemos considerar $\left(\frac{30}{5}\right)=0$.

Proposição 1: Para qualquer primo ímpar p, vale $\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)=0$.

Demonstração: Pelo que vimos no tópico anterior, metade dos números do conjunto $\{1,2,\ldots,p-1\}$ são resíduos quadráticos módulo p, de modo que na soma $\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)$ há $\frac{p-1}{2}$ parcelas iguais a 1. Também sabemos que os demais números, em igual quantidade, não são resíduos quadrático módulo p, por isso há também $\frac{p-1}{2}$ parcelas iguais a –1. Somando todas as parcelas, obteremos soma zero, como desejado.

Adiante, provaremos um resultado também conhecido como critério de Euler, que determina se um número é resíduo quadrático apenas pela determinação do resto de uma divisão.

Proposição 2: Se p é um primo ímpar e a é um inteiro positivo não divisível por p, então $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

Demonstração: Se $\left(\frac{a}{p}\right) = 1$, então existe um número inteiro x tal que $x^2 \equiv a \pmod{p}$ e como $a \neq 0$, é claro que x não é múltiplo de p, de onde obtemos que $(x, p) = 1$. Usando o pequeno teorema de Fermat, sabemos que $x^{p-1} \equiv 1 \pmod{p}$. Nestes termos, fazemos:

$$a^{\frac{p-1}{2}} \equiv \left(x^2\right)^{\frac{p-1}{2}} \pmod{p}, \text{ que equivale a } a^{\frac{p-1}{2}} \equiv x^{p-1} \pmod{p}.$$

Juntando os fatos, concluímos que $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, ou seja, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$ e o primeiro caso fica provado. O segundo caso é análogo e vem do fato de que a quantidade de resíduos quadráticos módulo p é $\frac{p-1}{2}$.

EXEMPLO 2A:

Vale $\left(\frac{2}{11}\right) \equiv 2^{\frac{11-1}{2}} \pmod{11}$, ou seja, $\left(\frac{2}{11}\right) \equiv 2^5 \pmod{11}$. Como $2^5 = 32$, vale $2^5 \equiv -1 \pmod{11}$. Assim, $\left(\frac{2}{11}\right) = -1$ e, logo, 2 não é um resíduo quadrático módulo 11.

EXEMPLO 2B:

Temos $\left(\frac{3}{13}\right) \equiv 3^6 \pmod{13}$ e, como $3^6 \equiv 1 \pmod{13}$, vale que 3 é um resíduo quadrático módulo 13.

Neste tópico, definimos o símbolo de Legendre, que é uma maneira simplificada de afirmar quando um número é resíduo quadrático módulo p e apresentamos o critério de Euler, que transfere o problema de decidir se um número é resíduo quadrático para a determinação do resto da divisão entre dois inteiros. No tópico a seguir, veremos outras propriedades do símbolo de Legendre.

TÓPICO 3

Lei da reciprocidade quadrática

OBJETIVO

- Continuar o estudo dos resíduos quadráticos, analisando métodos de simplificação do cálculo do símbolo de Legendre

Continuamos o estudo do símbolo de Legendre $\left(\frac{a}{p}\right)$, analisaremos a existência de soluções para equações do tipo $x^2 \equiv a \pmod{p}$. Para começar, veremos que o símbolo de Legendre, visto como função de a, ou seja, com denominador fixo, é completamente multiplicativa.

Proposição 3: Se a e b são inteiros positivos não divisíveis pelo primo p, então $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right).\left(\frac{b}{p}\right)$.

Demonstração: Inicialmente, vemos que $(ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}}.b^{\frac{p-1}{2}}$. Pelo critério de Euler (final do tópico 2), temos $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$ e $\left(\frac{b}{p}\right) \equiv b^{\frac{p-1}{2}} \pmod{p}$. Assim, $\left(\frac{a}{p}\right).\left(\frac{b}{p}\right) \equiv a^{\frac{p-1}{2}}.b^{\frac{p-1}{2}} \pmod{p}$, isto é, $\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right).\left(\frac{b}{p}\right) \pmod{p}$. Uma vez que o símbolo de Legendre assume apenas os valores 1 e -1, a congruência acima implica a igualdade desejada.

EXEMPLO 1A:

Usando o critério de Euler, podemos concluir que $\left(\frac{3}{11}\right) \equiv 3^{\frac{11-1}{2}} \pmod{11}$, ou seja, $\left(\frac{3}{11}\right) \equiv 3^5 \pmod{11}$. Mas, como $3^5 = 243$ deixa resto 1 na divisão por 11, temos que $\left(\frac{3}{11}\right) = 1$. Pelo visto no exemplo 2a do tópico 2, vale $\left(\frac{2}{11}\right) = -1$.

Usando a multiplicabilidade do símbolo de Legendre, concluímos que $\left(\frac{6}{11}\right)=\left(\frac{2}{11}\right).\left(\frac{3}{11}\right)\equiv(-1).1=-1$, logo 6 não é um resíduo quadrático módulo 11.

EXEMPLO 1B:

Para qualquer inteiro positivo a não divisível por p, vale $\left(\frac{a^n}{p}\right)=\left(\frac{a}{p}\right)^n$. Dessa forma, como os possíveis valores de $\left(\frac{a}{p}\right)$ são 1 e –1, vale $\left(\frac{a^n}{p}\right)=1$ para qualquer n par.

EXEMPLO 1C:

Vale que $2^5=32\equiv 1(\text{mod}\,31)$. Assim $\left(\frac{2^5}{31}\right)=\left(\frac{1}{31}\right)=1$, ou seja, 32 é um resíduo quadrático módulo 31. Além disso, $\left(\frac{2}{31}\right)^5=\left(\frac{32}{31}\right)=1$, de onde podemos concluir que $\left(\frac{2}{31}\right)=1$, isto é, 2 é um resíduo quadrático módulo 31.

Como consequência da multiplicabilidade do símbolo de Legendre, reduzimos o trabalho de procurar resíduos quadráticos a números primos. Para começar, um critério segundo os quais saberemos se 2 é resíduo quadrático.

Proposição 4: Se p é um primo ímpar, então $\left(\frac{2}{p}\right)=\begin{cases}1, \text{ se } p\equiv\pm 1(\text{mod}\,8)\\ -1, \text{ se } p\equiv\pm 3(\text{mod}\,8)\end{cases}$.

EXEMPLO 2A:

Como $17\equiv 1(\text{mod}\,8)$, então $\left(\frac{2}{17}\right)=1$, ou seja, 2 é um resíduo quadrático módulo 17. Exemplo 2b:

Como $43\equiv 3(\text{mod}\,8)$, então $\left(\frac{2}{43}\right)=-1$, ou seja, 2 não é um resíduo quadrático módulo 43.

A seguir, enunciaremos um resultado que simplifica o cálculo do símbolo de Legendre, conhecido como a Lei da Reciprocidade Quadrática.

Teorema: Se p e q são primos ímpares distintos, então $\left(\frac{p}{q}\right).\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}.\frac{q-1}{2}}$.

EXEMPLO 3A:

Calcule $\left(\frac{41}{43}\right)$.

Solução:

Pela lei da reciprocidade quadrática, temos $\left(\frac{41}{43}\right).\left(\frac{43}{41}\right)=(-1)^{\frac{43-1}{2}.\frac{41-1}{2}}=(-1)^{21.20}=1$. A partir daí, percebemos que $\left(\frac{41}{43}\right)$ e $\left(\frac{43}{41}\right)$ têm o mesmo sinal. Mas, se $43\equiv 2(\mathrm{mod}\,41)$, logo $\left(\frac{43}{41}\right)=\left(\frac{2}{41}\right)$. Por fim, já que $41\equiv 1(\mathrm{mod}\,8)$, vale $\left(\frac{2}{41}\right)=1$. Assim, $\left(\frac{41}{43}\right)=\left(\frac{43}{41}\right)=\left(\frac{2}{43}\right)=1$, de onde obtemos que 41 é um resíduo quadrático módulo 43.

EXEMPLO 3B:

Calcule $\left(\frac{48}{97}\right)$.

Solução:

Como 48 não é primo, começamos pela fatoração $48=2^4.3$. Usando a multiplicabilidade do símbolo de Legendre, $\left(\frac{48}{97}\right)=\left(\frac{2^4}{97}\right).\left(\frac{3}{97}\right)=\left(\frac{2}{97}\right)^4.\left(\frac{3}{97}\right)$. Como o símbolo de Legendre assume apenas os valores 1 e –1, necessariamente teremos $\left(\frac{2}{97}\right)^4=1$ e o teste do resto na divisão por 8 é desnecessário. Passemos, então, à determinação de $\left(\frac{3}{97}\right)$. Para tanto, usemos a lei da reciprocidade quadrática $\left(\frac{3}{97}\right).\left(\frac{97}{3}\right)=(-1)^{\frac{3-1}{2}.\frac{97-1}{2}}=(-1)^{1.48}=1$. Assim, $\left(\frac{3}{97}\right)$ e $\left(\frac{97}{3}\right)$ têm o mesmo sinal. Uma vez que $97\equiv 1(\mathrm{mod}\,3)$, temos que 97 é um resíduo quadrático módulo 3, logo $\left(\frac{97}{3}\right)=1$. Concluindo: a partir daí, obtemos que $\left(\frac{41}{43}\right)$ e $\left(\frac{43}{41}\right)$ têm o mesmo sinal. Mas $43\equiv 2(\mathrm{mod}\,41)$, logo $\left(\frac{48}{97}\right)$ = 1.

EXEMPLO 4:

Mostre que não existe inteiro n tal que $7\,|\,4n^2-3$.

Solução:

Observe que $7\,|\,4n^2-3$ equivale a $4n^2\equiv 3(\mathrm{mod}\,7)$, ou seja, $(2n)^2\equiv 3(\mathrm{mod}\,7)$ e, se fizermos $x=2n$, teremos $x^2\equiv 3(\mathrm{mod}\,7)$. Podemos aqui usar o que foi feito no tópico 1, no qual obtemos que 3 não é um resíduo quadrático módulo 7, para afirmar que a equação não possui solução. Alternativamente, usando a lei da reciprocidade quadrática, podemos ver que $\left(\frac{3}{7}\right).\left(\frac{7}{3}\right)=(-1)^{\frac{3-1}{2}.\frac{7-1}{2}}=(-1)^{1.3}=-1$,

isto é, $\left(\frac{3}{7}\right)$ e $\left(\frac{7}{3}\right)$ têm sinais contrários. Mas, como $7 \equiv 1 (\mathrm{mod}\, 3)$, temos $\left(\frac{7}{3}\right) = 1$, de onde obtemos que $\left(\frac{3}{7}\right) = -1$ e, da mesma forma, concluímos que 3 não é um resíduo quadrático módulo 7.

Com estes dois testes simples, encerramos nossa aula sobre resíduos quadráticos. Vimos como a investigação sobre existência de soluções para equações do tipo $x^2 \equiv a (\mathrm{mod}\, p)$ pode ser bem simplificada.

AULA 8 | Problemas diversos

Caro(a) aluno(a),

Chegamos à nossa última aula de Teoria dos Números. Aqui revisitaremos os principais resultados apresentados no decorrer do curso, através de problema resolvidos de diversos níveis de dificuldade. Não hesite em procurar nas aulas passadas as definições pertinentes a cada situação. Fique atento também às hipóteses de cada enunciado e aos momentos nos quais elas são usadas.

Objetivo

- Apresentar problemas resolvidos sobre a teoria desenvolvida nas aulas anteriores e discutir a aplicação das técnicas apresentadas em suas soluções

TÓPICO 1 | Miscelânea de exercícios

PROBLEMA 1:

Mostre que a soma de dois números inteiros é ímpar se, e somente se, um deles for par e outro for ímpar.

Solução:

Inicialmente, verifique que, se a for par e b for ímpar, podemos escrever $a = 2m$ e $b = 2n+1$ para certos inteiros m e n. Daí teremos $a+b = 2m+2n+1 = 2(m+n)+1$, que é um número ímpar, isto é, a soma de um número par com um número ímpar resulta em um número ímpar. Se considerarmos a e b ambos pares, podemos escrever $a = 2m$ e $b = 2n$ para certos inteiros m e n. Assim encontraremos $a+b = 2m+2n = 2(m+n)$, que é um número par. Se a e b forem ambos ímpares, podemos escrever $a = 2m+1$ e $b = 2n+1$ para certos inteiros m e n. Daí teremos $a+b = 2m+1+2n+1 = 2m+2n+2 = 2(m+n+1)$, que é um número par. Dessa forma, a soma de dois números pares é sempre par e a soma de dois números ímpares também é par. O mesmo resultado vale para a diferença de dois números.

PROBLEMA 2:

Mostre que se a e b são números ímpares, então a^2+b^2 não pode ser um quadrado perfeito.

Solução:

Comecemos observando que, se a e b são ímpares, o mesmo ocorre com a^2 e b^2, logo a^2+b^2 é um número par. Para que um número par seja um quadrado

perfeito, é necessário que ele seja um múltiplo de 4, pois $2 \mid n^2 \Rightarrow 2 \mid n \Rightarrow 4 \mid n^2$. Mas, como a é ímpar, vale $a \equiv 1 (\mathrm{mod}\, 4)$ ou $a \equiv 3 (\mathrm{mod}\, 4)$ e, em ambos os casos, tem-se $a^2 \equiv 1 (\mathrm{mod}\, 4)$, o mesmo ocorrendo para b, isto é, vale $b^2 \equiv 1 (\mathrm{mod}\, 4)$. Somando as duas congruências, obtemos $a^2 + b^2 \equiv 2 (\mathrm{mod}\, 4)$, de onde concluímos que $a^2 + b^2$ não é um múltiplo de 4 e, assim, não pode ser um quadrado perfeito (como consequência deste resultado, um triângulo retângulo com lados de medidas inteiras tem pelo menos um dos catetos de medida par).

PROBLEMA 3:

Prove que $M = 3^{2n+1} + 2^{n+2}$ é um múltiplo de 7 para qualquer inteiro positivo n.

Solução:

Observe inicialmente que $3^2 \equiv 2 (\mathrm{mod}\, 7)$, logo $\left(3^2\right)^n \equiv 2^n (\mathrm{mod}\, 7)$ e, assim, $3^{2n+1} \equiv 2^n.3 (\mathrm{mod}\, 7)$. Da segunda parcela da soma que define M, podemos afirmar $2^{n+2} = 2^n.2^2 = 2^n.4$ que gera a congruência imediata $2^{n+2} \equiv 2^n.4 (\mathrm{mod}\, 7)$. Somando então as duas últimas congruências, obtemos $3^{2n+1} + 2^{n+2} \equiv 2^n.3 + 2^n.4 (\mathrm{mod}\, 7)$, mas $2^n.3 + 2^n.4 = 2^n.(3+4) = 2^n.7$, que é, claramente, um múltiplo de 7.

PROBLEMA 4:

Mostre que a representação decimal de um número quadrado perfeito não pode ter algarismo das unidades terminando em 2, 3, 7 ou 8.

Solução:

O algarismo das unidades na representação decimal é o resto da divisão do número por 10. Considere, então, os possíveis restos e observe o que acontece com o quadrado:

$$n \equiv 0 (\mathrm{mod}\, 10) \Rightarrow n^2 \equiv 0 (\mathrm{mod}\, 10)$$
$$n \equiv 1 (\mathrm{mod}\, 10) \Rightarrow n^2 \equiv 1 (\mathrm{mod}\, 10)$$
$$n \equiv 2 (\mathrm{mod}\, 10) \Rightarrow n^2 \equiv 4 (\mathrm{mod}\, 10)$$
$$n \equiv 3 (\mathrm{mod}\, 10) \Rightarrow n^2 \equiv 9 (\mathrm{mod}\, 10)$$
$$n \equiv 4 (\mathrm{mod}\, 10) \Rightarrow n^2 \equiv 6 (\mathrm{mod}\, 10)$$
$$n \equiv 5 (\mathrm{mod}\, 10) \Rightarrow n^2 \equiv 5 (\mathrm{mod}\, 10)$$
$$n \equiv 6 (\mathrm{mod}\, 10) \Rightarrow n^2 \equiv 6 (\mathrm{mod}\, 10)$$
$$n \equiv 7 (\mathrm{mod}\, 10) \Rightarrow n^2 \equiv 9 (\mathrm{mod}\, 10)$$
$$n \equiv 8 (\mathrm{mod}\, 10) \Rightarrow n^2 \equiv 4 (\mathrm{mod}\, 10)$$
$$n \equiv 9 (\mathrm{mod}\, 10) \Rightarrow n^2 \equiv 1 (\mathrm{mod}\, 10)$$

Assim, os possíveis algarismos das unidades de um quadrado perfeito são apenas 0, 1, 4, 5, 6 e 9. De modo que, se um número terminar em algarismo diferente destes, quando escrito na base 10, ele certamente não será um quadrado perfeito. Como consequência deste critério, podemos, sem nenhum cálculo, auxiliar, dizer que os números $\sqrt{10253443}$, $\sqrt{3278812}$ e $\sqrt{20003417}$ são irracionais, pois os radicandos não são quadrados perfeitos.

PROBLEMA 5:

Prove que o produto de três números inteiros consecutivos é sempre divisível por 6.

Solução:

Em uma sequência de três inteiros consecutivos, há necessariamente um múltiplo de 3, de modo que o produto de três inteiros consecutivos é um múltiplo de 3. De maneira análoga, certamente um dos fatores será um número par e, assim, múltiplo de 2. Assim, o número obtido é divisível por 2 e por 3 ao mesmo tempo, sendo portanto, múltiplo de 6.

PROBLEMA 6:

Usando o algoritmo de Euclides, determine o máximo divisor comum entre 432 e 28, em seguida determine o mínimo múltiplo comum entre 432 e 28.

Solução:

Começando pela divisão de 432 por 28, obtemos

$$432 = 28.15 + 12$$

Assim, o problema é transferido para a determinação do máximo divisor comum entre 28 e 12. Dividindo 28 por 12, obtemos

$$28 = 12.2 + 4$$

Desse modo, temos que o máximo divisor comum entre 28 e 12 é o mesmo que entre 12 e 4, mas, como 4 é um divisor de 12, temos (28,12)=4. Logo, o máximo divisor comum entre 432 e 28 é 4. Usando a identidade $[a,b].(a,b) = a.b$, ganhamos que $[432,28] = \frac{432.28}{(432,28)} = \frac{432.28}{4} = 432.7 = 3024$, ou seja, o mínimo múltiplo comum entre 432 e 28 é 3024.

PROBLEMA 7:

Mostre que a equação $42x + 180y = 14$ não possui soluções inteiras.

Solução:

Do estudo de equações diofantinas, sabemos que $ax+by=c$ possui solução $(x,y)\in\mathbb{Z}\times\mathbb{Z}$ se, e somente se, $(a,b)\,|\,c$. Para a equação dada, basta ver que $(42,180)=6$, mas 6 não divide 14.

PROBLEMA 8:

Determine o resto na divisão de 22.33.44.55 por 7.

Solução:

Como $22\equiv 1(\mathrm{mod}\,7)$, $33\equiv 5(\mathrm{mod}\,7)$, $44\equiv 2(\mathrm{mod}\,7)$ e $55\equiv 6(\mathrm{mod}\,7)$, temos, pela multiplicação das congruências, que $22.33.44.55\equiv 1.5.2.6(\mathrm{mod}\,7)$. Como 1.5.2.6=50 deixa resto 4 na divisão por 7, temos que 22.33.44.55 deixa resto 4 na divisão por 7.

PROBLEMA 9:

Determine o número inteiro positivo n que satisfaz $12\,|\,n$ e $\tau(n)=14$.

Solução:

Seja $n=p_1^{\alpha_1}.p_2^{\alpha_2}.....p_k^{\alpha_k}$ a fatoração em primos de n, temos que $\tau(n)=(\alpha_1+1)(\alpha_2+1)...(\alpha_k+1)$. Assim, devemos procurar as formas segundo as quais 14 pode ser escrito como produto de números inteiros positivos. São elas $14=14.1$, e neste caso, teremos $n=p^{13}$, para algum primo p, ou $14=7.2$, caso no qual vale $n=p^6q$ para primos p e q. Como $12\,|\,n$ e $12=2^2.3$, necessariamente os primos 2 e 3 devem aparecer na fatoração de n, de modo que a primeira opção não ocorre. Então temos $n=2^6.3$ ou $n=3^6.2$. Mas a segunda opção não ocorre, pois o expoente do 2 deve ser no mínimo 2 para que se tenha $12\,|\,n$. Assim, a única possibilidade é $n=2^6.3=192$.

PROBLEMA 10:

Encontre todos os restos possíveis na divisão de um quadrado perfeito por 8.

Solução:

Uma vez que os possíveis restos na divisão por 8 são apenas 0, 1, 2, ..., 7, avaliaremos apenas os possíveis restos na divisão de n^2 por 8 nos seguintes casos:

se $n\equiv 0(\mathrm{mod}\,8)$, temos $n^2\equiv 0(\mathrm{mod}\,8)$ e o resto é, portanto, 0

se $n\equiv \pm 1(\mathrm{mod}\,8)$, temos $n^2\equiv 1(\mathrm{mod}\,8)$ e o resto é, portanto, 1

se $n\equiv \pm 2(\mathrm{mod}\,8)$, temos $n^2\equiv 4(\mathrm{mod}\,8)$ e o resto é, portanto, 4

se $n\equiv \pm 3(\mathrm{mod}\,8)$, temos $n^2\equiv 9(\mathrm{mod}\,8)$ e o resto é, portanto, 1

se $n\equiv 4(\mathrm{mod}\,8)$, temos $n^2\equiv 16(\mathrm{mod}\,8)$ e o resto é, portanto, 0

Esgotadas todas as possibilidades, concluímos que um quadrado perfeito deixa resto 0, 1 ou 4 na divisão por 8.

PROBLEMA 11:

Mostre que, se $k \equiv 7(\mathrm{mod}\,8)$, então k não pode ser escrito como soma de três quadrados perfeitos.

Solução:

Pelo problema anterior, um quadrado perfeito deixa resto 0, 1 ou 4 na divisão por 8, logo a soma de três quadrados será congruente à soma de três números do conjunto $\{0,1,4\}$. Porém 7 não pode ser escrito como soma de três dos números dados, por isso é impossível que um número que deixa resto 7 na divisão por 8 possa ser escrito como soma de três quadrados perfeitos.

PROBLEMA 12:

Determine o resto da divisão de $19^6 + 44^{24}$ por 7.

Solução:

Como 19 não é divisível por 7, temos, pelo Teorema de Fermat, que $19^{7-1} \equiv 1(\mathrm{mod}\,7)$, ou seja, $19^6 \equiv 1(\mathrm{mod}\,7)$. Usando argumento semelhante, concluímos que $44^6 \equiv 1(\mathrm{mod}\,7)$, de onde obtemos $\left(44^6\right)^4 \equiv 1^4(\mathrm{mod}\,7)$, isto é, $44^{24} \equiv 1(\mathrm{mod}\,7)$. Por fim, temos $19^6 + 44^{24} \equiv 1 + 1(\mathrm{mod}\,7)$ e o resto procurado é, portanto, 2.

PROBLEMA 13:

Encontre a quantidade de números inteiros positivos menores que 3600 que são múltiplos de 2, 3 ou 5.

Solução:

Observe que a fatoração de 3600 em primos é $3600 = 2^4.3^2.5^2$. Assim os fatores primos de 3600 são exatamente 2, 3 e 5, de modo que os múltiplos de 2, 3 ou 5 são aqueles que não são relativamente primos com 3600. Podemos encontrar a quantidade dos que são relativamente primos com 3600 pela função de Euler $\phi(3600) = 3600.\left(1-\frac{1}{2}\right).\left(1-\frac{1}{3}\right).\left(1-\frac{1}{5}\right) = 3600.\frac{1}{2}.\frac{2}{3}.\frac{4}{5} = 960$. Assim, se retirarmos esses 960 números dos 3599 inteiros positivos menores que 3600, obteremos os 2639 que são múltiplos de 2, 3 ou 5.

PROBLEMA 14:

Encontre o menor inteiro positivo n para o qual $\tau(n) = 13$.

Solução:

Seja $n = p_1^{\alpha_1}.p_2^{\alpha_2}.....p_k^{\alpha_k}$ a fatoração em primos de n, temos que $\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1)...(\alpha_k + 1) = 13$, porém, como 13 é um número primo, não poderá ser escrito como produto de dois números menores que ele. Logo os números que possuem exatamente 13 divisores positivos são da forma $n = p^{12}$, com p primo. De modo a minimizar o valor de n, consideramos o menor primo e obtemos $n = 2^{12} = 4096$.

PROBLEMA 15:

Prove que se n não é um quadrado perfeito, então $\tau(n)$ é par.

Solução:

Se n não é um quadrado perfeito, então pelo menos um dos expoentes de sua fatoração em primos é ímpar, de modo que pelo menos um dos consecutivos destes expoentes é par. Mas, quando um dos fatores é par, o produto é par, logo a quantidade de divisores de n que é calculada pelo produto dos consecutivos dos expoentes de sua fatoração em primo será par.

PROBLEMA 16:

Determine todos os números inteiros positivos menores que 12 que possuem inverso módulo 12.

Solução:

Um número n possui inverso módulo 12 quando existe um inteiro k tal que $nk \equiv 1 (\mathrm{mod}\, 12)$ e isso ocorre se, e somente se, $(n,12) = 1$. Investigando quais dos inteiros positivos menores que 12 lhe são relativamente primos, obtemos a lista 1, 5, 7, 11. Mais ainda, cada um dos números listados é seu próprio inverso módulo 12.

PROBLEMA 17:

Mostre que a equação $n^3 + 5n - 27 = 0$ não possui solução inteira.

Solução:

Veja que a equação é equivalente a $n^3 + 5n = 27$, ou seja, $n(n^2 + 5) = 27$. Observe que $n^2 + 5$ é um número necessariamente positivo e maior que n, de modo que escrevemos 27 como produto de dois números inteiros positivos, mas só há duas maneiras de fazer isso: $27 = 1.27$, caso em que $n = 1$ e $n^2 + 5 = 27$, o que não se verifica; e $27 = 3.9$, caso em que $n = 3$ e $n^2 + 5 = 9$, o que é igualmente falso. Assim concluímos que a equação dada não possui raízes inteiras.

PROBLEMA 18:

Dado o número inteiro $B>3$, mostre que o número $(1331)_B$ é um cubo perfeito.

Solução:

Aqui basta ver que $(1331)_B = B^3+3B^2+3B+1=(B+1)^3$, que é o cubo do inteiro $B+1$.

PROBLEMA 19:

Mostre que existem infinitos números inteiros n para os quais $10 \mid \phi(n)$.

Solução:

Observe que $\phi(11)=10$, logo, se m for relativamente primo com 11, teremos $\phi(11m)=\phi(11)\phi(m)=10\phi(m)$, assim $10 \mid \phi(11m)$, isto é, $10 \mid \phi(n)$ para todo inteiro positivo da forma $n=11m$, com $(11,m)=1$. Mas há infinitos números que podem ocupar o lugar de m, por exemplo todos os outros primos.

PROBLEMA 20:

Mostre que, para qualquer inteiro positivo $n>1$, existem infinitos números inteiros m para os quais $\tau(m)=n$.

Solução:

Observe que $\tau(m)=n$ ocorre para qualquer número da forma $m=p^{n-1}$, onde p é primo. O resultado segue do fato de que há infinitos números primos.

PROBLEMA 21:

Determine o algarismo das unidades de 7^{202}, quando expresso em base decimal.

Solução:

O algarismo das unidades de um número é o resto da divisão pela base. Assim, devemos determinar o resto da divisão de 7^{202} por 10. Sabemos pelo teorema de Euler, que $a^{\phi(n)} \equiv 1 (\mathrm{mod}\, n)$, para quaisquer inteiros positivos a,n relativamente primos. Assim, temos $7^{\phi(10)} \equiv 1 (\mathrm{mod} 10)$. Mas $\phi(10)=4$, daí vale $7^4 \equiv 1 (\mathrm{mod} 10)$. Dividindo 202 por 4, obtemos quociente 50 e resto 2, de onde concluímos $7^{202}=7^{50.4+2}=\left(7^4\right)^{50}.7^2 \equiv 1^{50}.7^2 (\mathrm{mod} 10)$. Por fim, como $7^2=49 \equiv 9 (\mathrm{mod} 10)$, o algarismo procurado é 9.

REFERÊNCIAS

LANDAU, Edmund. **Elementare Zahlentheorie**. Leipzig: S. Hirzyel Verlag, 1927.

SANTOS, José Plínio de Oliveira. **Introdução à Teoria dos Números**. Rio de Janeiro: Instituto de Matemática Pura e Aplicada, 1998.

CURRÍCULO

Jânio Kléo de Castro Sousa

Jânio Kléo começou seus estudos de Matemática em 2000, quando ingressou no bacharelado da Universidade Federal do Ceará, colando grau em julho de 2004. A partir de 2001 e por três anos, foi monitor de Cálculo Diferencial e Integral na UFC, desempenhando atividade de acompanhamento e tira-dúvidas para alunos de graduação.

Durante os anos de 2006, 2007 e 2008, foi professor da UFC, com turmas de diversos cursos, ministrando aulas de Álgebra Linear, Equações Diferenciais, Variáveis Complexas e Geometria Hiperbólica, entre outras.

Desde o começo de 2009 é professor do Instituto Federal de Educação, Ciência e Tecnologia do Ceará, atuando nos campus de Fortaleza e Maracanaú, nos cursos presenciais e semipresenciais.