4.

TEOREMA FUNDAMENTAL DA ARITMÉTICA: APLICAÇÕES

1).– Achando os divisores de um número natural
2).– Quantidade de divisores de um número natural
3).– Decidindo se um número natural divide outro
4).– Extrema indivisibilidade: números relativamente primos
5).– Decidindo se um número natural divide o produto de outros números
6).– Determinando o máximo divisor comum de dois naturais
7).– Exercícios e problemas.

Significado de divisor, divide e divisível

No contexto dos números naturais, essas palavras têm o mesmo significado. Mais precisamente:

Sendo a e b números naturais:
"a é um divisor de b" significa "existe um número natural c tal que $ac = b$;
"a divide b" significa "existe um número natural c tal que $ac = b$;
"b é divisível por a" significa "existe um número natural c tal que $ac = b$;

A notação FAT (a)

Vimos na aula anterior que o Teorema Fundamental da Aritmética garante que todo número natural $a \geqslant 2$ pode ser escrito como um produto de primos[1] e que essa decomposição em primos é única, a menos da ordem com que os fatores primos são escritos. Isso nos permite usar uma notação para denotar tal fatoração: FAT (a).

Exemplo –
Temos $1512 = 2\times2\times2\times2\times3\times3\times7 = \mathrm{FAT}\,(1512) = 2^3\times3^2\times7$. A segunda maneira de escrever a fatoração é um exemplo de *notação exponencial* da decomposição em primos.
Prefere-se escrever toda decomposição em primos em ordem crescente dos primos, como fizemos acima no caso de 1512; isso nos permite facilmente fazer referência aos *expoentes* da decomposição; no caso de 1512, os expoentes são 3, 2 e 1.

Exemplo –
Consideremos as seguintes fatorações de $a = 90$: $a = 2\times3^2\times5 = 2\times5\times3^2 = 2\times45$. As duas primeiras são fatorações em primos e diferem apenas na ordem como os primos foram escritas: são consideradas

[1] não obrigatoriamente distintos, e possivelmente reduzidos a um único fator, se o próprio a já for primo

como iguais. A terceira fatoração não é uma fatoração em primos, de modo que não tem importância que ela difira das duas primeiras em mais do que na ordem dos fatores.

1).– Achando os divisores de um número natural

Como exemplo inicial, seja determinar todos os divisores de a = 200.
Na base da força bruta, podemos fazer isso dividindo 200 por cada um dos números de 1 a 200 e verificando os casos em que o resultado da divisão é um número inteiro; tais casos são os dos divisores de 200. Fazendo isso, obtemos: 1, 2, 4, 5, 8, 10, 20, 25, 40, 50, 100 e 200.

Como chegar a essa conclusão usando um *raciocínio matemático*? Uma maneira simples de se fazer isso consiste em partir de FAT (200) = $2^3 \times 5^2$ e observar que certamente são divisores de 200 todos os inteiros que podem ser escritos como

$$2^{\alpha} \times 5^{\beta}, \quad \text{com } 0 \leqslant \alpha \leqslant 3, 0 \leqslant \beta \leqslant 2.$$

Façamos a lista de todos eles, variando α e β de todas as maneiras permitidas:

$2^0 \times 5^0 = 1$	;	$2^0 \times 5^1 = 5$	;	$2^0 \times 5^2 = 25$
$2^1 \times 5^0 = 2$	;	$2^1 \times 5^1 = 10$	;	$2^1 \times 5^2 = 50$
$2^2 \times 5^0 = 4$	;	$2^2 \times 5^1 = 20$	;	$2^2 \times 5^2 = 100$
$2^3 \times 5^0 = 8$	;	$2^3 \times 5^1 = 40$	;	$2^3 \times 5^2 = 200$

Mas, por que podemos garantir que somente esses inteiros acima são divisores de 200 ? Ou seja, por que basta variar os valores de α e β para obtermos todos os divisores? Para mostrar que não fica faltando nenhum divisor, denotemos por c um divisor qualquer de 200 (de modo que 200=c × q, para algum inteiro q) e mostremos que ele tem de estar na lista acima. Ora, temos

$$2^3 \times 5^2 = \text{FAT}\,(200) = \text{FAT}\,(c \times q) = \text{FAT}\,(c) \times \text{FAT}\,(q),$$

e então c só pode ter 2 e 5 como fatores primos (lembre da unicidade da fatoração em primos!); além disso, o expoente de 2 como *possível* fator primo de c não pode superar 3; e nem o expoente de 5 como *possível* fator primo de c pode superar 2. Conclusão: obrigatoriamente c tem de ter a forma $2^{\alpha} \times 5^{\beta}$, com $0 \leqslant \alpha \leqslant 3, 0 \leqslant \beta \leqslant 2$.

No caso de números grandes, pode ser conveniente sistematizar os cálculos acima de modo ligeiramente diferente. A seguir, mostramos dois modos de se fazer isso.
Exemplo –

$252 = 2^2 \cdot 3^2 \cdot 7$		
1	2	4
3	6	12
9	18	36
7	14	28
21	42	84
63	126	252

$1078 = 2 \cdot 7^2 \cdot 11$	
1	2
7	14
49	98
11	22
77	154
539	1078

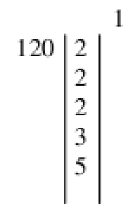
$1750 = 2 \cdot 5^3 \cdot 7$	
1	2
5	10
25	50
125	250
7	14
35	70
175	350
875	1750

$29645 = 5 \cdot 7^2 \cdot 11^2$	
1	5
7	35
49	245
11	55
77	385
539	2695
121	605
847	4235
5929	29645

Exemplo –
Seja achar todos os divisores do número 120.
(Après texto do Prof. Gerson Henrique.)

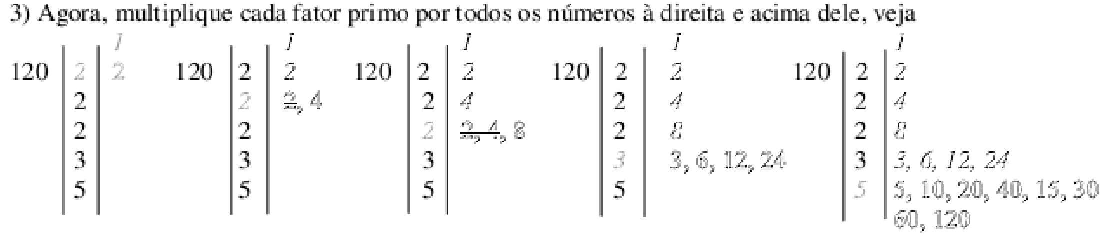
1) Fatore em primos o número em questão

2)Acrescente o número 1 à direita e acima da coluna de primos



Sempre adicionaremos o 1, já que ele é divisor de todo e qualquer número.

3) Agora, multiplique cada fator primo por todos os números à direita e acima dele, veja



Repare que os divisores 2 e 4 repetiram, então foram cortados com um traço. Dessa maneira, os divisores de 120 são {1, 2, 3, 4, 5, 6, 8, 10, 12,15, 20, 24, 30, 40, 60, 120}

2).– Quantidade de divisores de um número natural

Conhecendo essa quantidade, podemos verificar se, ao aplicar qualquer um dos procedimentos acima, não esquecemos algum divisor.
Dado um número natural a de fatoração em primos conhecida, $a = \mathrm{FAT}(a) = p_1^{\alpha} \times p_2^{\beta} \times p_3^{\gamma} \times \ldots$, sua quantidade de divisores será indicada por $\mathrm{T}(a)$ e, pelo que vimos acima, é dada por

$$a = \mathrm{FAT}(a) = p_1^{\alpha} \times p_2^{\beta} \times p_3^{\gamma} \times \ldots \quad \longrightarrow \quad T(a) = (\alpha+1)(\beta+1)(\gamma+1)\ldots$$

Exemplo –
Verifiquemos o caso de 120. Do exemplo anterior, temos $120 = \mathrm{FAT}(120) = 2^3 \times 3 \times 5$, de modo que T(120) = (3+1)(1+1)(1+1) = 4 x 2 x 2 = 16, o que confere com o que achamos acima.

A associação $a \rightsquigarrow T(a)$ é um exemplo de *função aritmética*. Boa parte da Teoria dos Números trata do estudo e aplicação dessa e outras funções aritméticas.

3).– Decidindo se um número natural divide outro

O raciocínio feito no item anterior demonstra o seguinte resultado:

Teorema –
Sendo $a, b \geqslant 2$ dois números naturais, teremos que a divide b quando, e somente quando, o expoente de cada fator primo em $\mathrm{FAT}(a)$ não superar o expoente deste primo em $\mathrm{FAT}(b)$.

Uma maneira prática de implementar esse resultado consiste em procurar simplificar os primos em

$$\frac{b}{a} = \frac{\mathrm{FAT}(b)}{\mathrm{FAT}(a)}.$$

O a dividirá b quando, e somente quando, conseguirmos remover todos os primos do denominador!

Exemplifiquemos. Seja verificar se a=28 divide b=360. Temos

$$\frac{b}{a} = \frac{360}{28} = \frac{2^3 \times 3^2 \times 5}{2^2 \times 7} = \frac{2 \times 3^2 \times 5}{7}$$

e como o primo 7 no denominador não pode ser removido, segue que 28 não divide 360.
Será que 45 divide 810? Procedemos semelhantemente:

$$\frac{b}{a} = \frac{810}{45} = \frac{2 \times 3^4 \times 5}{3^3 \times 5} = \frac{2 \times 3 \times 5}{1} = 2 \times 3 \times 5\,,$$

logo, 45 divide 810.

Na prática, podemos raciocinar mais rapidamente. Por exemplo:

- *O número 6 divide 142?*
  Não! Pois $\mathrm{FAT}\,(6) = 2 \times 3$ e certamente 3 não aparece na $\mathrm{FAT}\,(142)$, pois o primo 3 não divide 142. Ou seja: não é verdade que o expoente de 3 em FAT (6) (que vale 1) não supera o expoente de 3 em FAT (142) (o qual vale zero).
- *Obviamente, 219 não é divisível por 15*, pois 15 tem o fator primo 5, mas 219 não.

Sendo a um número ***primo****, dado um número natural qualquer b:*
– se a aparece em $\mathrm{FAT}\,(b)$*, então a divide b;*
– se a não aparece em $\mathrm{FAT}\,(b)$*, então a não divide b.*

– se a divide b, então a aparece em $\mathrm{FAT}\,(b)$*;*
– se a não divide b, então a não pode aparecer em $\mathrm{FAT}\,(b)$.

4).– Extrema indivisibilidade: números relativamente primos

Definição –
Dizemos que dois números naturais, $a, b \geqslant 2$, são ***relativamente primos*** *(também se diz* coprimos, ou primos entre sí*) quando, e só quando, não tiverem nenhum fator primo em comum, ou seja: não existe nenhum primo simultâneamente em FAT(a) e FAT(b).*
Esta definição se estende imediatamente ao caso de mais de dois naturais: não podem ter nenhum fator primo em comum.

É importante não confundir os conceitos de "número primo" e de "relativamente primos". Por exemplo, os números 4 e 9 são relativamente primos, embora nenhum deles seja primo.

Exemplos: como 14 = 2 x 7 e 35 = 5 x 7, segue que 14 e 35 não são relativamente primos (7 é fator comum); por outro lado, 4 = 2 x 2 e 9 = 3 x 3 são relativamente primos.

Dois cuidados –
• Pode ocorrer que a e b sejam *indivisíveis* (ou seja: nem a divide b e nem b divide a), e mesmo assim a e b *não sejam* relativamente primos. Com efeito, o relativamente primo ocorre em casos de extrema indivisibilidade. Por exemplo, 6 e 8 são indivisíveis, mas 6 e 8 não são relativamente primos, pois têm o fator primo 2 em comum.

• Não confunda os conceitos de “número primo” e de “relativamente primos”. Por exemplo, os números 4 e 9 são relativamente primos, embora nenhum deles seja primo.

O conceito de mdc pode ser estendido ao caso de três, ou mais, números; assim, 14, 35 e 20 é uma trinca de relativamente primos, pois em 14 = 2 x 7, 35 = 5 x 7 e 20=2 x 2 x 5 não há nenhum primo comum a todas essas fatorações.

- *dois primos sempre são relativamente primos;*
- *dois não primos podem ser ou não ser relativamente primos;*
- *dois números naturais consecutivos sempre são relativamente primos;*
- *um primo e um não primo (outro que o zero e a unidade) somente deixarão de ser relativamente primos se o primo for divisor do não primo;*
- *sendo $a, b \geqslant 2$, temos que a e b são relativamente primos quando, e só quando, o único divisor comum entre eles for a unidade.*

5).– Decidindo se um número natural divide o produto de outros números

Na resolução de problemas, é muito importante termos condições de decidir se um número natural divide o produto de dois ou mais outros naturais.Disso trata o seguinte resultado.

Lema de Euclides –
Dados três números naturais, $a, b, c \geqslant 2$:

- *se c divide $a \cdot b$ e é relativamente primo com a, então c divide b ;*
- *se c divide ab e é primo, então c divide ao menos um entre a e b .*

Prova. Nos dois casos, c divide ab, de modo que podemos escrever:

$$\text{inteiro} = \frac{ab}{c} = \frac{\text{FAT}\,(a)}{\text{FAT}\,(c)} = \frac{\text{FAT}\,(a) \times \text{FAT}\,(b)}{\text{FAT}\,(c)}\,.$$

• Se c é relativamente primo com a: FAT (a) e FAT (c) não têm fator primo comum, logo para que ab/c seja inteiro os fatores primos de FAT (c) têm de estar em FAT (b); ou seja: c divide b.
• Se c é primo: para que ab/c seja inteiro, agora c terá de estar em ao menos um dentre FAT (a) e FAT (b); ou seja: c divide ao menos um entre a e b.

6).– Determinando o máximo divisor comum (mdc) de dois números naturais

Pode ocorrer que um mesmo número seja divisor de dois ou mais outros. Assim, 9 divide 36, 63 e 108. Dizemos, então, que 9 é um divisor comum de 63, 210 e 420. Em geral, dados dois naturais quaisquer, digamos a e b, eles têm ao menos um divisor em comum: a unidade; assim, podemos falar no maior de seus divisores comuns. Ele é denominado **máximo divisor comum** de a e b, e o denotaremos por mdc (a,b). De modo semelhante podemos falar no mdc de três ou mais números naturais.

Os divisores de 15 são 1, 3, 5, e 15, enquanto que os de 12 são: 1, 2, 3, 4, 6, e 12; logo, os divisores comuns entre esses dois números são 1 e 3, e então o valor do mdc (15,12) = 3.

Em geral, o procedimento usado no exemplo anterior é demorado, principalmente no caso de números grandes. Existem muitos outros procedimentos mais eficientes, os dois mais conhecidos baseiam-se na fatoração em primos, o primeiro, e na divisão euclidiana, o segundo.

– Determinando o mdc por meio da decomposição em fatores primos

Seja determinar o mdc(159 390, 49 005). Iniciamos determinando a FAT de cada um desses dois números e as escrevemos em forma de fração:

$$\frac{159\,390}{49\,005} = \frac{\text{FAT}\,(159\,390)}{\text{FAT}\,(49\,005)} = \frac{2\times 3^2\times 5\times 7\times 11\times 23}{3^4\times 5\times 11^2}.$$

Simplificando tudo o que for possível nessa fração, removemos $3^2 \times 5 \times 11 = 495$, o qual é, então, o mdc (159 390, 49 005).

No caso do mdc de três ou mais números, pode-se usar a seguinte variante da disposição acima. Seja achar o mdc (686, 2 156, 1 666). Achamos as FAT de cada um desses números e as dispomos assim:

$$\begin{aligned} 686 &= 2\times 7^3 \\ 2\,156 &= 2^2\times 7^2\times 11 \\ 49\,005 &= 2\times 7^2\times 17 \end{aligned}$$

de modo que o mdc procurado é $2 \times 7^2 = 98$.

– Determinando o mdc por meio de divisões euclidianas: algoritmo de Euclides

Este antigo algoritmo consiste em fazer uma sequência de divisões e explora que todo divisor comum de “a e b" também é divisor comum de “b e o resto da divisão de a por b". Detalhes: vide notas de aula.

– Propriedades do mdc

- *Todo número que divide dois outros também divide seu mdc.*
- $\text{mdc}\,(ka, kb) = k\,\text{mdc}\,(a, b)$.
- *Os divisores comuns de dois números são os divisores do mdc destes números.*

Exemplos –

mdc (2 079, 735) = 21, mdc (8316, 2940) = mdc (4 x 2 079, 4 x 735) = 4 x 21 = 84.

Seja determinar os divisores comuns de 2 079 e 735. Visto que o mdc desses dois números é 21, basta achar os divisores de 21, os quais são 1, 3, 7 e 21.

EXERCÍCIOS DIDÁTICOS

Exercício –

Resposta rápida para cada item abaixo.

a). Qual é o mdc de dois números, um dos quais divide o outro?
    Resp.:

b). Que precisamos fazer para que o mdc de dois números aumente quatro vezes?
    Resp.:

c). Dois números são primos entre sí e foram multiplicados por 28. Qual o mdc dos produtos?
    Resp.:

d). É primo o número 113? e 161?
    Resp.:

e). Por que dois números naturais consecutivos são relativamente primos?
    Resp.:

f). Por que dois ímpares consecutivos sempre são relativamente primos?
    Resp.:

g). Quando o mdc de três números consecutivos vale um?
    Resp.:

h). Quem pode ser o dígito das unidades de um número divisível por 15?
    Resp.:

j). Um número é divisível por dois números consecutivos. Será ele divisível pelo produto deles?
    Resp.:

Exercício –

O número dado pelo produto $2^3 \times 3^3 \times 5 \times 11$ é divisível por

a). $2 \times 3^2 \times 11$?
    Resp.:

b). $2^2 \times 3^3 \times 5$?
    Resp.:

c). $2 \times 3 \times 5 \times 7$?
    Resp.:

Exercício –

Achar a menor potência de 60 que é divisível por 36^4 .
Resp.:

Exercício –

Achar a quantidade de divisores 210, e a seguir calcular todos estes divisores.
Resp.: $210 = 2 \times 3 \times 5 \times 7$, logo $T\,(210) = (1+1) \times (1+1) \times (1+1) \times (1+1) = 16$ e os tais 16 divisores são: 1, 2, 3, 6, 5, 10, 15, 30, 7, 14, 21, 42, 35, 70, 105 e 210.

Exercício –

Mostrar que, dado um inteiro $a \geqslant 2$, temos só duas alternativas para cada primo p: ou “p divide a”, ou “p e a são relativamente primos”.

PROBLEMAS OLÍMPICOS

Problema 1 –

Usando as propriedades do mdc, mostre que *todo número que divide um produto de dois fatores, e é relativamente primo com um deles, divide o outro* (Lema de Euclides).

Para isso, trabalhe com o caso numérico de 9 que divide 36 x 25 = 900; como 9 e 25 são relativamente primos, o 9 deverá dividir 36. Com efeito, 9 é um divisor comum de 36 x 25 (pela hipótese) e de 36 x 9 (um seu múltiplo), e o mdc desses dois números é mdc (36 x 25, 36 x 9) = 36 mdc (25, 9) = 36, logo (propriedade do mdc: todo divisor de dois números também é divisor do seu mdc) 9 é divisor de 36.

Problema 2 –

Usando o exercício anterior, prove a outra parte do Lema de Euclides: *todo número primo que divide um produto de dois fatores, divide ao menos um destes fatores.*

Sug.: além do exerc. anterior, use que se um primo não divide um número, então ele é relativamente primo com este número.

Problema 3 –

Prove as seguintes consequências do Lema de Euclides:

a). todo primo que divide um produto de primos é igual a um deles

b). todo primo que divide o quadrado de um número também divide este número

c). se dois números forem relativamente primos, também o serão seus quadrados.

Problema 4 –

Prove que o quadrado de todo número natural tem ou a forma 4n ou a forma 4n +1.

Problema 5 –

Prove que na sequência 11, 111, 1111, 11111, etc. não existe nenhum quadrado de inteiro.

Sug.: sendo $n \geqslant 3$, observe que o esquema abaixo mostra que todo número da sequência dada tem a forma 4n -1, e então use o exerc. anterior:

$$\underbrace{11\ldots1}_{n \text{ uns}} = \underbrace{11\ldots11}_{n-2 \text{ uns}}00 + 12 - 1 = 100 \times \underbrace{11\ldots11}_{n-2 \text{ uns}} + 12 - 1$$

Problema 6 –

Prove que na sequência dos números dados por $23 + n^2$ (n=0, 1, 2, 3, etc.) existem infinitos números divisíveis por 24.

Sug.: observe que $n^2 + 23 = n^2 - 1 + 24 = (n+1)(n-1) + 24$, e então considere os n da forma $n = 24m + 1$.

Problema 7 –

Seja p um primo tal que 1+11 p é o quadrado de algum inteiro. Pede-se determinar p.

Sug.: inicie observando que $1 + 11p = a^2$ pode ser escrito como $11p = (a-1)(a+1)$, e então considere as duas possibilidades: “11 divide $a-1$” e “11 divide $a+1$”.