Lógica para Computação

aula 04: Raciocinando sobre números

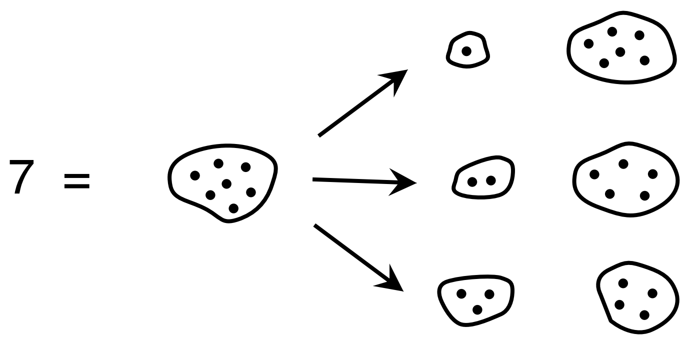
1 Introdução

(. . .)

2 Desmontando números

É bom pensar com números porque um número pode ser desmontado de muitas maneiras diferentes.

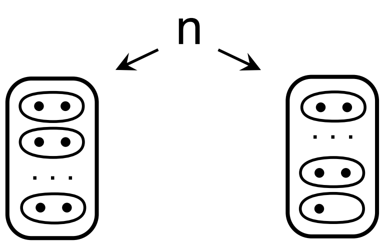
Veja só



(*Você consegue desmontar o número 1?*)

(*E o número 0, você consegue?*)

Quando a gente começa a brincar de desmontar números, a gente descobre que só existem dois tipos de números



Quer dizer, os números que podem ser desmontados em grupinhos de 2, e aqueles que não podem ser desmontados assim.

(*Porque só existem esses dois tipos?*)

E quando a gente descobre isso, a gente pode começar a fazer perguntas.

Vejamos.

Exemplo 1: *O número abaixo, é par ou é ímpar?*

$$n^2 \; + \; n \; + \; 5$$

Bom, depende se n ele próprio é par ou ímpar ...

Se n é par, então ele pode ser decomposto em grupinhos de 2, e escrito como $n = 2k$.

Mas, então, o número acima pode ser escrito como

$$n^2 \; + \; n \; + \; 5 \quad = \quad (2k)^2 \; + \; (2k) \; + \; 5$$

e, fazendo algumas contas simples,

$$\begin{aligned} (2k)^2 \; + \; (2k) \; + \; 5 \quad &= \quad 4k^2 \; + \; 2k \; + \; 4 \; + \; 1 \\ &= \quad \underbrace{2 \cdot \left[k^2 \; + \; k \; + \; 2\right]}_{\text{par}} \; + \; 1 \end{aligned}$$

nós descobrimos que o número é ímpar.

Por outro lado, se n é ímpar, então ele não pode ser decomposto em grupinhos de 2 (pois sempre sobra 1 sozinho), e pode ser escrito como $n = 2k + 1$.

Mas, então, o número acima pode ser escrito como

$$n^2 \; + \; n \; + \; 5 \quad = \quad (2k+1)^2 \; + \; (2k+1) \; + \; 5$$

e, fazendo algumas contas simples,

$$\begin{aligned} (2k+1)^2 \; + \; (2k+1) \; + \; 5 \quad &= \quad 4k^2 \; + \; 4k \; + \; 1 \; + \; 2k \; + \; 1 \; + \; 5 \\ &= \quad \underbrace{2 \cdot \left[2k^2 \; + \; 3k \; + \; 3\right]}_{\text{par}} \; + \; 1 \end{aligned}$$

nós descobrimos que o número é ímpar.

Ou seja, não depende!

Quer dizer, não importa se n é par ou ímpar, o número $n^2 + n + 5$ é sempre ímpar.

Legal!

Mas, a gente também pode raciocinar de uma outra maneira.

Veja que o nosso número também pode ser escrito assim

$$n^2 \; + \; n \; + \; 5 \quad = \quad n \cdot (n \; + \; 1) \; + \; 5$$

(*Aqui nós estamos montando, ao invés de desmontar ...*)

E agora é bem fácil ver que o número

$$n \cdot (n \; + \; 1)$$

tem que ser par — porque se n é par então $n + 1$ é ímpar, e vice-versa.

E se esse número é par, então o número

$$n \cdot (n + 1) + 5$$

tem que ser ímpar.

$\diamond$

Exemplo 2: *Se você sabe que $m - n$ é par, então o que você pode dizer sobre o número:*

$$m^2 - n^2$$

Par ou ímpar?

Bom, dessa vez depende se m e n são pares ou ímpares ...

Uma maneira simples de decidir a questão consiste em examinar todas as possibilidades:

m	n	$(m-n)$ é par?	(m^2-n^2) é par?
p	p	Sim	Sim
p	i	Não	Não
i	p	Não	Não
i	i	Sim	Sim

Essa tabela mostra apenas as respostas.

Mas, para obter cada resposta é preciso raciocinar.

Por exemplo, na primeira linha nós estamos supondo que tanto m como n são pares.

Nesse caso, é bem fácil ver que $(m - n)$ é par — (*Porque?*)

E se m, n são pares, então m^2, n^2 são pares também — (*Porque?*)

Mas, então isso implica que $m^2 - n^2$ é par.

E isso nos dá a resposta da última coluna.

Nas outras linhas, o raciocínio é análogo.

(*Você quer tentar fazer um?*)

Bom, agora, examinando a tabela, nós vemos que em todas as linhas onde $m - n$ é par (a primeira e a última linha), $m^2 - n^2$ também é par.

Isso significa que a resposta para a pergunta acima é: *Par*!

Mas, como (quase) sempre, essa não é a única maneira de fazer as coisas.

A observação chave, dessa vez, é que o nosso número pode ser escrito como

$$m^2 - n^2 = (m - n) \cdot (m + n)$$

A seguir nós lembramos que $(m - n)$ é par (a pergunta diz isso).

Isso significa que nós podemos escrever

$$(m - n) = 2k$$

Mas então o nosso número pode ser escrito como

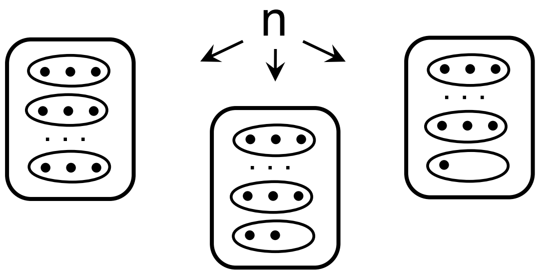
$$m^2 - n^2 = 2k \cdot (m + n)$$

e nós vemos novamente que ele é par! ◇

3 Desmontando números de outras maneiras

Não é verdade que só existem dois tipos de números ...

Na verdade existem três:



Quer dizer, os números que podem ser desmontados em grupinhos de 3, e mais dois tipos de números que não podem ser decompostos assim.

Quando alguém pergunta

- *O número 498375, de que tipo é?*

Todos sabem responder

- *Se você somar os dígitos e der múltiplo de 3, então o número é múltiplo de 3.*

E nesse caso isso é verdade: $4 + 9 + 8 + 3 + 7 + 5 = 36$.

Mas, porque essa regra funciona?

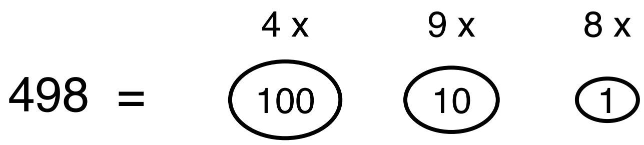
Para entender isso, nós vamos desmontar os números ainda de uma outra maneira.

Você já se deu conta de que ao escrever o número "`quatrocentos e noventa e oito`" como

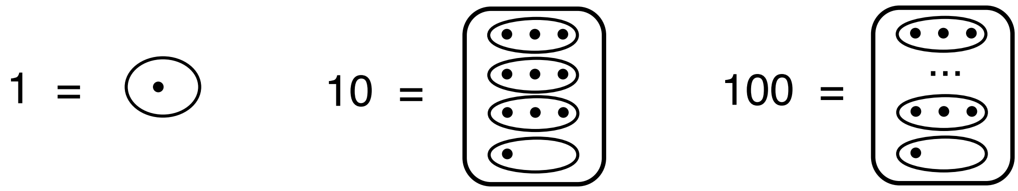
$$4\,9\,8$$

nós já estamos desmontando ele?

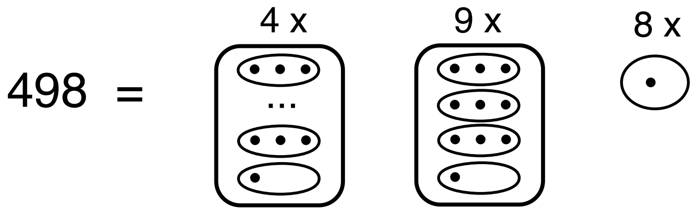
Veja só



E, você já se deu conta de que todas as potências de 10 são números do segundo tipo acima — aqueles onde sobra 1 quando divididos em grupinhos de 3.



Juntando as duas coisas



nós vemos que, ao dividir tudo em grupinhos de 3, vão sobrar

- 4 unidades na primeira parte
- 9 unidades na segunda parte
- 8 unidades na terceira parte

E, se isso que sobra é divisível por 3, então a coisa toda também é divisível por 3.

Legal, não é?

Vejamos outros exemplos.

Exemplo 3: *Na verdade mesmo, existem números de todo tipo ...*

Por exemplo, quando consideramos a divisão por 11, nós descobrimos que existem 11 tipos de números:

$$11k, \quad 11k+1, \quad ,11k+2, \quad \ldots, \quad 11k+10$$

E alguém, um dia, descobriu uma regra para saber se um número é divisível por 11:

- *Some os dígitos das posições ímpares,*
  Some os dígitos das posições pares,
  E subtraia a primeira soma da segunda.
  Se o resultado for divisível por 11,
  Então o seu número é divisível por 11.

Por exemplo, o número 498375 não é divisível por 11:

$$\big[\,9\;+\;3\;+\;5\,\big]\;-\;\big[\,4\;+\;8\;+\;7\,\big]\quad=\quad-2$$

Mas, trocando as posições dos dígitos 3 e 4, nós obtemos o número 398475, que é divisível por 11:

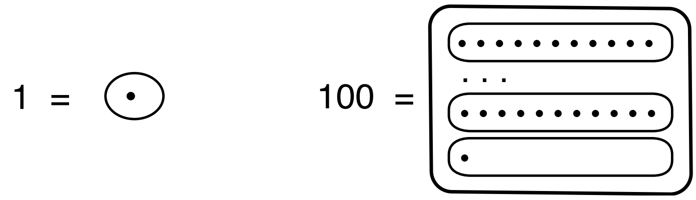
$$\big[\,9\;+\;4\;+\;5\,\big]\;-\;\big[\,3\;+\;8\;+\;7\,\big]\quad=\quad 0$$

Certo.

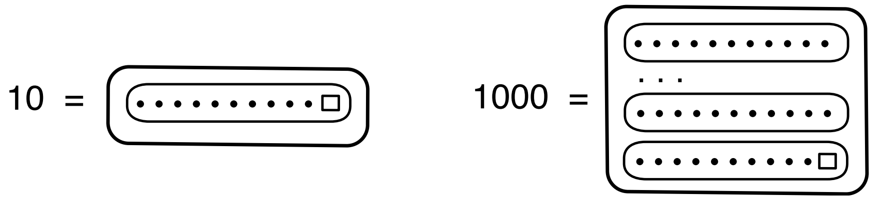
Mas, porque a regra funciona?

Para entender isso, nós observamos que existem dois tipos de potências de 10:

- Aquelas onde <u>*sobra*</u> 1 quando a dividimos por 11:



- E aquelas onde <u>*falta*</u> 1 quando a dividimos por 11:



E agora fica fácil entender a regra:

- *Somando as unidades que sobram das potências pares,*
  E subtraindo as unidades que faltam na potências ímpares,
  Nós descobrimos que, se uma coisa compensa a outra,
  Então a coisa toda pode ser decomposta em grupinhos de 11.

Legal, não é?

◇

Exemplo 4: *Pensando sobre o número 7, alguém descobriu a seguinte regra:*

- *Duplique o último dígito*
  E subtraia o resultado
  Do número formado pelos outros dígitos.
  Se aquilo que der for divisível por 7,
  Então o seu número é divisível por 7.

Abaixo nós temos alguns exemplos simples

672 $\qquad\qquad$ 108

67 - 4 = 63 $\qquad\qquad$ 10 - 16 = - 6

Mas o mais legal é que a regra pode ser aplicada recursivamente

14641

1464 - 2 = 1462

146 - 8 = 138

13 - 16 = - 3

Certo.

Mas, porque a regra funciona?

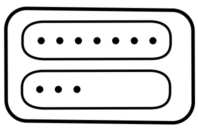
Note que os números agora estão sendo decompostos de uma maneira diferente.

Por exemplo,

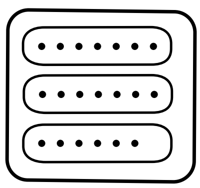
435 x $\qquad$ 6 x

4356 = $\qquad$ 10 $\qquad$ 1

É fácil ver que ao dividir 10 por 7 vão sobrar 3

10 = 

Mas, a esperteza está em observar que ao somar 10 com 10, fica faltando 1

10 + 10 = 

A ideia então é que esse 1 que falta vira da casa das unidades.

Mas, ainda existe uma pequena dificuldade.

Se nós temos uma quantidade ímpar de grupos de 10, como no exemplo acima, então não é possível reagrupá-los em grupos de 20.

Essa é a hora para uma segunda esperteza.

Note que

- *Se x é divisível por 7 então $2x$ também é, e vice-versa.*

Quer dizer, para saber se x é divisível por 7, nós podemos testar o número $2x$!

Agora, observe que

	435 x	2 x 6 x
2 x 4356 =	20	1

E agora é fácil entender a regra ...

Rá, esse foi legal mesmo!

◇

4 Demonstração por desmontação

A seguir nós vamos ver que a técnica de raciocínio por decomposição (ou desmontaçã) é muito poderosa.

Quer dizer, nós podemos chegar muito longe apenas *desmontando, desmontando, desmontando, ...*

Abaixo nós temos dois exemplos.

Exemplo 5: *Alguém diz para você que o número*

$$2^{2n+1} \; + \; 1$$

é sempre divisível por 3.

Mas, será que isso é verdade?

Vejamos.

Todo mundo sabe que

$$2^a \;\times\; 2^b \;=\; 2^{a+b}$$

Olhando essa equação da esquerda para a direita nós temos uma *regra de montar.*

E olhando a equação da direita para a esquerda nós temos uma *regra de desmontar.*

Utilizando a segunda regra, nós desmontamos o nosso número da seguinte maneira:

$$2^{2n+1} \; + \; 1 \quad \Rightarrow \quad 2 \cdot 2^{2n} \; + \; 1$$

E (quase) todo mundo sabe também que

$$2^{a \times b} \quad = \quad (2^a)^b$$

Mais uma vez, a equação nos dá uma regra de montar e uma regra de desmontar.

Utilizando a regra de desmontar, nós transformamos o nosso número mais uma vez

$$2 \cdot 2^{2n} \ + \ 1 \quad \Rightarrow \quad 2 \cdot \left(2^2\right)^n \ + \ 1$$

E, como todo mundo sabe que $2^2 = 4$, nós podemos escrever o nosso número agora dessa maneira:

$$2 \cdot 4^n \ + \ 1$$

Legal.

O próximo passo consiste em desmontar o 4

$$2 \cdot (3+1)^n \ + \ 1$$

E em seguida nós desmontamos a potência

$$2 \cdot \underbrace{(3+1) \cdot (3+1) \cdot \ldots \cdot (3+1)}_{\text{n vezes}} \ + \ 1$$

Agora, concentre a sua atenção na expressão

$$(3+1) \cdot (3+1) \cdot \ldots \cdot (3+1)$$

Desmontar essa expressão significa realizar todas as multiplicações indicadas, mas isso deixaria as coisas muito complicadas.

A solução, então, consiste em apenas imaginar o que acontece quando realizamos as multiplicações.

O que a gente vê (?) quando imagina isso

$$\underbrace{(3+1)}_{*} \cdot \underbrace{(3+1)}_{*} \cdot \ \ldots \ \cdot \underbrace{(3+1)}_{*} \cdot$$

é que os termos que aparecem no resultado são montados selecionando um número em cada par de parênteses, e multiplicando todos eles.

Por exemplo,

$$3 \cdot 3 \cdot 3 \cdot \ldots \cdot 3 \qquad \text{ou} \qquad 1 \cdot 3 \cdot 1 \cdot \ldots \cdot 3 \qquad \text{ou} \qquad 1 \cdot 1 \cdot 1 \cdot \ldots \cdot 3$$

Quando a gente vê isso, a gente percebe que todos eles possuem um fator 3, com a exceção do termo

$$1 \cdot 1 \cdot 1 \cdot \ldots \cdot 1$$

Ora, todo termo que possui um fator 3 pode ser decomposto em grupinhos de 3.

Portanto, quando nós decompomos a coisa toda em grupinhos de 3 vai sobrar 1.

Quer dizer, nós podemos escrever

$$(3+1) \cdot (3+1) \cdot \ldots \cdot (3+1) \quad = \quad 3k \;+\; 1$$

Levando esse resultado de volta para a nossa expressão original, nós obtemos

$$2 \cdot (3+1)^n \;+\; 1 \qquad = \qquad 2 \cdot \big(3k+1\big) \;+\; 1$$

E, fazendo as contas

$$2 \cdot \big(3k+1\big) \;+\; 1 \qquad = \qquad 6k \;+\; 2 \;+\; 1 \qquad = \qquad 6k \;+\; 3$$

é bem fácil ver que o número é divisível por 3.

$\diamond$

Exemplo 6: *Agora suponha que alguém diz para você que o número*

$$2^n \;-\; 1$$

só pode ser primo se o número n é primo também.

Será que isso é verdade?

Bom, antes de começar a raciocinar, é importante entender a lógica da coisa direito.

Veja que o seu amigo <u>não</u> está dizendo que se n é primo então $2^n - 1$ é primo também.

Quer dizer, isso pode até ser verdade em alguns casos como

$$2^2 \;-\; 1 \quad = \quad 3 \qquad\qquad \text{ou} \qquad\qquad 2^7 \;-\; 1 \quad = \quad 127$$

Mas, eventualmente nós descobrimos que

$$2^{11} \;-\; 1 \quad = \quad 2047 \quad = \quad 23 \times 89$$

Certo.

Mas, então, o que o seu amigo está tentando dizer?

Bom, ele está tentando dizer que

- *o número* $2^n - 1$ <u>*não*</u> *pode ser primo*

  se n <u>*não*</u> *for primo também*

O que é uma maneira meio complicada de dizer que

- *se* n *é um número composto*

  então $2^n - 1$ *é um número composto também*

Legal.

Mas, será que isso é verdade?

Vejamos.

A primeira observação é que um *número composto* é um número que pode ser decomposto

$$n \quad = \quad a \times b$$

E o exemplo mais simples de números compostos são os números pares

$$n \quad = \quad 2b$$

(Quer dizer, os números pares maiores que 2 — pois o 2 não pode ser decomposto ...)

Nós podemos, então, começar trabalhando com a situação em que $n = 2b$.

Nesse caso, nós podemos desmontar o nosso número da seguinte maneira

$$2^{2b} \; - \; 1 \quad = \quad \left(2^b\right)^2 \; - \; 1$$

Daí a gente lembra que

$$x^2 \; - \; 1 \quad = \quad (x \; - \; 1) \cdot (x \; + \; 1)$$

O que nos permite a desmontar o nosso número mais um pouquinho

$$\left(2^b\right)^2 \; - \; 1 \quad = \quad (2^b \; - \; 1) \cdot (2^b \; + \; 1)$$

E isso já mostra que o número é composto nesse caso.

Legal.

Mas, será que a gente consegue repetir esse argumento em outros casos?

Vejamos.

Suponha dessa vez que o número n é divisível por 3, isto é, $n = 3k$.

Daí, nós podemos perguntar se o nosso número pode ser decomposto como:

$$2^{3b} - 1 = (2^b - 1) \cdot (\ ?\ \ ?\ \ ?\ )$$

A primeira observação é que a segunda parte deve conter o termo 2^{2b}.

Porque?

Bom, porque ao multiplicar 2^{2b} pelo termo 2^b (na primeira parte), nós obtemos o termo 2^{3b} que faz parte do resultado.

O problema é que isso gera o efeito colateral -2^{2b}, que é o resultado da multiplicação do termos 2^{2b} pelo -1 da primeira parte.

Esse problema pode ser resolvido adicionando o termo 2^b à segunda parte, veja só

$$\begin{aligned}(2^b - 1) \cdot (2^{2b} + 2^b) &= 2^{3b} - 2^{2b} + 2^{2b} - 2^b \\ &= 2^{3b} - 2^b\end{aligned}$$

O problema, como se pode ver, é que isso introduz o efeito colateral -2^b.

Mas, o problema é resolvido adicionando mais um termo à segunda parte

$$\begin{aligned}(2^b - 1) \cdot (2^{2b} + 2^b + 1) &= 2^{3b} - 2^{2b} + 2^{2b} - 2^b + 2^b - 1 \\ &= 2^{3b} - 1\end{aligned}$$

E isso já mostra que o número $2^{3b} - 1$ é composto.

Não é legal?

O mais legal é que isso funciona para qualquer número.

Por exemplo, não é difícil verificar que

$$2^{5b} - 1 = (2^b - 1) \cdot (2^{4b} + 2^{3b} + 2^{2b} + 2^b + 1)$$

E agora, nós podemos finalizar o argumento com a observação geral de que

$$2^{a \cdot b} - 1 = (2^b - 1) \cdot (2^{(a-1)b} + \ldots + 2^{2b} + 2^b + 1)$$

que prova que todos os números da forma $2^{a \cdot b} - 1$ são compostos.

◇