

Matemática Discreta

aula 05: Vendo a divisibilidade

1 Introdução

Abrindo um livro de matemática ao acaso, a gente encontra o seguinte

$$\rightarrow 2^{2n} - 1 \text{ é sempre divisível por } 3$$

Mas porque?

Ou melhor, como é que a gente vê isso?

Bom, a resposta é: desmontando.

E a gente começa desmontando a palavra ‘sempre’.

Quer dizer, a palavra ‘sempre’ significa que todos os números abaixo são divisíveis por 3

$$2^2 - 1, \quad 2^4 - 1, \quad 2^6 - 1, \quad 2^8 - 1, \quad 2^{10} - 1, \quad \dots$$

Mas porque?

Bom, aqui a gente precisa desmontar outra vez.

Quer dizer, primeiro a gente nota que as potências de 2 são todas pares.

E daí, a gente reescrev qualquer um dos termos assim

$$\underbrace{2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot \dots \cdot 2 \cdot 2}_{2k} = 1$$

Daí, porque isso é uma quantidade par de 2's, a gente pode formar grupinhos assim

$$\underbrace{(2 \cdot 2) \cdot (2 \cdot 2) \cdot (2 \cdot 2) \cdot \dots \cdot (2 \cdot 2)}_{2n} = 1$$

Finalmente, fazendo a multiplicação dentro de cada grupinho, a gente chega no seguinte

$$\underbrace{4 \cdot 4 \cdot 4 \cdot \dots \cdot 4}_k = 1$$

Quer dizer, no final das contas, a frase do livro está falando de potências de 4

$$4^1 - 1, \quad 4^2 - 1, \quad 4^3 - 1, \quad 4^4 - 1, \quad 4^5 - 1, \quad \dots$$

Sim, mas porque essas coisas são divisíveis por 3?

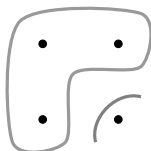
Ora, mas isso é uma coisa bem fácil de ver.

Só que para isso, a gente vai ter que desmontar outra vez.

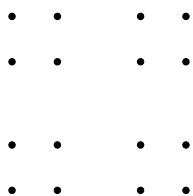
Quer dizer, a gente começa notando que o 4 é um quadrado



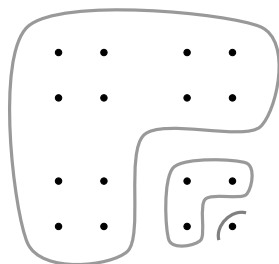
E daí a gente vê que tirando 1 do quadrado, aquilo que sobra é divisível por 3



A seguir, a gente nota que o 4^2 é um quadrado de quadrados

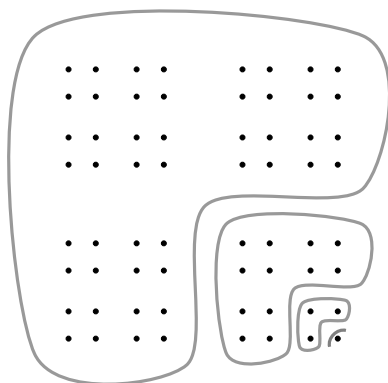


E daí a gente vê que tirando 1 do quadrado de quadrados, aquilo que sobra é divisível por 3



A seguir, a gente nota que o 4^3 é um quadrado de quadrados de quadrados.

E daí a gente vê que tirando 1, aquilo que sobra é divisível por 3



Legal.

Já deu pra ver que a coisa entrou em repetição.

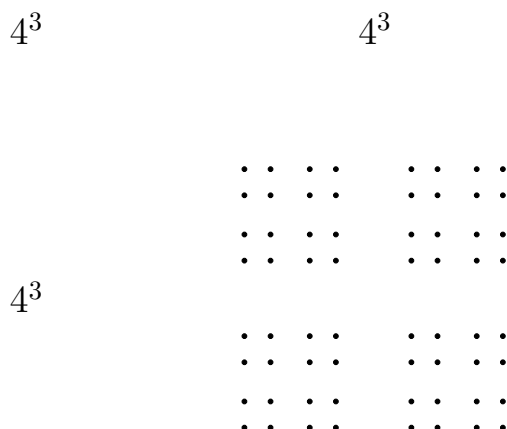
Mas, como é que a gente vê isso?

Bom, dessa vez a resposta é: montando.

Quer dizer, agora a gente vai olhar para o 4^4 .

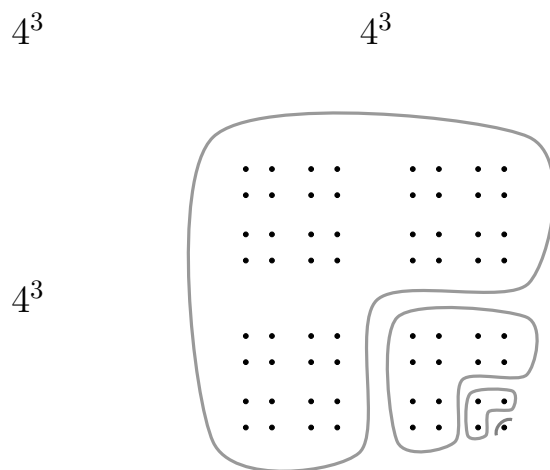
A gente já sabe que o 4^4 é um quadrado de quadrados de quadrados de quadrados.

E a gente monta ele assim



Sim! o 4^3 aparece dentro do 4^4 .

Pois é, e tirando 1 de uma das cópias, essa cópia fica divisível por 3



E é claro que as outras 3 cópias juntas também são uma coisa divisível por 3.

Logo, a coisa toda é divisível por 3 — (*depois que a gente tira 1*)

Legal!

Sim, mas essa não é a única maneira de ver a repetição.

Quer dizer, a gente também pode escrever a figura aí de cima assim

$$4^4 = 3 \cdot 4^3 + 3 \cdot 4^2 + 3 \cdot 4 + 3 + 1$$

Daí, a gente olha para o 4^5 .

E vê que ele é um quadrado de 4^4 assim

$$4^5 = 4 \cdot 4^4$$

O próximo passo é reescrever a coisa assim

$$4^5 = 3 \cdot 4^4 + 4^4$$

e depois assim

$$4^5 = 3 \cdot 4^4 + \underbrace{3 \cdot 4^3 + 3 \cdot 4^2 + 3 \cdot 4 + 3 + 1}_{4^4}$$

Agora, já é bem fácil ver que tirando 1, aquilo que sobra é divisível por 3.

Legal!

Sim, mas essa não é a única maneira de ver a repetição.

Quer dizer, a gente também pode ver a repetição desmontando.

Para isso, a gente olha para o 4^n .

Mas ...

Sim, o n é um “*número qualquer*” ...

E a gente pode raciocinar com ele também.

Quer dizer, o 4^n é um quadrado que a gente pode desmontar assim

$$4^n = 4 \cdot 4^{n-1}$$

e depois reescrever assim

$$4^n = 3 \cdot 4^{n-1} + 4^{n-1}$$

Daí, a gente desmonta o 4^{n-1}

$$4^n = 3 \cdot 4^{n-1} + 3 \cdot 4^{n-2} + 4^{n-2}$$

Já deu pra ver o que está acontecendo, não é?

Quer dizer, a gente pode continuar desmontando a potência de 4 que aparece no fim.

Porque as potências de 4 são como uma cebola.

Ou melhor, as potências de 4 são como um rocambole — (*porque a cebola não tem caroço, mas o rocambole tem ...*)

Daí, desenrolando o rocambole até o fim a gente vê o caroço — (*ou o recheio*)

$$4^n = 3 \cdot 4^{n-1} + \dots + 3 \cdot 4^2 + 3 \cdot 4 + 3 + 1$$

Sim! o caroço é o 1!

Pois é, daí ao tirar o caroço do rocambole, a gente vê que aquilo que sobra é divisível por 3

$$4^n - 1 = 3 \cdot 4^{n-1} + \dots + 3 \cdot 4^2 + 3 \cdot 4 + 3$$

Legal!

Sim, mas isso é uma coisa que a gente já sabia.

Quer dizer, vamos escrever a coisa ao contrário

$$3 + 3 \cdot 4 + 3 \cdot 4^2 + \dots + 3 \cdot 4^{n-1} = 4^n - 1$$

Daí, a gente coloca o 3 em evidência

$$3 \cdot [1 + 4 + 4^2 + \dots + 4^{n-1}] = 4^n - 1$$

E daí a gente passa o 3 para o outro lado

$$1 + 4 + 4^2 + \dots + 4^{n-1} = \frac{4^n - 1}{3}$$

Essa é a fórmula da soma da PG!

É isso aí ...

2 Mais truques de desmontação

Vamos olhar outra vez para isso aqui

$$\rightarrow 2^{2n} - 1 \text{ é sempre divisível por 3}$$

E daí, concentrando a atenção aqui

$$2^{2n} - 1$$

a gente pode pensar que alguém chegou aqui depois de usar o truque do peteleco

$$2^{2n} - 1 = 1 + 2 + 2^2 + 2^3 + \dots + 2^{2n-1}$$

— (*sim, isso é mais um truque de desmontação ...*)

Daí, o que o livro está dizendo é que essa soma é sempre divisível por 3.

Será?

Bom, vamos olhar para cada termo.

Ou melhor, vamos olhar para o resto de cada termo na divisão por 3

$$\begin{array}{ccccccccccc} 2^{2n} - 1 & = & 1 & + & 2^1 & + & 2^2 & + & 2^3 & + & 2^4 & + & \dots & + & 2^{2n-1} \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & & & \\ & & 1 & & 2 & & 1 & & 2 & & 1 & & \dots & & \end{array}$$

Sim! a coisa entra em repetição — (*é sempre assim, ou será que não?*)

Daí a gente nota que nas potências pares o resto é 1, e nas potências ímpares o resto é 2

$$\begin{array}{cccccccc}
 2^{2n} - 1 & = & 1 & + & 2^1 & + & 2^2 & + & 2^3 & + & \dots & + & 2^{2n-2} & + & 2^{2n-1} \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \dots & & \downarrow & & \downarrow \\
 & & 1 & & 2 & & 1 & & 2 & & \dots & & 1 & & 2
 \end{array}$$

E daí, a gente nota que ao somar os pares de termos consecutivos, o resto sempre dá 3 — (*o que é o mesmo que resto 0*)

$$\begin{array}{cccccccc}
 2^{2n} - 1 & = & 1 & + & 2^1 & + & 2^2 & + & 2^3 & + & \dots & + & 2^{2n-2} & + & 2^{2n-1} \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \dots & & \downarrow & & \downarrow \\
 & & 1 & & 2 & & 1 & & 2 & & \dots & & 1 & & 2 \\
 & & \underbrace{\hspace{1.5cm}} & & & & \underbrace{\hspace{1.5cm}} & & & & & & \underbrace{\hspace{1.5cm}} & & \\
 & & 3 & & & & 3 & & & & & & 3 & &
 \end{array}$$

E aqui já dá pra ver que a coisa toda é divisível por 3.

Legal, não é?

Sim, mas essa não é a única maneira de ver as coisas.

Quer dizer, vamos dar um passo atrás e olhar outra vez para isso

$$2^{2n} - 1 = 1 + 2 + 2^2 + 2^3 + \dots + 2^{2n-2} + 2^{2n-1}$$

A gente pode pensar que alguém chegou aqui depois de usar o truque do peteleco

Daí, a esperteza dessa vez é reescrever a coisa assim

$$2^{2n} - 1 = 1 + 2 \cdot 1 + 2^2 + 2 \cdot 2^2 + \dots + 2^{2n-2} + 2 \cdot 2^{2n-2}$$

e depois assim

$$2^{2n} - 1 = (1 + 2) \cdot 1 + (1 + 2) \cdot 2^2 + \dots + (1 + 2) \cdot 2^{2n-2}$$

e depois assim

$$2^{2n} - 1 = 3 \cdot 1 + 3 \cdot 2^2 + \dots + 3 \cdot 2^{2n-2}$$

Pronto! aqui a gente já pode ver outra vez que $2^{2n} - 1$ é sempre divisível por 3.

Legal.

Mas, essa não é a única maneira de ver as coisas.

Quer dizer, vamos olhar mais uma vez para isso

$$2^{2n} - 1 = 1 + 2 + 2^2 + 2^3 + \dots + 2^{2n-1}$$

o que a gente reescreve assim

$$2^{2n} - 1 = 1 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3 + \dots + 1 \cdot 2^{2n-1}$$

O que é isso?

Bom, a gente pode pensar que isso é um número na base 2

$$2^n - 1 = \underbrace{(111 \dots 111)}_{2n}_2$$

Agora, a gente quer ver que isso é divisível por 3.

Ora, então basta aplicar a regra do 3 na base 2.

Que regra é essa?

Bom, o 3 é o “onze” da base 2.

Logo, nós usamos a regra do 11

→ Some os dígitos das posições ímpares
some os dígitos das posições pares
e subtraia uma coisa da outra

Se aquilo que der for divisível por $(11)_2$
então o seu número é divisível por $(11)_2$

Daí, aplicando essa regra a gente obtém o seguinte

$$\underbrace{[1 + 1 + \dots + 1 + 1]}_n - \underbrace{[1 + 1 + \dots + 1 + 1]}_n = 0$$

Logo, $2^{2n} - 1$ é divisível por 3.

Legal, não é?

Sim, mas essa não é a única maneira de ver as coisas.

Quer dizer, vamos colocar outra vez a atenção no termo

$$2^{2n} - 1$$

E vamos lembrar que isso é igual a

$$4^n - 1$$

Daí a gente pergunta: *O que é isso?*

Bom, a resposta é: depende de como se olha ...

Dessa vez, a gente quer olhar a coisa na base 4.

E para ver o que é isso na base 4, primeiro a gente nota que

$$10^n = \text{um } n\text{-lhão}$$

— (*i.e.*, 1 seguido por n zeros)

Daí que, o 4^n é o um n -lhão da base 4.

Agora, a gente pode reescrever a coisa assim

$$4^n - 1 = (100 \dots 000)_4 - 1$$

E fazendo essa continha, a gente obtém o seguinte

$$4^n - 1 = (333 \dots 333)_4$$

E aqui já dá pra ver outra vez que a coisa é divisível por 3.

2.1 Generalização

A gente já viu muitas vezes que $2^{2n} - 1$ é divisível por 3.

Então agora a gente pode tentar ver outras coisas.

E a gente pode utilizar qualquer um dos nossos caminhos de raciocínio para ver isso — (*contanto que a coisa seja parecida*)

Por exemplo, considere a expressão

$$2^{3n} - 1$$

Aqui já não é difícil reescrever a coisa assim

$$(2^3)^n - 1$$

e depois assim

$$8^n - 1$$

Nesse ponto, a gente reconhece o um n -lhão da base 8.

Daí, a gente reescreve a coisa assim

$$8^n - 1 = (100 \dots 000)_8 - 1$$

e faz a continha para obter

$$(777 \dots 777)_8$$

Pronto, nós acabamos de descobrir que

$$\rightarrow 2^{3n} - 1 \text{ é sempre divisível por } 7$$

A seguir, a gente olha para a expressão

$$2^{4n} - 1$$

E daí, a gente raciocina assim

$$\begin{aligned}
 2^{4n} - 1 &= (2^4)^n - 1 \\
 &= 16^n - 1 \\
 &= (100 \dots 000)_{16} - 1 \\
 &= ((15)(15)(15) \dots (15)(15)(15))_{16}
 \end{aligned}$$

o que já mostra que a coisa é divisível por 15.

Logo, nós descobrimos que

$$\rightarrow 2^{4n} - 1 \text{ é sempre divisível por } 15$$

Aqui já dá pra notar que a coisa entrou em repetição.

Para ver o padrão repetitivo, a gente reescreve a coisa assim

$$\rightarrow 2^{4n} - 1 \text{ é sempre divisível por } 2^4 - 1$$

E agora, a gente escreve a repetição assim

$$\rightarrow 2^{kn} - 1 \text{ é sempre divisível por } 2^k - 1$$

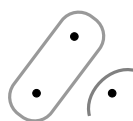
3 Vendo a divisibilidade

Para obter outra generalização fácil, a gente começa observando que

$$\rightarrow 3^n - 1 \text{ é sempre divisível por } 2$$

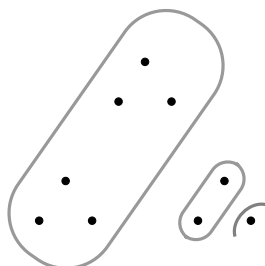
Porque o 3 é um triângulo.

E tirando 1 do triângulo, aquilo que sobra é divisível por 2



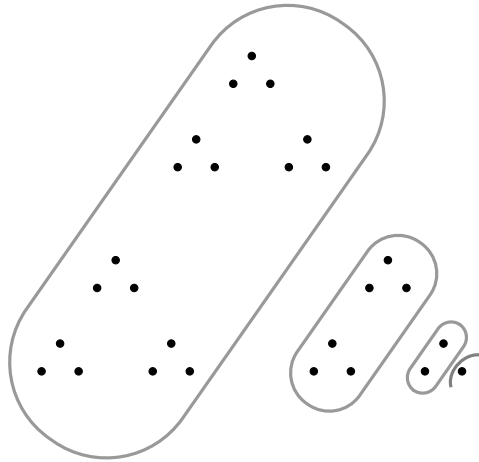
Daí, a gente nota que o 3^2 é um triângulo de triângulos.

E tirando 1 do triângulo de triângulos, aquilo que sobra é divisível por 2



Daí, a gente nota que o 3^3 é um triângulo de triângulos de triângulos.

E tirando 1 do triângulo de triângulos de triângulos, aquilo que sobra é divisível por 2

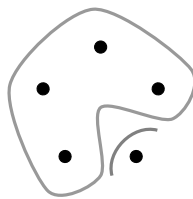


E por aí vai ...

A coisa também funciona para o 5.

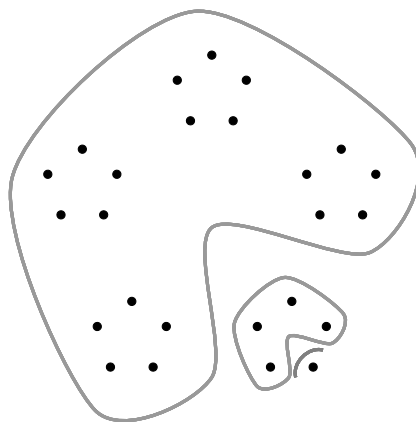
Porque o 5 é um pentágono.

E tirando 1 do pentágono, aquilo que sobra é divisível por 4



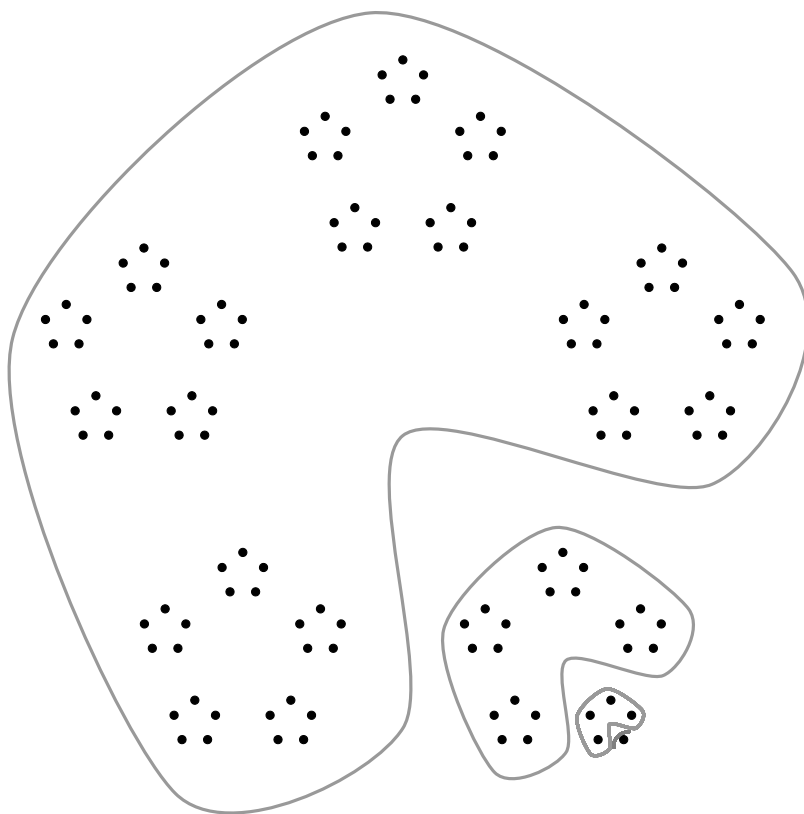
Daí a gente nota que o 5^2 é um pentágono de pentágonos.

E tirando 1 do pentágono de pentágonos, aquilo que sobra é divisível por 4



Daí a gente nota que o 532 é um pentágono de pentágonos de pentágonos.

E tirando 1 do pentágono de pentágonos de pentágonos, aquilo que sobra é divisível por 4



E por aí vai ...

Quer dizer, a coisa sempre funciona.

Porque o princípio da coisa é sempre o mesmo.

Então, nós acabamos de descobrir que

$$\rightarrow k^n - 1 \text{ é sempre divisível por } k - 1$$

3.1 Mais divisibilidade

Mas isso ainda não é tudo.

Porque um pouquinho mais adiante no livro, a gente encontra o seguinte

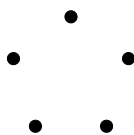
$$\rightarrow 5^n - 2^n \text{ é sempre divisível por } 3$$

E agora?

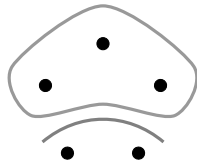
Como é que a gente vê isso?

Bom, a resposta é sempre: desmontando.

E a gente começa desmontando o 5

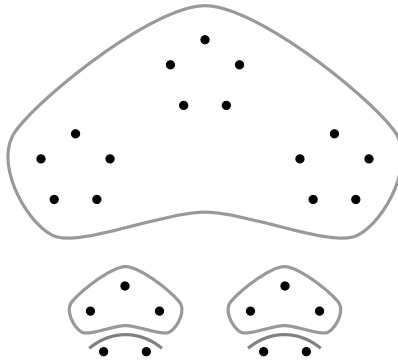


E daí a gente vê que tirando 2 do pentágono, aquilo que sobra é divisível por 3



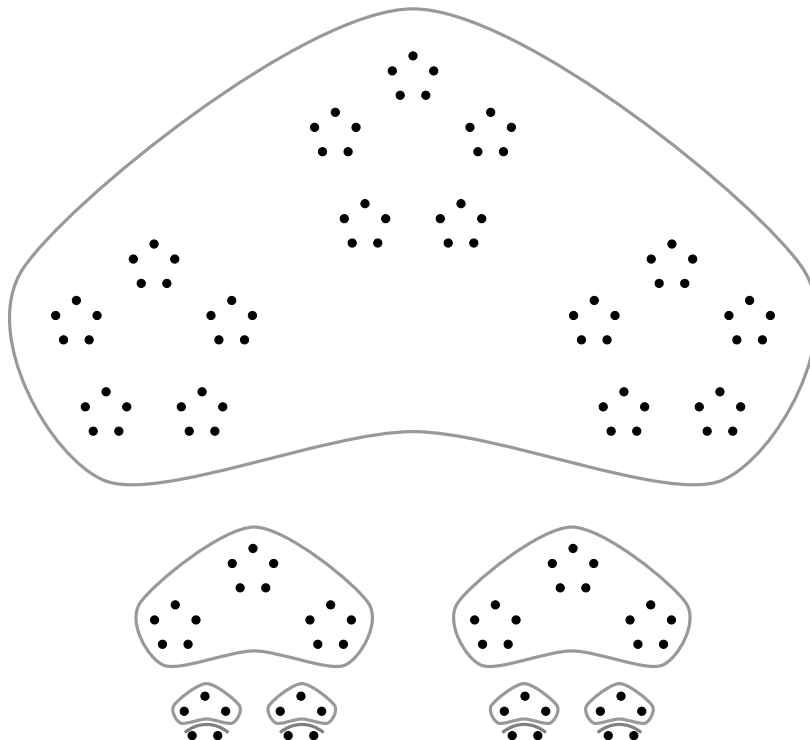
Daí a gente lembra que o 5^2 é um pentágono de pentágonos.

E vê que tirando duas vezes 2 do pentágono de pentágonos, aquilo que sobra é divisível por 3



Daí, a gente lembra que o 5^3 é um pentágono de pentágonos de pentágonos.

E vê que tirando duas vezes duas vezes 2 do pentágono de pentágonos de pentágonos, aquilo que sobra é divisível por 3



E por aí vai ...

Certo.

Mas porque funciona?

Bom, vamos começar com o pentágono de pentágonos de pentágonos

$$5^3$$

Daí a gente desmonta assim

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

e depois assim

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

A seguir a gente foca no segundo 5^2 .

Daí a gente desmonta ele assim

$$5^3 = 3 \cdot 5^2 + 2 \cdot (5 \cdot 5)$$

e depois assim

$$5^3 = 3 \cdot 5^2 + 2 \cdot (3 \cdot 5 + 2 \cdot 5)$$

Finalmente, a gente foca no segundo 5 — (*dentro dos parênteses*)

Daí a gente desmonta ele assim

$$5^3 = 3 \cdot 5^2 + 2 \cdot (3 \cdot 5 + 2 \cdot (3 + 2))$$

Agora, a gente pode fazer as multiplicações

$$5^3 = 3 \cdot 5^2 + 2 \cdot \left(3 \cdot 5 + \underbrace{2 \cdot (3 + 2)}_{3 \cdot 2 + 2^2} \right)$$

$$\underbrace{\hspace{10em}}_{3 \cdot 2 \cdot 5 + 3 \cdot 2^2 + 2^3}$$

o que dá

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

E passando o 2^3 para o outro lado

$$5^3 - 2^3 = 3 \cdot 5^2 + 3 \cdot 2 \cdot 5 + 3 \cdot 2^2$$

a gente vê que $5^3 - 2^3$ é divisível por 3.

Na prática, esse raciocínio é igual à figura — (*you can see it?*)

E agora a gente pode repetir ele para o 5^4 .

Quer dizer, a gente começa desmontando assim

$$5^4 = 5 \cdot 5^3$$

e depois assim

$$5^4 = 3 \cdot 5^3 + 2 \cdot 5^3$$

A seguir, a gente foca no segundo 5^3 .

E substitui ele pela expressão que a gente encontrou mais acima

$$5^4 = 3 \cdot 5^3 + 2 \cdot [3 \cdot 5^2 + 3 \cdot 2 \cdot 5 + 3 \cdot 2^2 + 2^3]$$

Fazendo a multiplicação, a gente obtém

$$5^4 = 3 \cdot 5^3 + 3 \cdot 2 \cdot 5^2 + 3 \cdot 2^2 \cdot 5 + 3 \cdot 2^3 + 2^4$$

E passando o 2^4 para o outro lado

$$5^4 - 2^4 = 3 \cdot 5^3 + 3 \cdot 2 \cdot 5^2 + 3 \cdot 2^2 \cdot 5 + 3 \cdot 2^3$$

a gente vê que $5^4 - 2^4$ é divisível por 3.

Quer dizer, aqui a gente já viu a repetição.

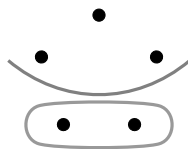
E assim já dá pra ver que

$$\rightarrow 5^n - 2^n \text{ é sempre divisível por } 3$$

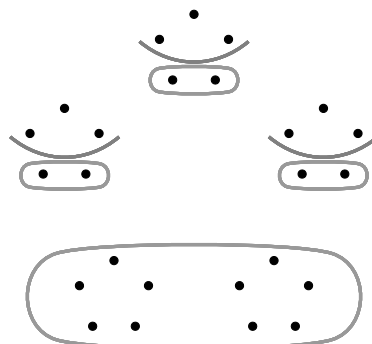
Mas isso ainda não é tudo.

Porque a gente também pode fazer o contrário.

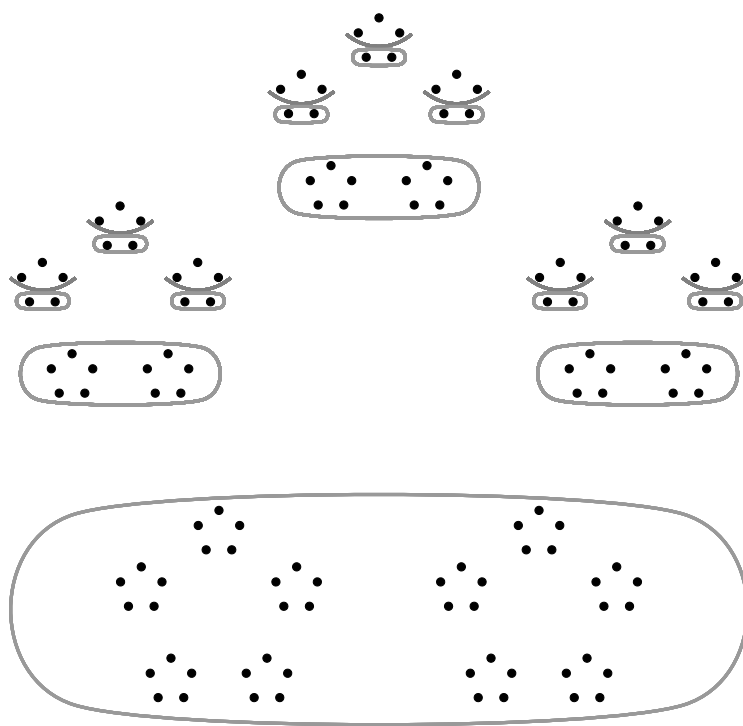
Quer dizer, se a gente tira 3 do pentágono, aquilo que sobra é divisível por 2



E se a gente tira três vezes 3 do pentágono de pentágonos, aquilo que sobra é divisível por 2



E se a gente tira três vezes três vezes 3 do pentágono de pentágonos de pentágonos, aquilo que sobra é divisível por 2



Aqui a gente já viu a repetição.

E assim já dá pra ver que

$$\rightarrow 5^n - 3^n \text{ é sempre divisível por } 2$$

Quer dizer, o princípio da coisa é o mesmo.

E ele funciona sempre.

Por exemplo, agora a gente vai ver que

$$\rightarrow 7^n - 4^n \text{ é sempre divisível por } 3$$

Bom, o 7 é o heptágono.

E tirando 4 do heptágono, aquilo que sobra é divisível por 3

$$7 - 4 = 3$$

A seguir, a gente nota que o 7^2 é o heptágono de heptágonos

$$7^2 = 7 \cdot 7$$

Daí, a gente desmonta a coisa assim

$$7^2 = 3 \cdot 7 + 4 \cdot 7$$

reescreve a coisa assim

$$7^2 = 3 \cdot 7 + 4 \cdot (3 + 4)$$

e depois assim

$$7^2 = 3 \cdot 7 + 3 \cdot 4 + 4^2$$

e depois assim

$$7^2 - 4^2 = 3 \cdot 7 + 3 \cdot 4$$

E aqui a gente vê que tirando quatro vezes 4 do heptágono de heptágonos, aquilo que sobra é divisível por 3.

A seguir, a gente nota que o 7^3 é o heptágono de heptágonos de heptágonos

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

Daí, a gente desmonta a coisa assim

$$7^3 = 3 \cdot 7^2 + 4 \cdot 7^2$$

E substitui o segundo 7^2 pela expressão que a gente encontrou antes

$$7^3 = 3 \cdot 7^2 + 4 \cdot [3 \cdot 7 + 3 \cdot 4 + 4^2]$$

o que a gente reescreve assim

$$7^3 = 3 \cdot 7^2 + 3 \cdot 4 \cdot 7 + 3 \cdot 4^2 + 4^3$$

e depois assim

$$7^3 - 4^3 = 3 \cdot 7^2 + 3 \cdot 4 \cdot 7 + 3 \cdot 4^2$$

E aqui a gente vê que tirando quatro vezes quatro vezes 4 do heptágono de heptágonos de heptágonos, aquilo que sobra é divisível por 3.

Aqui a gente já viu a repetição.

E assim já dá pra ver que

$$\rightarrow 7^n - 4^n \text{ é sempre divisível por 3}$$

Quer dizer, o princípio da coisa é sempre o mesmo — (na figura ou por escrito)

Então agora a gente pode escrever

$$\rightarrow a^n - b^n \text{ é sempre divisível por } a - b$$