Matemática Discreta

aula 08: Números primos e o MMC

1 Introdução

Nas últimas duas aulas nós vimos várias maneiras de desmontar números.

Mas a maneira mais velha de fazer isso é a *decomposição em fatores primos* — (*Euclides já fazia isso em 300AC*)

Bom, todo mundo sabe o que é um *número primo*.

Quer dizer, um número primo é um número que não pode ser dividido por nenhum outro.

A não ser por ele mesmo — (*que não é algum outro*)

E a não ser pelo 1 — (*mas o 1 não conta ...*)

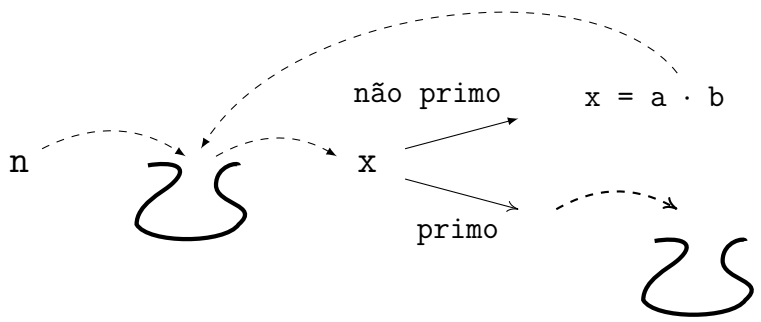
Certo.

Essa definição já implica que todo número pode ser decomposto em fatores primos — (*porque?*)

Quer dizer, ninguém divide os números primos, mas os números primos dividem todos os outros.

E isso é bem fácil de ver.

Considere o seguinte programa de computador



O programa funciona assim

- Tudo começa quando você coloca um número n dentro do primeiro saquinho.
- E daí, a coisa fica rodando até que esse saquinho fique vazio.
- A cada volta, a gente pega um número x do primeiro saquinho, e daí existem duas opções:
  - → se x é primo, então ele é colocado no segundo saquinho
  - → se x não é primo, então existe alguém que divide ele, e nós podemos escrever $x = a \cdot b$; daí, nós pegamos os números a, b e colocamos de volta no primeiro saquinho

Quando a coisa acaba, o segundo saquinho contém uma decomposição de n em fatores primos

$$n \quad = \quad p_1 \cdot p_2 \cdot \ldots \cdot p_k$$

Mas quem disse que a coisa acaba?

Quer dizer, em princípio, o programa podia ficar rodando para sempre.

Mas não pode.

E isso também é bem fácil de ver.

A observação chave é que sempre que x não é primo e nós escrevemos

$$x \quad = \quad a \cdot b$$

os números a e b são menores do que x.

— (*quer dizer, a menos que a ou b seja igual a 1; mas o 1 não conta — ele não entra nesse jogo*)

Daí que, os números do primeiro saquinho vão sempre ficando menores.

Até que uma hora eles viram números primos
— (*porque eles não podem ficar menores para sempre, e nem podem chegar em 1*)

E nessa hora eles são colocados no segundo saquinho.

Logo, mais cedo ou mais tarde, o primeiro saquinho sempre acaba ficando vazio.

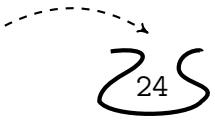
Legal, não é?

2 Unicidade da fatoração em primos

Mas, o mais legal é que só existe uma maneira de decompor um número em fatores primos.

Só que isso não é assim tão fácil de se ver.

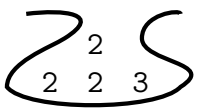
Por exemplo, imagine que você coloca o 24 dentro do primeiro saquinho



Daí, quando você tira ele do outro lado, existem várias maneiras de escrever o 24 como um produto

- $24 \quad = \quad 2 \cdot 12$
- $24 \quad = \quad 4 \cdot 6$
- $24 \quad = \quad 8 \cdot 3$
- $24 \quad = \quad 3 \cdot 8$
- $24 \quad = \quad 6 \cdot 4$
- $24 \quad = \quad 12 \cdot 2$

Mas não importa o caminho que você escolha, no final das contas você sempre vai terminar com a mesma coisa no segundo saquinho



Quer dizer

$$24 \quad = \quad 2 \cdot 2 \cdot 2 \cdot 3$$

é a única maneira de decompor o número 24 em fatores primos.

Mas, porque isso?

Bom, porque os primos tem uma propriedade legal.

Quer dizer, o produto de primos diferentes sempre dá um resultado diferente

$$p_1 \cdot p_2 \quad \neq \quad p_3 \cdot p_4$$

Mas, como é que a gente vê isso?

Bom, na prática a gente mostra que o produto de dois primos

$$p_1 \ \cdot \ p_2$$

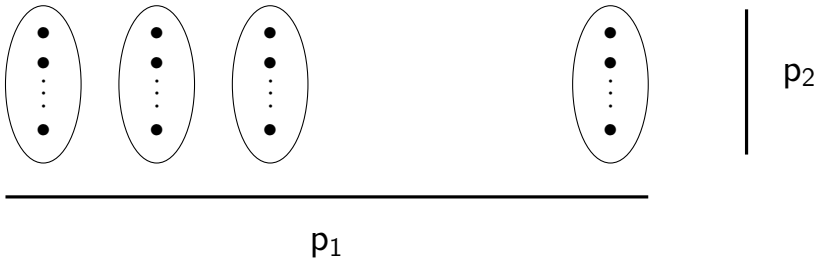
nunca é divisível por um terceiro primo p_3 — (*e isso já implica a desiguladade acima*)

Vejamos como é isso.

Argumento

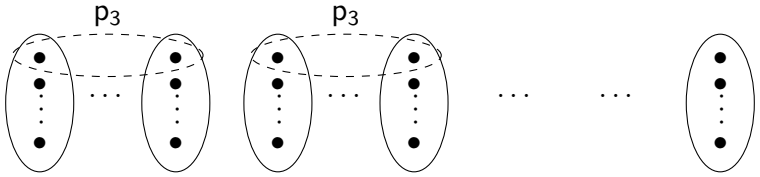
A ideia é mostrar que não é possível decompor $p_1 \cdot p_2$ bolinhas em grupinhos de tamanho p_3.

E para fazer isso, nós construímos o seguinte esquema



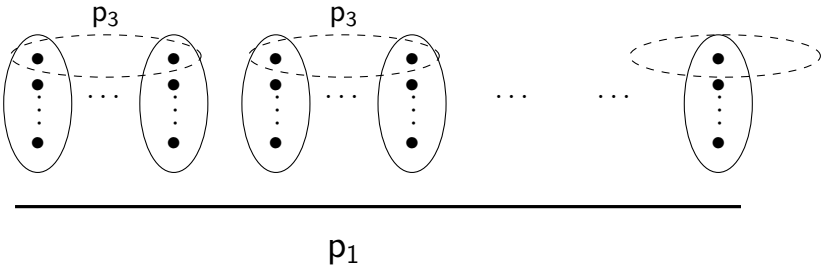
— (*i.e., p_1 grupinhos de tamanho p_2*)

Daí, a gente imagina que vai formando grupinhos de tamanho p_3, da seguinte maneira



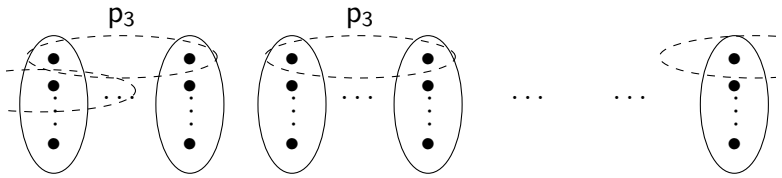
Nesse ponto, a gente faz a primeira observação importante

Fato 1: Quando a gente chega no final da primeira linha, não existem pontinhos suficientes para formar um grupinho completo



Ora, isso tem que ser assim, porque p_1 *é um número primo.*

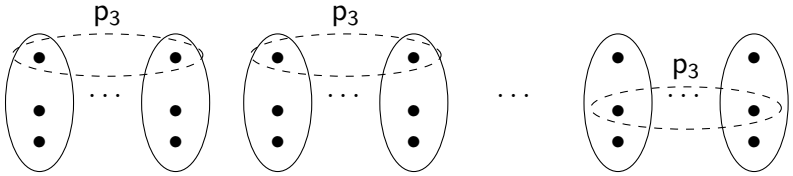
Só que daí, a gente pega pontinhos na próxima linha para completar o grupinho



Certo.

Nesse ponto, a gente faz mais uma observação simples

Fato 2: Mais cedo ou mais tarde, a gente sempre consegue terminar uma linha com um grupinho completo



Bom isso certamente acontece na linha p_3

— (*porque o número total de pontinhos até ali é igual a* $p_1 \cdot p_3$*, o que é um múltiplo de* p_3)

Mas daí, a gente pode pensar se isso não podia ter acontecido antes.

E isso nos leva para a observação mais importante da prova.

Fato 3: Não dá para formar um grupinho completo antes da linha p_3.

Bom, vamos imaginar que dá, só pra ver no que dá ...

Quer dizer, imagine que nós formamos um grupinho completo no final da linha $k < p_3$.

Daí, a gente vai começar do começo outra vez na linha $k + 1$.

E daí, o processo vai entrar em repetição!

Daí que, no final da linha $2k$ nós vamos ter um outro grupinho completo.

E no final da linha $3k$ também.

Quer dizer, os grupinhos completos vão sempre aparecer nas linhas múltiplas de k.

Mas daí, a gente lembra que aparece um grupinho completo no final da linha p_3.

Logo, p_3 é um múltiplo de k.

Só que isso não pode ser, porque p_3 *é um número primo.*

Legal.

Então, p_3 é a primeira linha que termina com um grupinho completo.

Daí, a gente vai começar do começo outra vez na linha $p_3 + 1$.

E daí, o processo vai entrar em repetição!

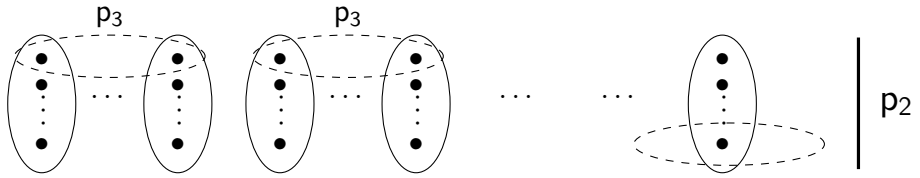
Daí que, no final da linha $2\,p_3$ nós vamos ter um outro grupinho completo.

E no final da linha $3\,p_3$ também.

Quer dizer, os grupinhos completos vão sempre aparecer nas linhas múltiplas de p_3.

E agora está na hora de terminar o argumento.

Fato 4: A última linha do esquema não termina com um grupinho completo



Ora, isso tem que ser assim.

Porque os grupinhos completos aparecem nas linhas múltiplas de p_3.

E p_2 *é um número primo.*

Portanto, $p_1 \cdot p_2$ nunca é divisível por p_3.

E nós sempre temos que

$$p_1 \cdot p_2 \quad \neq \quad p_3 \cdot p_4$$

Legal, não é?

Outro argumento

Outra coisa legal da matemática é que, depois que a gente vê e entende uma coisa, a gente consegue dizer a mesma coisa de forma mais sucinta — (*sem ver o que está acontecendo ...*)

Quer dizer, no final das contas, o que o Fato 3 está dizendo é o seguinte

Teorema: Se p, q são primos, então $p \cdot q$ é o menor múltiplo comum de p e q.

Porque?

Bom, para explicar isso a gente precisa do seguinte

Lema: Se k é o mínimo múltiplo comum de p e q, então todos os múltiplos comuns de p e q tem a forma

$$a \cdot k \qquad \text{, para algum } a \text{ inteiro.}$$

— (*aqui, p, q não precisam ser primos*)

Prova:

Suponha que não.

E imagine que existe um múltiplo comum m que satisfaz

$$\ell \cdot k \quad < \quad m \quad < \quad (\ell + 1) \cdot k$$

Nesse caso, nós podemos escrever

$$m \quad = \quad \ell \cdot k \quad + \quad r$$

onde $r < k$.

Daí, a gente observa o seguinte

- m é um múltiplo de p
- E $\ell \cdot k$ também é um múltiplo de p
- Logo, r é um múltiplo de p

E de maneira análoga

- m é um múltiplo de q
- E $\ell \cdot k$ também é um múltiplo de q
- Logo, r é um múltiplo de q

Portanto, r é um múltiplo comum de p e q.

Só que r é menor do que k.

E isso não pode ser. □

Legal.

Agora nós estamos prontos para provar o teorema.

Prova do teorema:

Suponha que não.

E imagine que $k < p \cdot q$ é um múltiplo comum de p e q.

Então, nós podemos escrever

$$k \quad = \quad b \cdot p$$

E podemos concluir que todos os múltiplos comuns de p e q tem a forma

$$a \cdot b \cdot p \qquad\qquad \text{, para algum } a$$

Ora, $p \cdot q$ é um múltiplo comum de p e q.

Logo, nós devemos ter

$$p \cdot q \quad = \quad a \cdot b \cdot p$$

O que implica

$$q \quad = \quad a \cdot b$$

Só que isso não pode ser — (*porque q é primo ...*) □

Finalmente, agora que temos o teorema, nós podemos provar o seguinte

Corolário: Se p_1, p_2, p_3, p_4 são primos diferentes, então nós sempre temos

$$p_1 \cdot p_2 \quad \neq \quad p_3 \cdot p_4$$

Prova:

Suponha que não.

E imagine que

$$p_1 \cdot p_2 \quad = \quad p_3 \cdot p_4$$

Então, $p_1 \cdot p_2$ é um múltiplo de p_3.

Só que $p_1 \cdot p_2$ também é múltiplo de p_1.

Então, $p_1 \cdot p_2$ é um múltiplo comum de p_1 e p_3.

Logo, ele deve ter a forma

$$a \cdot p_1 \cdot p_3$$

O que implica

$$p_1 \cdot p_2 \quad = \quad a \cdot p_1 \cdot p_3$$

O que implica

$$p_2 \quad = \quad a \cdot p_3$$

Só que isso não pode ser — (*porque* p_2 *é primo ...*) □

Legal, não é?

Generalização

Sim, mas a gente ainda não terminou.

Quer dizer, a gente já sabe que

$$p_1 \cdot p_2 \quad \neq \quad p_3 \cdot p_4$$

Mas alguém poderia encontrar 5 números primos tais que

$$p_1 \cdot p_2 \cdot p_5 \quad = \quad p_3 \cdot p_4$$

Só que isso não pode ser.

Corolário: Se p_1, p_2, p_3, p_4, p_5 são primos diferentes, então nós sempre temos que

$$p_1 \cdot p_2 \cdot p_5 \quad \neq \quad p_3 \cdot p_4$$

Prova:

Suponha que não.

E imagine que

$$p_1 \cdot p_2 \cdot p_5 \quad = \quad p_3 \cdot p_4$$

Então, $p_1 \cdot p_2 \cdot p_5$ é um múltiplo comum de p_3 e p_5.

Logo, ele deve ter a forma

$$a \cdot p_3 \cdot p_5$$

O que implica

$$p_1 \cdot p_2 \cdot p_5 \quad = \quad a \cdot p_3 \cdot p_5$$

O que implica

$$p_1 \cdot p_2 \quad = \quad a \cdot p_3$$

O que implica que $p_1 \cdot p_2$ é divisível por p_3.

Só que isso não pode ser — (*pelo Corolário anterior*) □

Aqui a gente entrou em repetição.

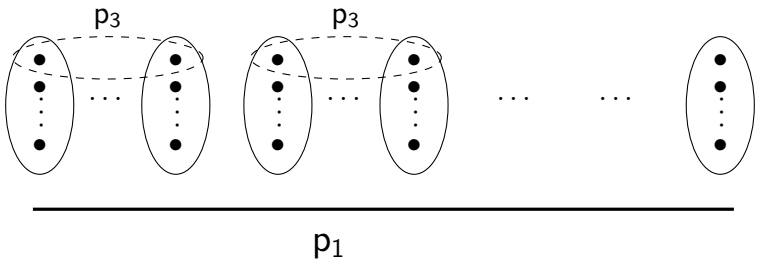
E isso nos permite concluir que

→ *Produtos de primos diferentes sempre dão um resultado diferente.*

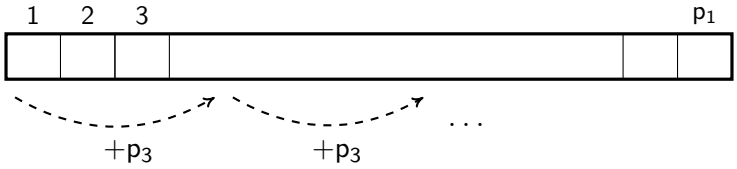
3 Outra propriedade legal dos primos

Certo.

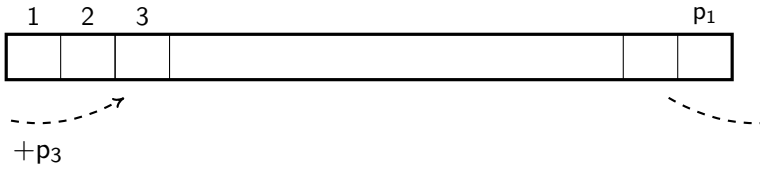
Mas a gente ainda pode tirar uma outra informação legal do nosso esquema



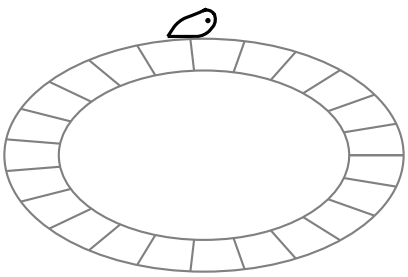
Quer dizer, formar grupinhos de tamanho p_3 nesse esquema é a mesma coisa que dar saltos de tamanho p_3 em uma lista de tamanho p_1



sendo que, na hora em que um salto ultrapassa o final da lista, a gente volta para o começo



E a gente também pode pensar em um sapo que dá voltas em torno de uma pista



Daí, se a gente continua saltando e saltando dessa maneira, alguém poderia perguntar

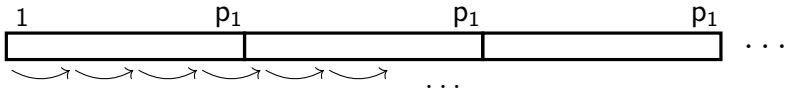
- *Quando é que, pela primeira vez,*

  a gente cai em uma posição onde a gente já passou antes ?

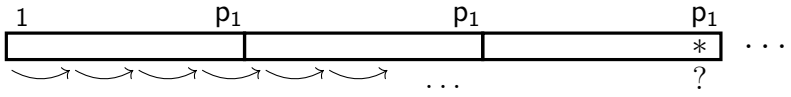
Bom, agora a gente precisa raciocinar.

E para fazer isso, nada melhor do que ver as coisas de um ângulo diferente.

Quer dizer, a gente pode imaginar que o processo salta sempre para frente, sobre uma sequência de cópias da lista



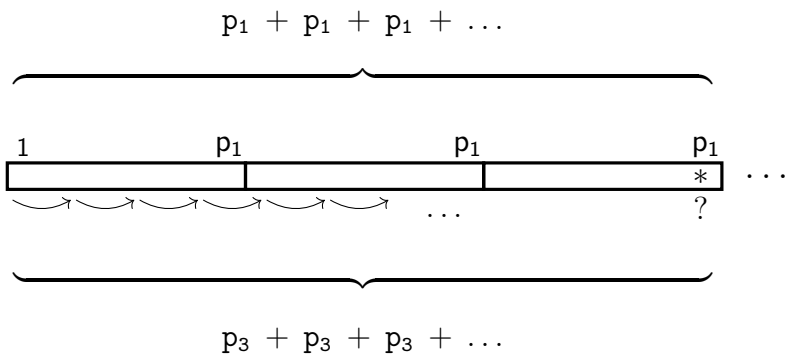
E daí, a gente pode perguntar: *quando é que o processo cai na última posição (p_1) pela primeira vez ?*



Mas isso a gente já sabe responder.

Quer dizer, quando o processo cai em p_1, a distância total que ele percorreu até aquele momento corresponde a

- uma soda de saltos de tamanho p_3
- e também uma soma de listas de tamanho p_1



Em outras palavras, um múltiplo comum de p_1 e p_3.

Ora, mas a gente já sabe que o menor múltiplo comum é $p_1 \cdot p_3$.

Daí que, a primeira visita à posição p_1 acontece após o processo ter percorrido a distância $p_1 \cdot p_3$

E isso corresponde a exatamente p_1 saltos.

Legal.

Agora a gente pode perguntar:

- *Será que alguma posição foi visitada duas vezes antes disso ?*

E a resposta é: claro que não!

Porque se o processo visitasse duas vezes a mesma posição ele entraria em repetição.

E daí, ele nunca iria visitar a posição p_1.

Mas isso não pode ser.

Logo, nenhuma posição é visitada duas vezes nos primeiros p_1 saltos.

Ora, mas a lista possui p_1 posições.

Daí que, nos primeiros p_1 saltos o processo visita todas as posições da lista.

E logo em seguida, saltando a partir da posição p_1 ele cai na posição p_3
— (*que foi onde tudo começou ...*)

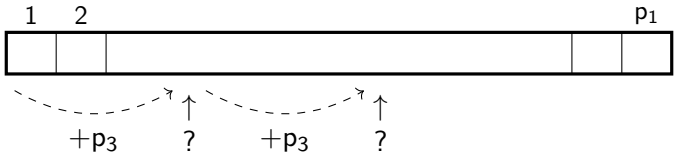
Não é legal?

E isso tem uma consequência ainda mais legal.

Quer dizer, imagine que você tem uma lista de tamanho p_1.

E imagine que você quer saber se o elemento `x` está na lista ou não.

Então, ao invés de percorrer o elemento `x` percorrendo a lista elemento a elemento, a gente pode fazer isso saltando de p_3 em p_3 posições — (*onde p_3 também é primo*)

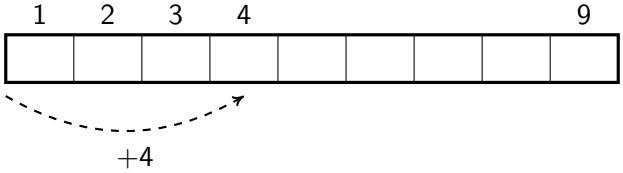


Daí, se você voltar ao lugar onde começou sem ter encontrado o elemento `x`, é porque ele não está lá.

4 Não apenas os primos

Mas, essa propriedade não é uma exclusividade dos números primos.

Por exemplo, imagine que a lista tem tamanho 9 e nós damos saltos de tamanho 4

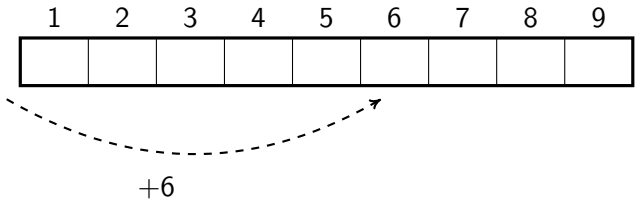


Daí, a sequência de posições por onde a gente passa é

$$4, \quad 8, \quad 3, \quad 7, \quad 2, \quad 6, \quad 1, \quad 5, \quad 9, \quad 4, \quad \ldots$$

Quer dizer, a gente passou por todas as posições outra vez.

Por outro lado, quando a lista tem tamanho 9 e nós damos saltos de tamanho 6



Daí, a sequência de posições por onde a gente passa é

$$6, \quad 3, \quad 9, \quad 6, \quad \ldots$$

Mas, o que está acontecendo aqui?

Bom, o que está acontecendo é que 4 e 9 não possuem nenhum divisor comum
— (*o que é sempre o caso quando a gente considera pares de primos*)

Por outro lado, 6 e 9 possuem um divisor comum: o 3.

Sim, mas e daí?

Bom, daí o seguinte

Fato 1: Quando dois números x e y não possuem divisores comuns, nós temos que

$$\mathsf{MMC}(x, y) \quad = \quad x \cdot y$$

Fato 2: Quando dois números x e y possuem um divisor comum, nós temos que

$$\mathsf{MMC}(x, y) \quad < \quad x \cdot y$$

Daí que, no primeiro caso, o processo só alcança a última posição da lista após 9 saltos
— (*e só entra em repetição depois de ter passado por todas as posições*)

E no segundo caso, o processo só alcança a última posição antes dos 9 saltos
— (*e entra em repetição antes de ter passado por todas as posições*)

Bom, a gente pode raciocinar assim

Argumento 1:

Suponha que x e y não possuem um divisor comum.

E suponha que mesmo assim, nós temos

$$\mathsf{MMC}(x, y) \quad = \quad z \quad < \quad x \cdot y$$

Bom, daí a lista completa de múltiplos comuns de x e y é

$$z, \quad 2 \cdot z, \quad 3 \cdot z, \quad 4 \cdot z, \quad \ldots$$

Mas, $x \cdot y$ é um múltiplo comum de x e y.

Então, $x \cdot y$ aparece nessa lista.

Mas, isso significa que

$$x \cdot y \quad = \quad k \cdot z \qquad \text{, para algum } k$$

Nesse ponto, a gente lembra que z é um múltiplo comum de x e y

$$z \quad = \quad x \cdot \alpha \qquad\qquad z \quad = \quad y \cdot \beta$$

Daí que, a equação acima implica

$$x \cdot y \quad = \quad k \cdot x \cdot \alpha \qquad\qquad x \cdot y \quad = \quad k \cdot y \cdot \beta$$

E isso implica que

$$y \quad = \quad k \cdot \alpha \qquad\qquad x \quad = \quad k \cdot \beta$$

Mas, isso implica que x e y possuem um fator comum.

Só que isso não pode ser.

Logo, nós devemos ter

$$\mathsf{MMC}(x, y) \quad = \quad x \cdot y$$

□

Argumento 2:

Suponha que x e y possuem um fator comum.

Então, nós podemos escrever E isso implica que

$$y \quad = \quad k \cdot \alpha \qquad\qquad x \quad = \quad k \cdot \beta$$

Agora, é bem fácil ver que $k \cdot \alpha \cdot \beta$ é um múltiplo comum de x e y.

Mas, $k \cdot \alpha \cdot \beta \; < \; x \cdot y$.

Logo,

$$\mathsf{MMC}(x, y) \quad < \quad x \cdot y$$

□

5 Raciocinando com primos

Abrindo um livro de Matemática Discreta, a gente encontra a seguinte observação

→ *Se p é um número primo e p divide $a \cdot b$,*
então p divide a ou p divide b — (ou p divide ambos)

Porque?

Bom, suponha que p não divide a.

Então, p e a não possuem divisores comuns — (*porque?*)

Daí que, o menor múltiplo comum de p e a é o produto $p \cdot a$.

Além disso, a lista completa de múltiplos comuns de p e a é

$$pa, \quad 2 \cdot pa, \quad 3 \cdot pa, \quad 4 \cdot pa, \quad \ldots$$

Mas, $a \cdot b$ é um múltiplo comum de p e a — (*porque p divide $a \cdot b$*)

Então, $a \cdot b$ aparece na lista acima.

Mas, isso significa que

$$a \cdot b \quad = \quad k \cdot p \cdot a \qquad \text{, para algum } k.$$

E isso significa que

$$b \quad = \quad k \cdot p$$

Logo, p divide b.

A seguir, nós vamos ver mais exemplos de raciocínios desse tipo.

Exemplos

a. Mais um fato sobre primos

Um pouco mais abaixo, no mesmo livro de Matemática Discreta, a gente encontra a seguinte observação

→ *Se p, q são números primos, e tanto p como q dividem o número a, então o produto $p \cdot q$ também divide a*

Porque?

Bom, a gente já sabe que o menor múltiplo comum de p e q é o produto $p \cdot q$.

Além disso, a lista completa de múltiplos comuns de p e q é

$$pq, \quad 2 \cdot pq, \quad 3 \cdot pq, \quad 4 \cdot pq, \quad \ldots$$

Mas, a é um múltiplo comum de p e q — (*porque p divide a, e q divide a*)

Então, o número a aparece na lista acima.

Mas, isso significa que

$$a \quad = \quad k \cdot pq \qquad \text{, para algum } k.$$

Logo, $p \cdot q$ divide a.

◇

b. Divisibilidade

Considere a seguinte pergunta

- *Será que o número $n^3 + 5n$ é divisível por 6 ?*

Bom, pelo resultado do exemplo anterior, basta verificar se 2 e 3 dividem o número $n^3 + 5n$.

A primeira observação é que

- se n é par, então n^3 é par e $5n$ também é par
- se n é ímpar, então n^3 é ímpar e $5n$ também é ímpar

Daí, como os dois termos sempre tem a mesma paridade, a sua soma é sempre um número par.

Certo.

Agora, a gente reescreve o número assim

$$n^3 \;+\; 5n \quad = \quad n \cdot \left(n^2 + 5\right)$$

Daí, a gente observa que se n é múltiplo de 3, então isso é um múltiplo de 3.

Mas, n pode ter a forma $3k \pm 1$.

Nesse caso, a gente observa que

- $(3k+1)^2 \quad = \quad 9k^2 + 6k + 1$
- $(3k-1)^2 \quad = \quad 9k^2 - 6k + 1$

Quer dizer, em ambos os casos, o resto da divisão por 3 é igual a 1.

Mas, isso significa que $n^2 + 5$ deixa resto 6 — (*o que é o mesmo que o resto 0*)

Logo, o número é divisível por 3 nesses dois casos também.

◇

c. Mais divisibilidade

Considere a seguinte pergunta

- *Será que o número $n^5 - n$ é divisível por 30 ?*

Bom, aqui basta verificar que o número é divisível por 2, 3 e 5.

Para isso, a gente começa reescrevendo

$$\begin{aligned} n^5 \;-\; n \quad &= \quad n \cdot \left(n^4 - 1\right) \\ &= \quad n \cdot \left(n^2 + 1\right) \cdot \left(n^2 - 1\right) \\ &= \quad n \cdot \left(n^2 + 1\right) \cdot \left(n + 1\right) \cdot \left(n - 1\right) \end{aligned}$$

Aqui, a gente já pode observar que

- existem dois fatores que são números consecutivos,
  logo, um deles é par, e portanto o número é divisível por 2
- existem três fatores que são números consecutivos,
  logo, um deles é múltiplo de 3, e portanto o número é divisível por 3

Agora, a gente vai examinar a divisibilidade por 5.

A primeira observação fácil é que

- se n tem a forma $5k$, ou a forma $5k \pm 1$

  então o número é divisível por 5 — (*porque?*)

Mas, n pode ter a forma $5k \pm 2$.

Nesse caso, a gente observa que

- $(5k+2)^2 = 25k^2 + 10k + 4$
- $(5k-2)^2 = 25k^2 - 10k + 4$

Quer dizer, em ambos os casos, o resto da divisão por 5 é igual a 4.

Mas, isso significa que $n^2 + 1$ deixa resto 5 — (*o que é o mesmo que o resto 0*)

Logo, o número é divisível por 5 nesses dois casos também.

◇

d. Entendendo a regra do 7

Lembre da seguinte regra do 7 que nós vimos na aula 04

→ Multiplique o último dígito do número por 2

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

Porque?

Bom, considere um número qualquer e faça a decomposição

$$N = \underbrace{\mathtt{d_n} \ldots \mathtt{d_2}\,\mathtt{d_1}}_{K} \Big| \mathtt{d_0}$$

Então,

$$N = 10 \cdot K + \mathtt{d_0}$$

Agora, multiplique os dois lados por 2

$$2N = 20 \cdot K + 2 \cdot \mathtt{d_0}$$

A ideia é que se $2N$ é divisível por 7, então N também é — (*porque?*)

Certo.

O próximo passo é uma pequena esperteza.

Quer dizer, a gente reescreve o número assim

$$2N = 21 \cdot K + 2 \cdot \mathtt{d_0} - \mathtt{K}$$

Agora, é fácil ver que o lado direito é divisível por 7 se isso aqui também for

$$2 \cdot \mathtt{d_0} - \mathtt{K}$$

E isso é divisível por 7 se isso aqui também for

$$K \quad - \quad 2 \cdot \mathtt{d}_0$$

Mas, é exatamente isso o que a regra do 7 está dizendo ...

$\diamond$