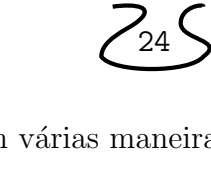


Unicidade da fatoraão em primos

Mas, o mais legal   que s  existe uma maneira de decompor um n mero em fatores primos.

S  que isso n o   assim t o f cil de se ver.

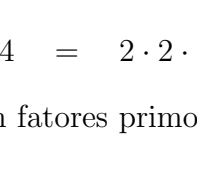
Por exemplo, imagine que voc  coloca o 24 dentro do primeiro saquinho



Da , quando voc  tira ele do outro lado, existem v rias maneiras de escrever o 24 como um produto

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

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



Quer dizer

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

  a  nica maneira de decompor o n mero 24 em fatores primos.

Mas, *porque isso?*

Bom, porque os primos tem uma propriedade legal.

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

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

Mas, *como   que a gente v  isso?*

Bom, na pr tica a gente mostra que o produto de dois primos

$$p_1 \cdot p_2$$

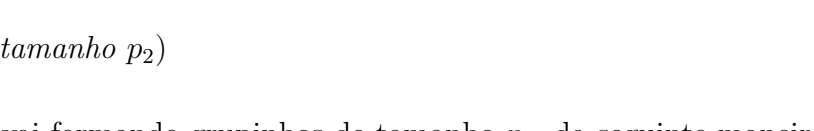
nunca   divis vel por um terceiro primo p_3 — (*e isso j  implica a desigualdade acima*)

Vejamos como   isso.

Argumento

A ideia   mostrar que n o   poss vel decompor $p_1 \cdot p_2$ bolinhas em grupinhos de tamanho p_3 .

E para fazer isso, n s constr mos o seguinte esquema



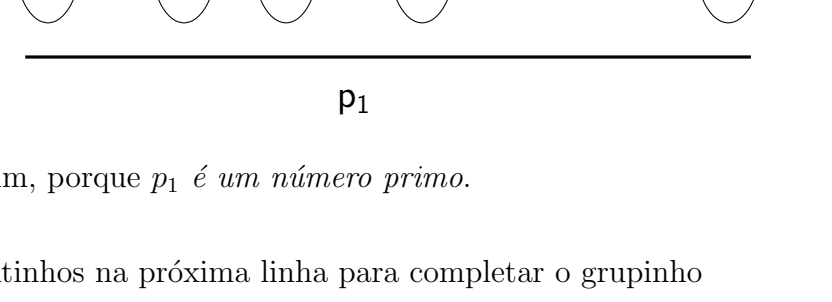
— (*i.e., p_1 grupinhos de tamanho p_2*)

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



Nesse ponto, a gente faz a primeira observa o importante

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



Ora, isso tem que ser assim, porque p_1   um n mero primo.

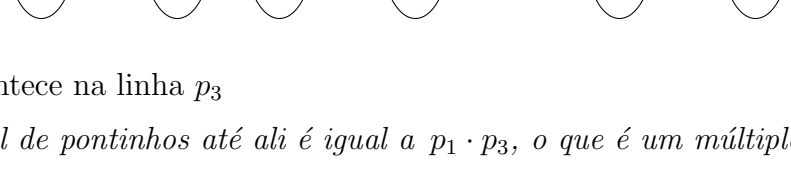
S  que da , a gente pega pontinhos na pr xima linha para completar o grupinho



Certo.

Nesse ponto, a gente faz mais uma observa o 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 n mero total de pontinhos at  ali   igual a $p_1 \cdot p_3$, o que   um m ltiplo de p_3*)

Mas da , a gente pode pensar se isso n o podia ter acontecido antes.

E isso nos leva para a observa o mais importante da prova.

Fato 3: N o d  para formar um grupinho completo antes da linha p_3 .

Bom, vamos imaginar que d , s  pra ver no que d  ...

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

Da , a gente vai come r do come o outra vez na linha $k + 1$.

E da , o processo vai entrar em repeti o!

Da  que, no final da linha $2k$ n s vamos ter um outro grupinho completo.

E no final da linha $3k$ tamb m.

Quer dizer, os grupinhos completos v o sempre aparecer nas linhas m ltiplas de k .

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

Logo, p_3   um m ltiplo de k .

S  que isso n o pode ser, porque p_3   um n mero primo.

Legal.

Ent o, p_3   a primeira linha que termina com um grupinho completo.

Da , a gente vai come r do come o outra vez na linha $p_3 + 1$.

E da , o processo vai entrar em repeti o!

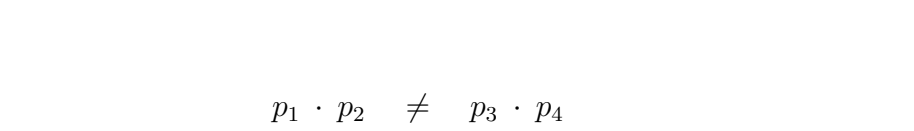
Da  que, no final da linha $2p_3$ n s vamos ter um outro grupinho completo.

E no final da linha $3p_3$ tamb m.

Quer dizer, os grupinhos completos v o sempre aparecer nas linhas m ltiplas de p_3 .

E agora est  na hora de terminar o argumento.

Fato 4: A  ltima linha do esquema n o termina com um grupinho completo



Ora, isso tem que ser assim.

Porque os grupinhos completos aparecem nas linhas m ltiplas de p_3 .

E p_2   um n mero primo.

Portanto, $p_1 \cdot p_2$ nunca   divis vel por p_3 .

E n s sempre temos que

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

Legal, *n o  ?*

Outro argumento

Outra coisa legal da matem tica   que, depois que a gente v  e entende uma coisa, a gente consegue dizer a mesma coisa de forma mais sucinta — (*sem ver o que est  acontecendo ...*)

Quer dizer, no final das contas, o que o Fato 3 est  dizendo   o seguinte

Teorema: Se p, q s o primos, ent o $p \cdot q$   o menor m ltiplo comum de p e q .

Porque?

Bom, para explicar isso a gente precisa do seguinte

Lema: Se k   o m nimo m ltiplo comum de p e q , ent o todos os m ltiplos comuns de p e q tem a forma

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

— (*aqui, p, q n o precisam ser primos*)

Prova:

Suponha que n o.

E imagine que existe um m ltiplo comum m que satisfaz

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

Nesse caso, n s podemos escrever

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

onde $r < k$.

Da , a gente observa o seguinte

- m   um m ltiplo de p
- E $\ell \cdot k$ tamb m   um m ltiplo de p
- Logo, r   um m ltiplo de p

E de maneira an loga

- m   um m ltiplo de q
- E $\ell \cdot k$ tamb m   um m ltiplo de q
- Logo, r   um m ltiplo de q

Portanto, r   um m ltiplo comum de p e q .

S  que r   menor do que k .

E isso n o pode ser. □

Legal.

Agora n s estamos prontos para provar o teorema.

Prova do teorema:

Suponha que n o.

E imagine que $k < p \cdot q$   um m ltiplo comum de p e q .

Ent o, n s podemos escrever

$$k = b \cdot p$$

E podemos concluir que todos os m ltiplos comuns de p e q tem a forma

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

Ora, $p \cdot q$   um m ltiplo comum de p e q .

Logo, n s devemos ter

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

O que implica

$$q = a \cdot b$$

S  que isso n o pode ser — (*porque q   primo ...*) □

Finalmente, agora que temos o teorema, n s podemos provar o seguinte

Corol rio: Se p_1, p_2, p_3, p_4 s o primos diferentes, ent o n s sempre temos

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

Prova:

Suponha que n o.

E imagine que

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

Ent o, $p_1 \cdot p_2$   um m ltiplo de p_3 .

S  que $p_1 \cdot p_2$ tamb m   m ltiplo de p_1 .

Ent o, $p_1 \cdot p_2$   um m ltiplo comum de p_1 e p_3 .

Logo, ele deve ter a forma

$$a \cdot p_1 \cdot p_3$$

O que implica

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

O que implica

$$p_2 = a \cdot p_3$$

S  que isso n o pode ser — (*porque p_2   primo ...*) □

Legal, *n o  ?*

Generaliza o

Sim, mas a gente ainda n o terminou.

Quer dizer, a gente j  sabe que

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

Mas algu m poderia encontrar 5 n meros primos tais que

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

S  que isso n o pode ser.

Corol rio: Se p_1, p_2, p_3, p_4, p_5 s o primos diferentes, ent o n s sempre temos que

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

Prova:

Suponha que n o.

E imagine que

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

Ent o, $p_1 \cdot p_2 \cdot p_5$   um m ltiplo comum de p_3 e p_5 .

Logo, ele deve ter a forma

$$a \cdot p_3 \cdot p_5$$

O que implica

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

O que implica

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

O que implica que $p_1 \cdot p_2$   divis vel por p_3 .

S  que isso n o pode ser — (*pelo Corol rio anterior*) □

Aqui a gente entrou em repeti o.

E isso nos permite concluir que

→ *Produtos de primos diferentes sempre d o um resultado diferente.*