

# O algoritmo de Euclides

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 ...*)

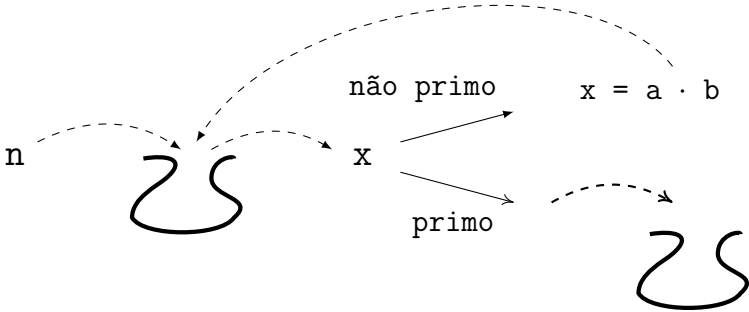
Certo.

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

$$n = p_1 \cdot p_2 \cdot \dots \cdot p_k$$

*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

$$x = a \cdot b$$

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?*