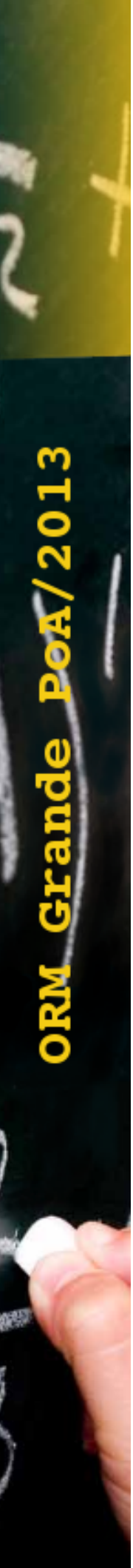


3.

NÚMEROS PRIMOS

O conhecimento dos números primos e da decomposição dos números compostos como produto de primos estão entre os conhecimentos mais úteis e importantes da Aritmética.

K. F. Gauss – *Estudos de Aritmética*, c. 1800

1).– Conceito de número primo

Nestas notas, trataremos da ideia de número primo apenas no contexto dos *números inteiros naturais*: 0, 1, 2, 3, 4, . . . ; note que o zero é número natural. Em cursos avançados essa ideia é estendida para números inteiros de sinal qualquer, para polinômios, e até mesmo para outros objetos matemáticos.

Os **números primos** são os números naturais com *exatamente* dois divisores.

Número	divisores	quantidade de divisores	primo?
0	~~0~~, 1, 2, 3, 4,...	infinitos	não
1	1	1	não
2	1, 2	2	sim
3	1, 3	2	sim
4	1, 2, 4	3	não
5	1, 5	2	sim
6	1, 2, 3, 6	4	não

Note que n ser primo não é o mesmo que ter apenas n e 1 como divisores. Com efeito, se assim fosse, como n=1 tem apenas n e 1 como divisores (iguais), *concluiríamos errôneamente* que n=1 é primo, apesar de ele ter apenas um divisor. A definição correta de número primo proibe que 1 seja primo! Essa proibição foi feita por razões de conveniência que adiante explicitaremos.

- ✔ 0 não é primo, pois tem infinitos divisores;
- ✔ 1 não é primo, pois tem apenas um divisor: 1, ele mesmo;
- ✔ 2 é primo; ele é o menor primo e o único primo que é número par;
- ✔ reciprocamente, o fato de um número ser ímpar não garante que ele seja primo; com efeito, como 9 tem três divisores (1, 3 e 9), segue que 9 não é primo.

Teorema – (uma caracterização dos não primos)
Os inteiros naturais que não são primos são os seguintes:

- *o número 0*
- *o número 1*
- *e os números naturais $n \geqslant 2$ que **têm fatoração não trivial**; ou seja, que podem ser fatorados como $n = a \times b$, onde tanto a como b são distintos de n e 1.*

Prova:
No terceiro caso, basta mostrar que um tal n tem no mínimo 3 divisores. Sabemos que a e b são divisores, mas não podemos afirmar que eles são distintos, de modo que precisamos achar mais outros dois. Ora, 1 e n são esses outros dois, pois $n \neq 1$ e tanto a como b são $\neq 1, n$.

Teorema – (uma caracterização dos primos)
*Os números primos são os inteiros naturais $n \geqslant 2$ que **só admitem a fatoração trivial** $n = 1 \times n$.*

É importante notar que esse teorema ficaria falso se incluísse o caso $n = 1$, pois $1 = 1 \times 1$ é a única maneira de fatorarmos 1.

Um conceito associado
Os números naturais $n \geqslant 2$ que têm fatoração não trivial são denominados números compostos.

Pelo primeiro teorema acima, o conjunto dos números naturais que *não são primos* é o conjunto formado do 0, 1 e dos números compostos. Dizendo isso de outro modo:

> o conjunto de todos os números inteiros naturais é o conjunto formado pelo 0, o 1, os números compostos e os números primos.

- ✔ a lista dos primos inicia com: 2, 3, 5, 7, 11, 13, 17, 19, etc.
- ✔ a lista dos compostos inicia com: 4, 6, 8, 9, 10, 12, 14, 15, etc.
- ✔ 0 e 1 não são primos e nem compostos.

Cuidado: "não primo"≠ "composto"; também observe que existem compostos ímpares.

(Recomendamos evitar o uso da expresão composto, pois há confusão nos livros. Obviamente, a fonte dessa confusão está no fato de 0 e 1 serem números naturais, e não serem nem primos e nem compostos. Alguns autores excluem o zero dos naturais, mas mesmo assim é preciso estar sempre lembrando que 1 não é primo e nem composto.)

Exercício 1 –
Explique por que cada definição abaixo está errada.

a). primos são os números que somente são divisíveis por sí e a unidade.

b). são os números que somente podem ser divididos por sí e pela unidade sem que deixem resto.

c). são os números que somente podem ser reconstruídos pela adição de unidades, e não pela multiplicação.

d). são os números que não são o produto de números.

e). compostos são os números (exceto a unidade) que não são primos.

f). o famoso astrônomo Carl Sagan, em seu livro e filme Contato, tem os extraterrestes transmitindo a sequência dos 261 primeiros primos, a qual inicia com 1, 2, 3, 5, 7, ...

g). primos são os números naturais que têm dois divisores.

h). primos são os números naturais que têm apenas fatoração trivial.

i). primo é todo natural n cujos únicos divisores são 1 e n.

Exercício 2 –
A seguinte caracterização dos números primos está correta?
"Um número natural é primo se nunca for possível escrevê-lo como o produto de dois naturais, ambos menores do que ele."
(resp.:)

Moral:
permitir zero ser número natural e proibir um ser primo exigem muito cuidado.

2).- Números primos e "talvez primos"famosos

✔ **Números de Fermat:** $F_n = 1 + 2^{(2^n)}$, $n = 0, 1, 2, 3,$ etc.
a lista destes números inicia com 3, 5, 17, 257, 65 537, 4 294 967 297, etc. Fermat provou facilmente que F_0, F_1, F_2, F_3, F_4 são primos, e conjecturou que o mesmo ocorre para os demais F_n. Como esses números crescem muito rapidamente, é difícil decidir sua primalidade. Apesar disso, Euler mostrou que a conjectura de Fermat é falsa, pois $F_5 = 4\,294\,967\,297 = 641 \times 6\,000\,417$.

✔ **Números de Mersenne:** $M_n = 2^n - 1$, $n = 2, 3, 4,$ etc.
os primeiros números de Mersennes são: 3, 7, 15, 31, 63, 127, 255, etc.; conforme vemos, nem todos eles são primos (15 é não primo); prova-se que para M_n ser primo é obrigatório que n seja primo, embora essa condição não seja uma garantia da primalidade; com efeito, $M_{11} = 2047 = 23 \times 89$.

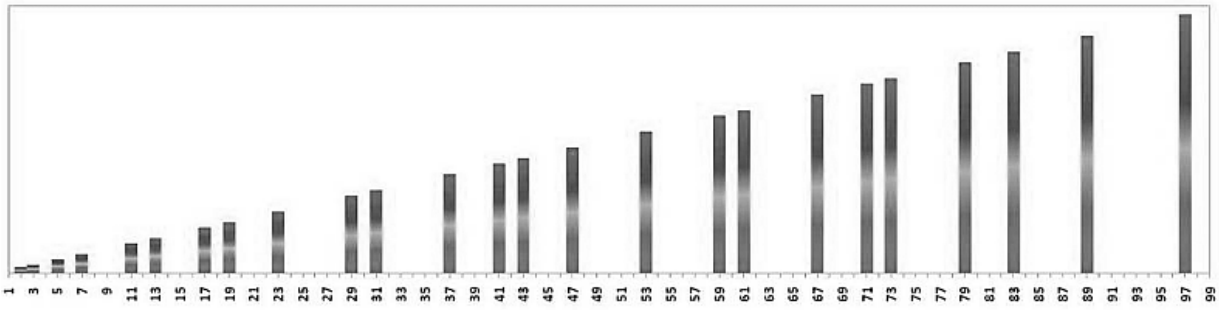
- ✔ **Números perfeitos:**
  número perfeito é todo natural da forma "um + (a soma de todos os seus divisores *primos*)".
  Exemplo: 6 é perfeito, pois 6 = 1 + 2 +3; por outro lado, 4 ≠ 1+2 não é perfeito. Não se conhece nenhum número perfeito ímpar: 3 ≠ 1+3, 5 ≠ 1+5, 7 ≠ 1+7, 9 ≠ 1+3, etc.

- ✔ **Números de gêmeos:**
  Números gêmeos são quaisquer dois *primos* da forma p, p+2.
  Exemplos de primos gêmeos: 3 e 5, 5 e 7, 11 e 13; note que 7 e 9 não são gêmeos, pois 9 nem é primo. Se conjectura que existem infinitos primos gêmeos.

3).- Importância dos números primos

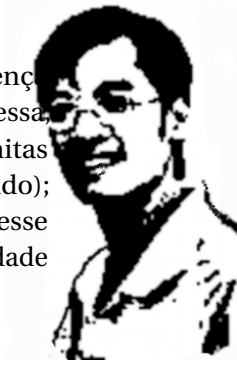
A ideia de número primo é das mais simples, mas também das mais ricas em resultados e aplicações, tanto na própria Matemática como nas Ciências e Tecnologia. A principal razão de sua enorme importância reside no fato de que eles *funcionam como uma espécie de tijolos* com os quais podemos construir, por meio de multiplicação, qualquer outro número natural (exceto os casos triviais n=0 e n=1). Quem nos garante isso é o *Teorema Fundamental da Aritmética*, que adiante estudaremos.

Outra razão da importância dos números primos está na enorme quantidade de problemas difíceis que facilmente podemos formular com eles. Por exemplo, um fato que prontamente nos chama a atenção é a irregularidade da distribuição desses números. Para ter uma ideia, observe a figura abaixo que mostra todos os primos entre 2 e 100.



Conforme sugere a figura, a medida que vão crescendo, os primos tornam-se cada vez mais raros. A partir de Gauss, muitos matemáticos tentaram caracterizar a raridade e o espaçamento dos primos. Se conseguiu demonstrar que, para para qualquer comprimento que se possa imaginar, existe um intervalo com tal comprimento e no qual não existe *nenhum* número primo!

Por outro lado, observe que a figura acima mostra vários primos cuja diferença vale 2, por exemplo: 5-3=2, 7-5=2, 13-11=2, 19-17=2, etc.; esses são pares de números gêmeos. Isso nos sugere um outro problema: *quantos são os pares de primos gêmeos*? Pois bem, apesar de esse ser um problema de simples formulação, ainda se desconhece sua resposta. Usando recursos computacionais poderosos, já se verificou que de 2 a 1 000 000 000 000 000 há 1 177 209 242 304 pares de gêmeos, e se conjectura que existam infinitos deles.



Ainda nessa linha de pensamento, observe a sequência 3, 13, 23: todos são primos e têm diferença sucessiva igual a 10. Sequências (possivelmente finitas) com diferenças sucessivas iguais, como essa, são ditas *progressões aritméticas de primos*. Só em 2004 se conseguiu mostrar que existem infinitas progressões de números primos. O autor da proeza foi o matemático Terence Tao (foto ao lado); ele ganhou a Medalha Fields (o "Prêmio Nobel" na Matemática) não apenas por ter resolvido esse problema, como porque as técnicas que introduziu para resolvê-lo têm se mostrado de grande utilidade em outros problemas.

Mesmo um problema matemático de formulação bem simples e elementar pode requerer a introdução de métodos sofisticados e de grande utilidade em outras áreas da Matemática. É exatamente isso que faz a grandeza de um problema.

4).- Resultados auxiliares de uso frequente

Lema –

a). Se $1 \leqslant a \leqslant b \leqslant n$ *verificam* $n = a \cdot b$, *então* $a \leqslant \sqrt{n} \leqslant b$.
b). Se $n \geqslant 2$ *não for primo, então existem a e b tais que* $n = a \cdot b$ *e* $2 \leqslant a \leqslant \sqrt{n} \leqslant b < n$.

Prova.
a). Como $1 \leqslant a \leqslant b$, temos apenas as seguintes possibilidades para o valor de $\sqrt{n}$: ou $a \leqslant b < \sqrt{n}$, ou $\sqrt{n} < a \leqslant b$, ou $a \leqslant \sqrt{n} \leqslant b$. Se demonstrarmos que as duas primeiras possibilidades não podem ocorrer, obrigatoriamente terá de valer a terceira. Essa demonstração será feita por contradição.
– Se valesse $a \leqslant b < \sqrt{n}$, teríamos $n = ab \leqslant bb < \sqrt{n}\sqrt{n} = n$, ou seja: teríamos $n < n$, um absurdo.
– Se valesse $\sqrt{n} < a \leqslant b$, também teríamos um absurdo: $n = \sqrt{n}\sqrt{n} < a\sqrt{n} \leqslant ab = n$.

b). É uma consequência do item anterior.

Teorema 1 –
Para cada número natural $n \geqslant 2$, *é verdade que*

- *n tem ao menos um divisor primo;*
- *e se n não for primo, podemos garantir mais: ele tem um divisor primo p verificando* $p \leqslant \sqrt{n}$.

Prova.
a). Se o próprio n for primo, o tal divisor é n mesmo; se n não for primo, a definição de primo nos garante que n tem um divisor entre 1 e n; seja p o menor deles. Afirmo que tal p é o divisor procurado, pois é divisor de n e é primo. Comprovo que p é primo por contradição. Com efeito, se p não fosse primo, ele teria um divisor d verificando $1 < d < p$, de modo que tal d seria um divisor de n (por quê?) e menor do que o menor deles: um absurdo!
b). Para um tal n, vale o item (b) do Lema e, pela primeira parte do presente teorema, podemos escolher um divisor primo, p, para o a do Lema; este divisor verifica $p \leqslant \sqrt{n}$.

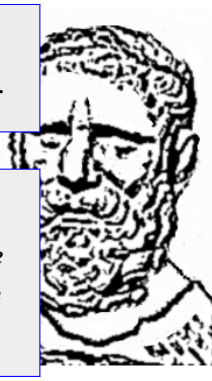
5).- Como verificar se um número dado é primo?

Para isso, existem vários procedimentos sistemáticos (ou seja: algoritmos) que podem ser executados com caneta e papel, ou com computador. Esses procedimentos são denominados *testes de primalidade*. Existem dois tipos deles.

– Testes de primalidade para números pequenos

O mais simples deles é baseado na seguinte consequência do teorema anterior:

Teorema de Eratóstenes –
Dado $n \geqslant 2$ inteiro, para garantir que n é primo basta mostrar que nenhum primo $\leqslant \sqrt{n}$ divide n.



Algoritmo da Divisão de Eratóstenes –
Para decidir a primalidade de um número $n \geqslant 2$ dividimos n pelos primos de 2 até somente $\sqrt{n}$, e vamos verificando se a divisão é exata ou não. Se uma *delas for exata, o número n não é primo;* se nenhuma *delas for exata, n é primo.*

Exemplo:
seja decidir a primalidade de 109 (ou seja, verificar se 109 é primo ou não), usando Eratóstenes.
Basta testar os primos cujo quadrado é menor do que 109, o que equivale a dizer que basta testar todos os primos de 2 até $\sqrt{109} \simeq 10.4$, os quais são 2, 3, 5 e 7. Ora dividindo 109 por cada um desses números vemos que o quociente não é inteiro, logo 109 é primo.

Exemplo:
vamos decidir a primalidade de 33, usando Eratóstenes.
Como $\sqrt{33} \simeq 5.7$, basta testar os primos 2, 3 e 5. Ora, 3 divide 33, logo 33 não é primo.

- ✔ Para decidir a primalidade de um $n \leqslant 100$, basta testar os primos $p \leqslant 7$;
- ✔ Para decidir a primalidade de um $n \leqslant 200$, basta testar os primos $p \leqslant 13$;
- ✔ Para decidir a primalidade de um $n \leqslant 1000$, basta testar os primos $p \leqslant 31$;
- ✔ etc.

Observação: na Escola é muito popular uma *outra* algoritmização do Teorema de Eratóstenes, a qual serve para calcular *todos* os primos entre 2 e n, é o denominado *Crivo de Eratóstenes*. Não o estudaremos, pois é menos eficiente para testar a primalidade de um único número.

– Testes de primalidade para números grandes

O algoritmo de Eratóstenes e assemelhados têm o inconveniente de exigirem muitos cálculos para decidirmos a primalidade de *números grandes*, como os usados em Criptografia. Nesses casos se usa algoritmos mais sofisticados, que fogem do nível introdutório deste texto. O estudo desse tipo de algoritmos é um dos problemas centrais da Teoria Computacional dos Números.

6).– Decomposição em fatores primos

Teorema Fundamental da Aritmética
Para cada número natural $n \geqslant 2$, temos duas alternativas:

- *ou n é primo;*
- *ou n pode ser escrito como o produto de primos*
  (essa escritura pode ser feita de uma única maneira, exceto pela ordem de fatores).

Abreviamos isso dizendo que todo número natural $n \geqslant 2$ pode ser decomposto (fatorado) como um produto de primos (possivelmente repetidos e possivelmente com um único fator), e essa decomposição é única, a menos da escolha da ordem dos fatores.

A escritura de um número natural *n* como um produto de primos é denominada "fatoração em primos de n"ou "decomposição em primos de n" , e expressões parecidas.
Exemplos de decomposição em fatores primos:

$6 = 2 \times 3$, $12 = 2 \times 2 \times 3$, $24 = 2 \times 2 \times 2 \times 3$, $77 = 7 \times 11$, $3 = 3$ (uma fatoração imprópria ou trivial).

Observação importante:
se, na definição de primo, tivéssemos incluído o um, perderíamos a unicidade. Por exemplo:
$6 = 2 \times 3 = 1 \times 2 \times 3 = 1 \times 1 \times 2 \times 3 =$ etc.

Prova do Teorema Fundamental.

- *Existência da fatoração* –
  Basta um exemplo numérico para percebermos a essência do argumento. Seja um não primo, 154, e mostremos que ele é o produto de primos. Como 154 não é primo, ele tem um menor divisor primo (vide Teorema 1), no caso: 2. Podemos fatorar: 154 = 2 x 77. Se 77 fosse primo, teríamos achado a fatoração em primos; como não o é, tomemos o menor divisor primo dele: é 7, de modo que 77 = 7 x 11 e daí 154 = 2 x 7 x 11. Esta é uma fatoração em primos de 154. (Se 11 nào fosse primo buscaríamos seu menor divisor primo, e assim por diante; note, e isto é importante, que os quocientes sucessivos (no caso, 77 e 11) vão diminuindo, de modo que o processo sempre acaba parando num último fator primo, qualquer que seja o n que tenhamos considerado).
- *Unicidade da fatoração* –
  para não nos alongarmos demasiadamente, apesar de sua importância, omitiremos a prova da unicidade, pois é mais difícil.

Procedimento prático para decompor em primos –
Para fatorar em primos um número natural:

- dividimos esse número por seu menor divisor primo;
- fazemos o mesmo com o quociente da divisão acima;
- continuamos até obter um quociente igual à unidade.

Exemplos –
Seja achar a fatoração em primos de 12. Temos 12 = 2 x 6; 6 = 2 x 3, logo 12 = 2 x 2 x 3; 3 = 3 x 1, logo a resposta é 12 = 2 x 2 x 3.
Seja achar a fatoração em primos de 252. Temos, sucessivamente: 252 = 2 x 126, 126 = 2 x 63, 63 = 3 x 21, 21 = 3 x 7, 7 = 7 x 1, de modo que a decomposição em primos procurada é:

$$252 = 2 \times 2 \times 3 \times 3 \times 7 = 2^2 \times 3^2 \times 7\,.$$

Dificuldades computacionais –
Já observamos que é muito laborioso decidir a primalidade de números grandes. Mais trabalhoso ainda é fatorar números grandes. Essa dificuldade é explorada pelos modernos sistemas criptográficos usados em comunicações militares, diplomáticas, bancárias, celulares, etc. Supercomputadores e algoritmos matemáticos cada vez mais sofisticados são usados para se obter tais fatorações, pois com elas pode-se descobrir as chaves desses sistemas. Nesse sentido, são famosos os desafios RSA. Em 2012, Shi Bai e associados "venceram" o RSA-704, que consistiu em fatorar o seguinte número que pode ser escrito com 704 algarismos binários: 74037563479561712828046796097429573142593188889231289084936232638972765034028266276891996419625117843995894330502127585370118968098286733173273108930900552505116877063299072396380786710086096962537934650563796359 . Restam outros desafios, o maior deles é fatorar RSA-2048, um número com 617 dígitos (ou 2048 binários); mais detalhes na Wikipedia – RSA Numbers.

Notação importante –
Usaremos a notação FAT(n) para denotar a fatoração em primos de um número natural n dado. Essa notação não traz ambiguidade, justamente porque n tem exatamente uma fatoração em primos (exceto pela ordem com que escrevemos os fatores). Assim, por exemplo:
FAT$(252) = 2^2 \times 3^2 \times 7$, FAT$(10) = 2 \times 5$, FAT$(1078) = 2 \times 7^2 \times 11$.

Consequência muito útil dessa notação –
Como ab = FAT(a) x FAT(b), temos que

$$\text{FAT}(a \times b) = \text{FAT}(a) \times \text{FAT}(b)$$

(Observe que mostrar que essa fórmula está correta não é imediato! Ela é uma consequência da unicidade garantida pelo Teorema Fundamental. Com efeito, como FAT$(a) \times$ FAT(b) certamente é "uma" fatoração em primos de $a \times b$, pela unicidade da fatoração segue que essa fatoração tem de ser "a" fatoração em primos de $a \times b$.)

Exemplificando, tomando $a = 135$, que tem FAT$(135) = 3^3 \times 5$, temos que

$$\text{FAT}(135^2) = \text{FAT}(135 \times 135) = \text{FAT}(135) \times \text{FAT}(135) = (3^3 \times 5)^2 = 3^6 \times 5^2\,.$$

Para guardar!

- ✔ Decidimos a primalidade de um $n \geqslant 2$ testando sua divisibilidade pelos primos $\leqslant \sqrt{n}$.
- ✔ TFAritm.: todo $n \geqslant 2$ pode ser escrito, e de modo único, como o produto de um ou mais *primos de valor crescente.*

EXERCÍCIOS DIDÁTICOS

Sobre o enunciado do Teorema Fundamental da Aritmética (TFA)

Exercício –
Aponte dois erros ou imprecisões na frase: "Todo número natural diferente da unidade pode ser escrito como um produto de primos, e essa forma é única."
Resp.: e o zero? $6 = 2 \times 3$ e $6 = 3 \times 2$ são a mesma forma?

Exercício –
Julgue se cada um dos itens seguintes reescreve, de modo correto e equivalente, o enunciado do Teorema Fundamental da Aritmética.

1).- É condição suficiente que n seja um número natural para que n possa ser decomposto como um produto de fatores primos, de modo único, a menos da ordem dos fatores.

2).- É condição necessária que n seja um número natural para que ele possa ser decomposto como um produto de fatores primos, de modo único, a menos da ordem dos fatores.

3).- Se n não possuir decomposição como um produto de fatores primos, que seja única, a menos da ordem dos fatores, então n não é um número natural diferente de 1.

4).- Ou n não é um número natural diferente de 1, ou n tem uma decomposição como um produto de fatores primos, que é única, a menos da ordem dos fatores.

5).- Podemos garantir que um número natural é diferente de 1 sempre que ele puder ser decomposto como um produto de fatores primos, de modo único, a menos da ordem dos fatores.

6).- Todo número natural $n \geqslant 2$ pode ser fatorado, e de modo único, por primos escritos em ordem crescente de valores.

Achando a fatoração em primos de um número dado.

Exercício –
Usando o algoritmo de Eratóstenes, achar a fatoração em primos de 1234, 34560 e 111111.
Resp.: $\text{FAT}(1234) = 2 \times 617$, $\text{FAT}(34560) = 28 \times 33 \times 5$, $\text{FAT}(111111) = 3 \times 7 \times 11 \times 13 \times 37$.

PROBLEMAS OLÍMPICOS

Problema –
Decompor 999 999 999 999 em primos.
Resp. Inicie estudando o padrão envolvido em 9999/101, 9999 9999/10001 e aproveite o resultado do exerc. anterior, para concluir que $\text{FAT}(999999999999) = 33 \times 7 \times 11 \times 13 \times 37 \times 101 \times 9901$.

Problema –
Lá por 1550, Tartaglia conjecturou que $1 + 2 + 4$, $1 + 2 + 4 + 8$, $1 + 2 + 4 + 8 + 16$, ... são somas cujos valores são, alternadamente, primos e não primos. Pede-se decidir a veracidade dessa conjectura.