O TEOREMA FUNDAMENTAL DA ARITMÉTICA – NÚMEROS PRIMOS E SUTILEZAS OCULTAS DA ARITMÉTICA

THE FUNDAMENTAL THEOREM OF ARITHMETIC –
PRIME NUMBERS AND HIDDEN SUBTLENESSES OF ARITHMETIC

Rubens Vilhena Fonseca[1]

Andreza Thalia Menezes Monteiro[2]

Richard Campos Vilhena Fonseca[3]

Resumo

Havia um engano muito comum no Ensino Básico em se pensar que a Aritmética era apenas um percurso inicial antes da Álgebra e sendo apenas a parte mais elementar da Matemática. A partir desse erro era comum, a Aritmética ser ensinada nos primeiros anos, enquanto, a Álgebra, apenas a partir de anos posteriores Neste aspecto particular, a BNCC faz indicações que procuram minimizar esse equívoco. A grande maioria das pessoas tem noções da Matemática que elas aprenderam na escola e a ideia sobre a elementaridade da Aritmética acaba tomando raízes profundas levando, em geral, a um desinteresse sobre o assunto. Entretanto, a verdade é que a Aritmética – estudo de propriedades dos números inteiros e de operações sobre eles – é um assunto profundo, difícil, de intensas pesquisas e longe de ser elementar para os matemáticos. É uma parte tão importante devido aos seus impressionantes resultados que, nos meios matemáticos, é considerada a "Rainha da Matemática'. Tópicos avançados de Aritmética pertencem à área conhecida como Teoria dos Números, de modo a distingui-la da aritmética escolar. Mas estas designações não alteram fatos. Tanto a Aritmética escolar quanto a Teoria dos Números pertencem a uma mesma esfera de conhecimento. Neste artigo, queremos mostrar isso. Consideraremos o chamado *Teorema Fundamental da Aritmética* (TFA) ou *Teorema da Fatoração Única em Primos* (TFUP). É um teorema muito usado na escola básica e possui uma rica história que deve ser conhecida para que se possa avaliar, com precisão, fatos e sutilezas aritméticas envolvidas na fatoração em primos que não percebemos e como esse importante teorema requer uma prova cuidadosa e detalhada que possa ser apresentada na escola básica.

Palavras-chave: Aritmética. Teoria dos Números. Teorema Fundamental da Aritmética. Fatoração em primos.

[1] Doutor em Educação Matemática pela Pontifícia Universidade Católica de São Paulo.
Professor da Universidade do Estado do Pará (UEPA). E-mail: rubens.vilhena@uepa.br

[2] Licenciada em Matemática pela Universidade do Estado do Pará (UEPA).
E-mail: andrezathaliamm@gmail.com

[3] Licenciando em Física (UCA). Bacharelando em Física (UFPA). E-mail: richardfonseca207@gmail.com

Abstract

There was a very common misconception in Basic Education in thinking that Arithmetic was just a starting point before Algebra, and that it was just the most elementary part of Mathematics. From this error it was common for Arithmetic to be taught in the early years, while Algebra was only taught in later years. Fortunately, BNCC makes indications that seek to correct this error. Since the vast majority of people know about Mathematics generally what they learned in school, the idea of elementary arithmetic ends up taking deep roots leading to a general lack of interest in the subject. However the truth is that arithmetic, which is the study of the properties of integers, and of operations on them, is a deep, difficult, research-intensive subject, and far from elementary for mathematicians. It is such an important part because of its impressive results that in mathematical circles it is considered the Queen of Mathematics. Advanced topics in Arithmetic are studies in an area known as Number Theory, in order to distinguish it from school arithmetic. But these designations do not alter facts. And the fact. is that both school arithmetic and the theory of numbers belong to the same sphere of knowledge. In this article we want to show that. Therefore, we will consider the so-called Fundamental Theorem of Arithmetic (TFA) or Unique Prime Factorization Theorem (TFUP). It is a widely used theorem in elementary school, but it has a rich history that must be known in order to accurately assess facts and arithmetic subtleties that we don't notice, and how this important theorem requires careful and detailed proof that can be presented in elementary school.

Key words: Arithmetic. Number Theory. Fundamental Theorem of Arithmetic. Factoring in primes.

Introdução

Estamos tão tranquilos com o conjunto dos Inteiros positivos ou Naturais, $\mathbb{N} = \{1, 2, 3, \dots\}$ que nem nos passa pela cabeça fazer a seguinte pergunta: falta algum número no conjunto dos Naturais? A resposta a esta pergunta tem implicações profundas e envolve questões de segurança para grandes empresas e nações.

Pode não parecer óbvio inicialmente, mas $a = (97599759)^{8999}$ e $b = (99999999)^{9999}$ são números naturais com $a < b$. Podemos garantir que, entre a e b, estão todos os naturais que fazem parte desse intervalo mesmo sabendo que não temos condições de verificar? Será possível que entre a e b exista algum número natural que possa ser escrito, pelo menos de dois modos, como um produto de fatores primos?

Veremos que estas questões que intuitivamente aceitamos como verdadeiras, estão sustentadas sobre a definição de número primo, operações de adição e multiplicação e um teorema considerado fundamental que são a própria razão da existência da Aritmética como a conhecemos em ℕ.

Os mistérios da fatoração única

O teorema, o qual, neste artigo, pode ser chamado de *Teorema da Fatoração Única em Primos* (TFUP) – também conhecido como *Teorema Fundamental da Aritmética* (TFA) – diz, precisamente, que dado qualquer número natural $n > 1$, há apenas um conjunto de de primos cujo produto é n.

Johann Carl Friedrich Gauss (1777-1855) foi o primeiro a apresentar uma prova completa em 1801. Vários matemáticos tinham feito trabalhos bastante profundos em Teoria dos Números antes de Gauss e, provavelmente, não tinham notado que muitos de seus resultados e procedimentos dependiam do TFA para sua validade.

Vamos apresentar um cenário no qual o TFA possa se destacar como um resultado muito sutil. O objetivo é motivar educadores matemáticos a refletir nos detalhes da prova que iremos apresentar de modo a terem a convicção de que o esforço vale a pena.

Primeiro de tudo, definir um *número primo p* como um número natural maior que 1, que possui exatamente apenas os dois fatores triviais: 1 e o p. Assim, estamos classificando os números em ℕ em três subconjuntos mutuamente exclusivos, em uma classe própria; os primos; e os chamados números compostos.

Em seguida, passamos para uma consequência importante do TFA Suponha que você exija o maior fator comum de dois números (ou maior divisor comum), digamos 10780 e 39102. Um método de fazer isso é fatorar ambos em primos, então, escolher os fatores comuns com a menor potência de cada fatoração, e multiplicá-las todas juntas:

$10780 = 2^2 \times 5 \times 7^2 \times 11$

e

$39102 = 2 \times 3 \times 7^3 \times 19$,

então, o maior fator comum é $2 \times 7^2 = 98$. Claramente, 98 será um fator comum de ambos, mas, somente, com TFA podemos garantir que é o maior. Pois, se 10780 e 39102 tivessem outras fatorações em primos, ao escolhermos os termos comuns poderíamos ser levados a algo diferente de 2×7^2.

A parte mais interessante, nesta abordagem do TFA, compreende uma análise cuidadosa de outro conjunto de números que chamaremos de $\mathcal{L}$, onde iremos considerar, no que diz respeito às ideias fatoração em primos, semelhante a $\mathbb{N}$, mas, no qual o TFA não se mantém em $\mathcal{L}$. Vamos considerar que $\mathcal{L}$ é o conjunto definido como

$$\mathcal{L} = \{4n - 3; n \in \mathbb{N}\} = \{1,5,9,13,17,21,25,29,33,37,41,45,49,53,57,61,65,69,73,77, \dots\}$$

Como podemos ver, $\mathcal{L}$ é um subconjunto de $\mathbb{N}$.

$\mathcal{L}$ tem a propriedade de ser fechado para multiplicação. Sejam $4s - 3$ e $4t - 3$ elementos de $\mathcal{L}$, então $(4s - 3) \times (4t - 3) = 4k - 3 \in \mathcal{L}$. Isso significa que podemos dar a classificação em três subconjuntos de $\mathcal{L}$ assim como fizemos com $\mathbb{N}$ com o $\{1\}$, os primos e os compostos. As três classes, neste caso, são $\{1\}$, aqueles em $\mathcal{L}$ que têm apenas os dois fatores (apenas os divisores 1 e o próprio número de $\mathcal{L}$), e os compostos. Vamos chamar os da segunda classe de $\mathcal{L}$-primos.

$$\mathcal{L} - primos = \{5,9,13,17,21,29,33,37,41,49,53,57,61,69,73,77, \dots\}$$

Claramente, qualquer elemento em $\mathcal{L}$ que é um primo em $\mathbb{N}$ é, necessariamente, um $\mathcal{L}$ −primo (por exemplo, o 13), mas há membros de

$\mathcal{L}$ como o 21 que é um $\mathcal{L}$−primo, mas não é um primo em $\mathbb{N}$. Observe que os únicos divisores de 21 em $\mathcal{L}$ são 1 e o próprio 21.

Agora, considera o número 1617, que está em $\mathcal{L}$ (1617 = 4×405 – 3). Fatorando 1617 em $\mathcal{L} - primos$, temos

1617= 33×49

e

1617 = 77×21,

onde 33, 49, 77 e 21 são todos $\mathcal{L} - primos$. Então, temos um caso de um sistema que não satisfaz o *Teorema da Fatoração Única em Primos.*

Observe que uma consequência indireta da falta de unicidade da fatoração em primos em $\mathcal{L}$ é perceber que faltam elementos no conjunto considerado. Assim, o fato que o TFA garante, e nos passa despercebido, é que no conjunto dos $\mathbb{N}$ não falta nenhum número.

Será que 1617 é apenas uma exceção? Infelizmente não é. Se você considerar primos ímpares *a, b, c,* em $\mathbb{N}$, pode mostrar que *ab*, c^2, *ac* e *bc* estão em $\mathcal{L}$ e observar que $ab \times c^2 = ac \times bc$. Mas, isso não é muito estranho? Afinal, $\mathcal{L} \subset \mathbb{N}$, então, não seria de esperar que eles tivessem as mesmas as propriedades? Tais questionamentos levam a necessidade de se aprofundar e perguntar exatamente quais diferenças entre $\mathcal{L}\, e\, \mathbb{N}$ são significativas do ponto do TFA. Foi como resultado dessa inquietação que os matemáticos perceberam que o TFA em $\mathbb{N}$ é um resultado surpreendente.

Veja que se a unicidade da fatoração em primos não fosse garantida, não podíamos dizer que o conjunto dos inteiros positivos estava completo. Pois, “novos números” podiam ser apenas combinações de mesmos fatores que já estavam em outros números. E o fato de os números primos serem infinitos, só iria nos fazer supor que deviam existir muitos números repetidos com outros fatores primos.

Antes de apresentamos uma demonstração que os professores da escola básica possam apresentar em sala, se faz necessário um passeio histórico resumido e informal sobre os principais trabalhos e pessoas por trás dessa outra grande aventura no campo da Aritmética, chamada por Gauss de *a rainha da Matemática.*

Um breve percurso histórico sobre a descoberta do Teorema Fundamental da Aritmética

O conceito de fatoração única se estende de volta à aritmética grega e, ainda assim, desempenha um papel importante na teoria moderna dos números. Basicamente, a fatoração única consiste em duas propriedades: existência e unicidade. Existência significa que um elemento está representado como um produto finito e irredutível e, unicidade, significa que esta representação é única em certo sentido. A Fatoração única apareceu pela primeira vez como uma propriedade dos números naturais. Esta propriedade é conhecida hoje como o *Teorema Fundamental da Aritmética* (TFA).

A história da TFA é estranhamente obscura. O TFA diz que "*qualquer número natural maior do que 1 pode ser representado como um produto de números primos de maneira única*".

O TFA não aparece nos *Elementos* de Euclides (BICUDO, 2010). No entanto, Euclides desempenhou um papel significativo na história do TFA. Especificamente, os Livros VII e IX contêm proposições que estão relacionados com o TFA.

Em seu livro, al-Farisi (RASHED, 1982) prova a existência da decomposição em primos e, posteriormente, mostra tudo o que é necessário para provar a sua unicidade. Sua Proposição 9 determina todos os divisores de um número dado a partir da fatoração em primos. Um resultado semelhante pode ser encontrado em Prestet, no livro *Nouveaux Elemens de Mathematiques* (1689) (GOLDSTEIN, 1992).

Podemos mencionar Euler. Em seu livro, *Elements of Algebra* (1770), Euler assumiu a existência do FTA e enunciou um resultado similar ao de al-Farisi e Prestet para encontrar todos os divisores. Mais tarde, Legendre provou parte do TFA em seu livro *Theorie des nombres* (1798) e assumiu a unicidade ao listar os fatores de um número dado, mas ele não afirmou explicitamente o TFA. O primeiro a declarar explicitamente e provar o TFA parece ter sido Gauss em seu *Disquisitiones Arithmeticae* (1801). Depois de Gauss, muitos matemáticos deram diferentes provas ao TFA em seus trabalhos (AGARGUN; FLETCHER, 1997).

Euclides e o TFA

Figura 1 – Euclides de Alexandria

Fonte: https://pt.wikipedia.org/wiki/Euclides#/media/Ficheiro:Euklid-von-Alexandria_1.jpg

Euclides foi um matemático grego que viveu em Alexandria, no Egito, durante aproximadamente entre 323-283 a.C., no reinado de Ptolomeu. Sua obra, *Os Elementos*, é composta de 13 volumes (BICUDO, 2010). Os Livros aritméticos são de VII a IX e contêm os resultados básicos da teoria dos números. Embora o TFA não apareça nos *Elementos,* existem duas proposições muito significativas, VII.30 e VII.31, que têm uma estreita conexão com ele. Há uma terceira proposição, IX.14, que é um teorema de unicidade. De fato, o TFA decorre das proposições VII.30 e VII.31.

> VII.30. Se dois números, multiplicados entre si originam algum número, e qualquer número primo mede o produto, então também mede um dos números iniciais [ou seja, se um número primo *c* mede *ab, então, c* vai medir *a* ou *b,* onde "medida" pode ser traduzida como "divisão", embora subtração repetida estaria mais perto do espírito da palavra grega].
>
> VII.31. Qualquer número composto é medido por algum número primo.

Facilmente, obtemos a existência (qualquer número natural maior que 1 pode ser representado como um produto de números primos) por VII.31, e a unicidade (ou seja, esta representação é única) por VII.30. Atualmente, muitos matemáticos provariam o TFA usando essas proposições. Para a unicidade supomos $p_1 \ldots p_n = q_1 \ldots q_m$ são duas decomposições em primos de qualquer inteiro positivo dado. Então, a partir da VII.30 temos $p_1 | q_1$ logo $p_1 = q_1$. Temos o mesmo para todos p's e q's e, assim, segue-se que $n = m$. No entanto, Euclides não especificou o TFA seguindo as proposições acima no Livro VII.

No livro IX, encontramos a Proposição 14: "Se um número é o menor que é medido por números primos, então ele não é medido por nenhum outro primo exceto aqueles que o mediam desde o princípio."

Há muitas semelhanças entre o TFA e IX.14. A Proposição IX.14 é um tipo de teorema de unicidade. É uma boa demonstração parcial da condição da unicidade do TFA, mas, é claro que IX.14 não abrange o caso dos números que possuem um fator quadrático. Por essa razão alguns autores, como Hendy (1975) e Mullin (1965), examinaram a IX.14 e afirmaram corretamente que os dois resultados (IX.14 e o TFA) não são tecnicamente equivalentes.

Além disso, temos de constatar que, sem uma implicação da existência de uma decomposição em primos, a IX.14 começa com uma coleção de números primos, enquanto o TFA começa com um inteiro. Os pontos de partida dos dois teoremas são completamente diferentes.

Os livros, comumente, consideram o TFA como um teorema fundamental. Começam com a definição de números primos e provam a unicidade da fatoração em primos. Isto é seguido pelas propriedades dos números inteiros relativamente primos e o máximo divisor comum. Esta abordagem parece ter se originado com Gauss.

Na Teoria dos Números de Euclides, as coisas são organizadas apenas na ordem inversa. Euclides começa com o algoritmo divisão para encontrar o máximo divisor comum dos números inteiros e, então, ele obtém uma definição operativa dos inteiros relativamente primos. A partir da investigação de ser relativamente primos, ele, finalmente, encontra resultados em números primos, incluindo, em particular, a importante Proposição VII.30 e, então, estabelece a Proposição VII.31 (como apresentado anteriormente) na ordem inversa novamente.

Na teoria de Euclides, o TFA perderia muito do seu significado. Longe de ser essencial, a IX.14 é colocada no fim da teoria aritmética de Euclides. Não se faz uso dessas proposições tanto quanto VII.30 e VII.36. Ela não pode ser considerada o ponto culminante de qualquer parte importante da teoria, nem é utilizada em qualquer resultado subsequente.

Al-Farisi e o TFA

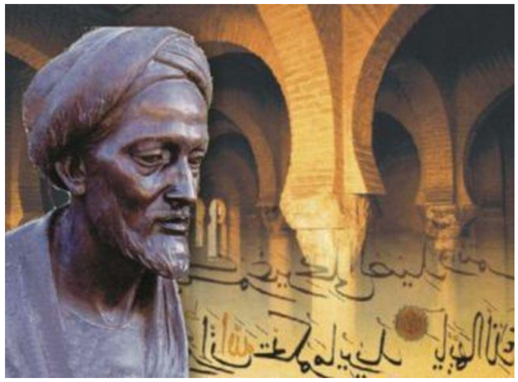


Figura 2 – Al-Farisi
Fonte: https://www.timetoast.com/

Kamal al-Din al-Farisi (1267- 1320) foi um importante matemático persa, físico, e astrônomo. Sua obra representa talvez o passo mais significativo para o TFA dado por um matemático antes de Gauss. Seus resultados aparecem no *Tadhkirat al-Ahbab fibayan altahabb* (Memorando para os amigos explicando a prova dos amigáveis). Sua principal investigação era sobre os números amigáveis[4], e seu objetivo era provar por um método diferente um teorema de Thabit Ibn Qurra (836 – 901) (RASHED; MORELON, 1996, p. 76) que afirmava: "se três números $p = 3.\ 2^{n-1} - 1$, $q = 3.\ 2^{n-1}$ e $r = 9.\ 2^{2n-1}$ são primos, e se p e q são ímpares, então o par $2^n pq$ e $2^n r$ são amigáveis" (HOGENDIJK, 1985).

Thabit Ibn Qurra tinha trabalhado apenas superficialmente na decomposição de inteiros e métodos combinatórios. Al-Farisi foi levado a desenvolver novas ideias na teoria de números, e investigou a decomposição de números inteiros mais profundamente do que Ibn Qura o fez, antes que ele pudesse introduzir métodos combinatórios nos quais era necessário considerar a existência da fatoração de um número inteiro em números primos e usar a propriedade da unicidade determinar os divisores.

[4] Números amigáveis são pares de números naturais onde um é igual à soma dos divisores do outro.

Agargun e Fletcher (1994) traduziram para o inglês nove de suas primeiras proposições com comentários sobre os métodos da Al-Farisi. O principal objetivo dessas nove proposições é conhecer e encontrar os divisores de um número e, portanto, é uma preparação para o trabalho com os números amigáveis.

Pode-se dizer que Euclides deu o primeiro passo no caminho para a existência da fatoração em primos e al-Farisi dá o passo final, na verdade, provando a existência de uma fatoração em primos em sua primeira proposição (RASHED, 2001, p.288)

> Proposição 1. Cada número composto pode ser decomposto em um número finito de produto de fatores primos.

Suponha que $a > 1$ é um número inteiro composto. Portanto, a partir de Euclides VII.31 possui um divisor primo b. Então, para $1 < c < a$,

$$a = bc.$$

Se c é primo, então, a proposição está provada; caso contrário, c possui um divisor primo d e, para $1 < e < c$, escrevemos

$$c = de.$$

Se e é primo, então a proposição esta provada, uma vez que $a = bde$. Caso contrário, repetimos o processo um número finito de vezes e, até o último fator se decompor num produto de dois fatores primos, uma vez que um número finito não pode ter um produto infinito de números. Então, escrevemos até o primo k

$$a = b.d.\mathrm{e}\cdots k$$

Essa proposição é a primeira declaração conhecida e provada da existência de uma fatoração em primos de um número composto. Depois de al-Farisi, Prestet não o citou, mas o usou para determinar todos os divisores de um inteiro dado. Euler declarou e o usou o para encontrar divisores. Legendre afirmou e provou-o (GOLDSTEIN, 1992, p. 184).

As Proposições de 2 até 5 de Al-Farisi 2-5 são os seguintes:

> PROPOSIÇÃO 2. Quando três números a, b, c, são dados, a razão do primeiro para o terceiro é constituído a partir da razão do primeiro para o segundo e da razão da segunda para o terceiro.
>
> PROPOSIÇÃO 3. A razão de 1 para qualquer número de composto é constituída pela sua razão a cada um dos seus fatores primos.
>
> PROPOSIÇÃO 4. Quaisquer dois números compostos que têm a mesma decomposição em fatores primos, são idênticos.
>
> PROPOSIÇÃO 5. Quaisquer dois números compostos distintos, não têm a mesma decomposição em fatores primos.

Após Proposição 5, al-Farisi deu o primeiro passo para determinar todos os divisores de um inteiro. Ele não considerou o próprio inteiro como um divisor. Assim como Prestet e Euler, o principal ponto de partida foi a decomposição em fatores primos.

> PROPOSIÇÃO 6. Se um número composto a é decomposto em números primos b, c, d, e, ..., k, dois a dois bc, bd, be, ..., etc., três a três bcd, bce, ..., etc., e assim por diante, então todos esses são divisores de a.

Então al-Farisi provou Proposição 7, que ele usou para provar a Proposição 8.

> PROPOSIÇÃO 7. Se a não divide b, então para $n = 3, 4, \ldots$, a^2 não divide ba e na não divide ba; a^3 não divide ba^2 e a^{n+1} não divide ba^2; a^4 não divide ba^3 e a^{n+2} não divide ba^3 e assim por diante.

A Proposição 8 é utilizada na proposição seguinte.

> PROPOSIÇÃO 8. Se um número composto a é decomposto em seus fatores primos, digamos $a = bcd \cdots k$, e um deles, digamos b, não se repita na fatoração de a, então b^2 não divide a e para $n = 3, 4, \ldots$, b^n não divide a. E se b repete uma única vez, então b^2 divide a, mas b^n não divide a. E se repete apenas duas vezes, então b^2 e b^3 dividem a, mas b^{n+1} não divide a.

Para determinar todos os divisores de um inteiro composto dado, al-Farisi provou a Proposição 9. Nesta proposição observa-se que todas as proposições anteriores são utilizadas diretamente ou indiretamente. Há um resultado semelhante em Prestet e em Euler, mas é claro que a Proposição 9 foi apresentada muito antes e, tanto quanto sabemos, este é o primeiro resultado conhecido para determinar tudo os divisores de um número composto (AGARGUN; FLETCHER, 1994, p.170). Uma vez mais, o principal ponto de partida foi a decomposição em fatores primos.

> PROPOSIÇÃO 9. Se um número composto, *a,* é decomposto em seus fatores primos tal como $a = bcdh \cdots kl$, então os únicos divisores de a são 1, *b, c, d, h, ..., k,* l, e dois a dois *bc, bd*, ..., etc., e três a três *bcd, bch*, ..., etc., ..., e os produtos de todos os fatores, exceto: $cdh \cdots kl, bdh \cdots kl, ..., bcdh \cdots k$.

Obviamente 1, *b, c, d, ..., k, l* são divisores de *a.* Os outros são imediatamente divisores a partir da Proposição 6. Suponha que a tem um outro divisor z que é primo ou composto. Se z é um primo, então vamos considerar a como $b(c.d.h \cdots l)$ e $z|\, b\ (cd \cdots l)$ implica $z|\, cdh \cdots l$ a partir de Euclides VII.30.

Da mesma forma $z|\, c(dh \cdots l)$ implica $z|\, dh \cdots l$. Portanto, pelo mesmo processo temos $z|\, kl$. Assim $z|\, k$ ou $z|\, l$ e isto implica $z = k$ ou $z = l$. Isso é uma contradição. Suponhamos, agora, que z é um número composto e é distinto daqueles divisores anteriormente já indicados. Portanto, a partir Proposição 5, existe um entre os fatores primos de z que não aparece entre os fatores de a, ou se este fator não existe, então há um fator de z que não se repete o mesmo número de vezes em z e a. Assim, temos três possibilidades:

(i) z tem um fator primo que não aparece entre os fatores de a, ou se z não tem esse fator, então,

(ii) um fator de z tem mais repetições do que nos fatores de a, ou

(iii) um fator de a se repete mais do que nos fatores de z.

Se for o primeiro caso e h é um número primo distinto de todos os fatores de a, então temos uma contradição a partir do caso anterior, em que z é assumido como sendo um número primo.

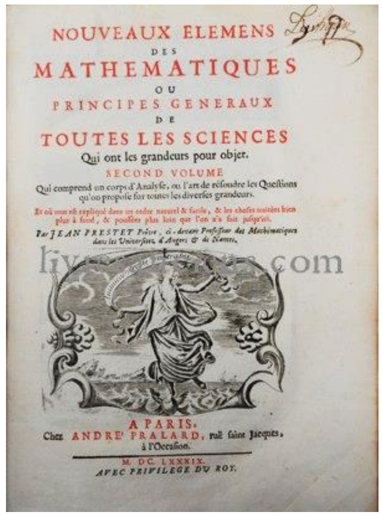
Se é o segundo, há um fator em z, digamos p, que se repete n vezes em z, mas inferior n vezes em a, então $p^{n+1} | z$ e $p^{n+1} | a$ o que é impossível a partir da Proposição 8.

Se é o terceiro, isto é, todos os fatores de z não se repetem mais vezes do que nos fatores *de* a então, z torna-se um divisor de a, o que tinha sido mencionado, e esta é uma contradição.

Vemos que a Al-Farisi fez um avanço importante para a TFA, embora ele não o tenha estabelecido. Ele afirmou e comprovou em parte a existência do TFA, mas ele não o declara e não tinha a intenção de provar a unicidade da fatoração em primos, uma vez que TFA não era importante para ele. Isso não quer dizer que ele não sabia sobre a unicidade. Se al-Farisi tinha a intenção de estabelecer e provar a unicidade, ele teria sido capaz de fazer.

Al-Farisi sabia muito bem sobre a unicidade, como pode ser visto na declaração e prova da sua Proposição 9. Na verdade, ele provou Proposição 9, a fim de determinar todos os divisores de um número composto e ela é usada para dar uma nova prova do teorema de ibn Qurra sobre números amigáveis. No entanto, ele mostrou tudo o que é necessário para provar a unicidade. Portanto, podemos considerar a Proposição 9 como sendo equivalente a parte da unicidade do TFA.

Jean Prestet e o TFA



NOUVEAUX ELEMENS
DES
MATHEMATIQUES
OU
PRINCIPES GENERAUX
DE
TOUTES LES SCIENCES
Qui ont les grandeurs pour objet.
SECOND VOLUME

A PARIS,
Chez ANDRE' PRALARD, ruë saint Jacques, à l'Occasion.
M. DC. LXXXIX.
AVEC PRIVILEGE DU ROY.

Figura 3 – Folha de rosto da obra Nouveaux Elemens des Mathematiques (1689)
Fonte: https://www.livresanciens.com/livres/prestet-nouveaux-elemens-des-mathematiques-principes-generaux-1689-2325

Jean Prestet (1648-1690) foi um sacerdote e matemático francês que contribuiu para os campos de combinatória e da Teoria dos Números. Apresentaremos alguns resultados publicados por Jean Prestet em 1689 no livro *Nouveaux Elemens de Mathematiques,* de acordo com as pesquisas feitas por Goldstein (1992). Eles confirmam que, antes dos tempos modernos, uma fatoração em primos não foi encarada como algo de interesse em si mesmo, mas como um meio de encontrar divisores.

Prestet não afirmou a existência e nem a unicidade do TFA. Ele foi influenciado por Euclides e estava interessado nos divisores. Como al-Farisi e Euler ele deu os principais resultados a fim de encontrar todos os divisores de um determinado número. Em particular, o seu Corolário IX tem um papel significativo. Esse resultado nos faz acreditar que Prestet sabia sobre o TFA. E é possível acreditar que ele poderia prová-lo, mas não estava preocupado com isso (GOLDSTEIN, 1992, p. 179).

No capítulo 6 do seu primeiro volume, encontramos o seguinte teorema (Ibid., 1996, p. 177):

> TEOREMA. Se dois números b e c são relativamente primos, seu produto bc é o menor número que cada deles pode dividir exatamente e sem resto.

Como corolário desse teorema Prestet estabeleceu:

> COROLÁRIO. Se *d* mede exatamente um produto *bc* de dois números *b* e *c* e se *c* e *d* são relativamente primos; o número *d* é um divisor do outro número *b*.

O objetivo dos próximos corolários era determinar todos os divisores de um número expresso como um produto de fatores primos.

> COROLÁRIO IV. Se dois números diferentes *a* e *b* são simples (primos), cada divisor do seu plano, ou produto *ab*, é 1, ou *a*, ou *b*, ou *ab*.

Prestet continuou com os Corolários V e VI, usando o mesmo argumento para um produto de três números primos diferentes *(sólido)* e de quatro números primos *(supersólido),* em seguida, cinco e, assim, indefinidamente.

No seguinte corolário, ele estudou as potências de alguns números primos.

> COROLÁRIO III. Se o número a é simples, cada divisor do seu quadrado a^2 é um dos três 1, *a*, *aa*. E todos os divisores do seu cubo a^3 é um dos quatro 1, *a*, a^2, a^3(...). E assim com os outros infinitamente.

Por fim, ele estabeleceu o corolário:

> COROLÁRIO IX. Se os número *a* e *b* são simples, cada divisor (de) aab dos três, *a, a, b* é um dos três 1, *a*, *aa* ou um dos diferentes produtos desses três por *b*; isto é, um dos seis 1, *a, aa, b, ab, aab*. Porque todas as possibilidades de planos (a multiplica-

ção dos diferentes fatores dois a dois obtidos) dos simples a, *a, b* são *aa* e *ab*. (Argumentos análogos para *aabb; aabbb;* aab^3cc*;* aab^3ccd*).* E assim com os outros.

É claro que Prestet não declara o TFA em seu trabalho, porque seu objetivo era fazer explícita relação entre qualquer fatoração de um dado número em primos e todos os seus possíveis divisores. No entanto, os resultados de Prestet estão muito perto do TFA, e no sentido de implicando um com o outro seu Corolário IX Corolário pode ser considerada como equivalente à unicidade da fatoração em primos.

Euler e o TFA

Figura 4 – Leonhard Euler
Fonte: https://pt.wikipedia.org/wiki/Leonhard_Euler#/media/Ficheiro:Leonhard_Euler_2.jpg

Em seu livro, *Elements of Algebra* (1765), Leonhard Paul Euler (1707-1783) estabelece uma parte do TFA sem prová-lo propriamente e também apresentou uma afirmação para a parte da unicidade análoga à Proposição 9 de al-Farisi 9 e ao Corolário IX de Prestet.

Na Parte I da Seção I do Capítulo IV e parágrafo 41, Euler afirmou a existência da fatoração em primos (EULER, 2011, p.11) e forneceu uma prova parcial. Mas sua prova omite alguns detalhes:

> 41. Todos os números de compostos podem ser representados por fatores, resultando a partir dos números primos acima mencionados; ou seja, todos os seus fatores são números primos. Para se encontrar um fator que não é um número primo, pode sempre ser decomposto e representado por dois ou mais números primos. Quando temos representado, por exemplo, o número 30 por 5 × 6, é evidente que 6 não ser um número primo, mas sendo produzido por 2 × 3, poderíamos ter representado 30 por 5 × 2 × 3, ou por 2 × 3 × 5; quer dizer, por fatores que são todos os números primos.

No parágrafo 43, por exemplo, Euler deu um método para encontrar a decomposição de qualquer número em seus fatores primos:

> 43. É fácil de encontrar um método para a análise um número qualquer, ou resolvendo-o nos seus fatores simples. Digamos que seja proposto, por exemplo, o número 360; vamos representá-lo pela primeira vez por 2 ×180. Agora 180 igual a 2 × 90, e 90 é o mesmo que 2 × 45, e 45 é o mesmo que 3 × 15 e, por último, 15 é o mesmo que 3 × *5*, de modo que o número 360 pode ser representado pelos fatores simples 2 × 2 × 2 × 3 × 3 × 5, uma vez que todos estes números multiplicados juntos produzem 360.

Euler não indicou a unicidade da fatoração em números primos, mas ele deu uma declaração relacionada, sem provas, no Parágrafo 65 do Cap. VI da Seção 1 da Parte 1 (EULER, 2011, p.18).

> 65. Quando, portanto, conseguimos representar qualquer número, por seus fatores simples, fica mais fácil exibir todos os números pelos quais ele é divisível. Para isso temos, em primeiro lugar, que tomar os fatores simples um a um, e, em seguida, multiplicá-los entre si dois a dois, três a três, quatro a quatro, etc., até que chegamos ao número proposto.

Observamos que Euler só estava interessado em encontrar todos os divisores de um número, ele foi seguindo a tradição de al-Farisi e Prestet. No parágrafo 65, Euler nos diz que todos os divisores de um número são obtidos a partir dos fatores primos que aparecem na representação do número como um produto de números primos e esta é a única maneira de ter todos os divisores do número considerado. Portanto, este pode ser considerado como a unicidade da fatoração em primos. Euler também forneceu um exemplo, no final do Parágrafo 64:

> Segue-se que 60, ou 2 × 2 × 3 × 5, pode ser dividido, não só por esses números simples, mas também por aqueles que são compostos de quaisquer dois deles; isto é, por 4, 6, 10 e 15; e também por aqueles que são compostos de qualquer três dos seus fatores simples; isto é, por 12, 20, 30, e por último, também, por si só, 60. (EULER, 2011, p.18).

Legendre e o TFA

Figura 5 – Adrien-Marie Legendre[5]
Fonte: http://www.numericana.com/answer/record.htm#legendre

Adrien-Marie Legendre (1752-1833) ao se referir aos números compostos, escreveu que,

[5] Essa caricatura de Adrien-Marie Legendre é a única imagem que se tem deste personagem até o presente momento. A litografia de Legendre, normalmente divulgada, é do seu padrinho, o matemático Louis Legendre (1752-1797). O equívoco de se atribuir a Adrien-Marie a imagem que era de Louis foi descrito por Peter Duren em seu artigo *Changing Faces: the mistaken portrait of Legendre*, publicado na revista *Notices of the American Mathematical Society*, em dezembro de 2009. No entanto, no final de 2007, o professor Gerard P. Michon, em seu site, *Numericana*, já anunciava essa polêmica em torno da imagem divulgalda de Adrien-Marie Legendre e indicava a sua utilização inapropriadamente. A caricatura que apresentamos na Figura *5* é do site de Gerard P. Michon, uma reprodução da ilustração encontrada no álbum de "*73 Portraits-Charge Aquarelle's des Membres de I'Institute"*, de Julien-Leopold Boilly, publicado em 1820.

> qualquer número não primo N pode ser representado por um produto de vários números primos α, β, γ, etc., cada elevado a alguma potência, de modo que sempre se pode supor $N = \alpha^m\beta^n\gamma^p$, etc. (LEGENDRE, 2009, p. 5).

Em seguida, sua prova segue-se imediatamente como:

> O método a seguir, a fim de executar essa decomposição, consiste em tentar dividir N por cada um dos números primos 2, 3, 5, 7, 11, etc., começando com o menor. Quando a divisão é bem sucedida com um destes números α, repete-se quantas vezes quanto for possível, por exemplo, m vezes, e chamando o último quociente P, temos $N = \alpha^m P$.
> O número P não pode ser dividido por α, e é inútil tentar dividir P por um número primo menor do que α, se P for divisível por θ, onde θ é inferior a α, é claro que N também seria divisível por θ, o que contraria a hipótese. Devemos, portanto, tentar dividir P por números primos maiores que α; assim obtemos em sucessão $P = \beta^n Q$; $Q = \gamma^p R$, *etc.*, que irá dar origem a $N = \alpha^m\beta^n\gamma^p$, etc.. (Ibidem).

Como vemos por esta prova, para qualquer número dado, sempre temos a mesma decomposição em fatores primos, de acordo com o método de Legendre. É evidente que não se pode supor que ela é equivalente a parte unicidade do TFA. No entanto, uma afirmação relacionada com a unicidade é dada:

> Um número N pode ser expresso na forma $\alpha^m\beta^n\gamma^p$, etc., cada um divisor de N será também de forma $\alpha^u\beta^v\gamma^q$, etc., onde os expoentes u, v, q, etc, não ser maior que m, n, p, etc ....

Neste ponto, a intenção de Legendre é encontrar todos os divisores de um número, e, ao mesmo tempo, a soma desses mesmos divisores. A partir dessa afirmação, se poderia facilmente provar unicidade.

Gauss e o TFA

Figura 6 – Johann Carl Friedrich Gauss
Fonte: https://pt.wikipedia.org/wiki/Carl_Friedrich_Gauss#/media/Ficheiro:Carl_Friedrich_Gauss.jpg

Johann Carl Friedrich Gauss (1777-1855) estabeleceu a unicidade da fatoração em primos para os números inteiros positivos no artigo 16 da Seção II em seu *Disquisitiones Arithmeticae* (GAUSS, 1801, p. 14). A Seção II inicia com o seguinte:

> 13. TEOREMA. O produto de dois números positivos, menores que um primo dado, não pode ser dividido por este número primo. (GAUSS, 1801, p. 13).

Então, Gauss reproduzida o Teorema VII.32 dos *Elementos* de Euclides e sua generalização.

> 14. Se nem *a* nem *b* podem ser divididos por *um* número primo *p,* o produto *ab* também não pode ser dividido por *p.*
>
> 15. Se nenhum dos números *a, b, c, d,* etc. pode ser divididos por um primo *p,* também não se pode dividir o produto *abcd* etc.

E aqui temos o seu artigo 16.

> 16. TEOREMA. Qualquer número composto pode ser resolvido em fatores primos de uma única maneira.

Demonstração. Gauss não comentou nada sobre a existência de provas de parte do TFA. Ele começou sua demonstração afirmando que "É evidente a partir de considerações elementares que qualquer número composto pode ser decomposto em fatores primos, mas é tacitamente suposto e, geralmente sem prova, que esta decomposição não pode ser feita de muitas maneiras diferentes". Em seguida, ele considera um número composto $A = a^{\alpha}b^{\beta}c^{\gamma}$ etc. com *a, b, c,* etc. números primos distintos e mostrou que A não pode ser decomposto em fatores primos de outra forma, que não seja apenas com os primos *a, b, c,* etc., ou que tenha alguns números primos que aparecem na decomposição mais vezes.

Assim, a primeira declaração clara e a prova do TFA parecem ter sido dadas por Gauss na sua *Disquisitiones Arithmeticae.* Desde então, muitas provas diferentes foram publicadas. Agargun e Fletcher (1997) investigam diferentes provas da TFA. A seguir, para finalizar, apresentamos uma demonstração desse teorema acessível a professores da educação básica.

Uma demonstração do TFA

Um esquema para a demonstração:

> Passo 1. Suponha que exista um número natural com mais de uma fatoração em primos (ou seja, o TFA não é verdade), e que k seja o menor número desse tipo.
>
> Passo 2. Deduza a partir disso que um número natural menor que k existe com a mesma propriedade. Isso contradiz claramente a definição de k, portanto não há o menor número natural onde não valha o TFA e, portanto, não há nenhum número natural onde o TFA não seja válido.
> Para ir do passo 1 ao passo 2, precisamos de duas conexões, C_1 e C_2.

São elas:

> C_1: Se k (o número introduzido na etapa 1) tem as fatorações em primos $a_1^{\alpha_1}a_2^{\alpha_2}a_3^{\alpha_3}\ldots$ e $b_1^{\beta_1}b_2^{\beta_2}a_3^{\beta_3}\ldots$, então os conjuntos de primos $(a_1, a_2, a_3,\ldots)$ e $(b_1, b_2, b_3,\ldots)$ são disjuntos.
>
> C_2: Se n é de acordo com TFA e sua fatoração única em primos é $p_1^{r_1}p_2^{r_2}p_3^{r_3}\ldots, p_j^{r_i}$, então n não tem fator primo fora do conjunto $(p_1, p_2, p_3,\ldots,p_j)$[6].

Antes de preencher os detalhes deste esquema, façamos uma análise de C_2 sobre ser um fato muito significativo.

Suponha, por exemplo, $n = 2 \times 5 \times 7^3 \times 53 \times 67$, e que n é de acordo com o TFA.

É possível que um primo diferente de 2, 5, 7, 53 ou 67 possa ser um fator de n, digamos o 13? Não, porque, se fosse, poderíamos, então, fatorar n como 13 vezes algum produto de primos, de modo que a fatoração em primos de n não seria única (começaríamos com um produto contendo 13 e não contendo os mesmos primos da primeira fatoração), nesse sentido, C_2 se torna significativo. E isso se verá claramente em sua importância na prova que apresentaremos.

Para verificar a validade de C_1, se um primo a_i estivesse em ambos os conjuntos (por exemplo, se $a_1 = b_1$), então $a_1.a_2.a_3,\ldots$ e $b_1.b_2.b_3\ldots$, seriam as fatorações diferentes em primos de $\frac{k}{a_1}$, um número menor que k, o que é impossível, porque dissemos que k era o menor número natural com fatorações diferentes em primos, ou seja, onde não valia o TFA.

[6] Para efeito de simplicidade, vamos considerar os primos sem repetição. Isso de modo nenhum interfere na prova. Assim, ao invés de escrever os primos com suas potências α_i, β_i, r_i, etc., vamos apenas escrever as bases, onde i = 1,2,3, ...

A demonstração em detalhes

Podemos escrever os primos na fatoração de k em qualquer ordem, por isso, por conveniência, escrevemos em ordem não-decrescente. Ou seja, $a_1 \leq a_2 \leq a_3 \ldots$ e $b_1 \leq b_2 \leq b_3 \ldots$.

Ambas as listas contêm pelo menos dois termos. Caso contrário, k seria primo e a única fatoração em primos de k seria o próprio k. A partir disso vemos que $k \geq a_1^2$ e $k \geq b_1^2$, e uma vez que por $C_1 a_1^2 \neq b_1^2$, mos $k^2 > a_1^2 b_1^2 \Leftrightarrow k > a_1 b_1$.

Assim, $k - a_1 b_1$ é um número natural menor que k e divisível tanto por a_1 quanto por b_1. Assim, pela propriedade que definiu k como menor valor com fatorações distintas e por C_2, pelo TFA, $k - a_1 b_1$ deve ter fatoração única da forma $a_1 b_1 q_1 q_2 q_3 \ldots$ (ou talvez apenas $a_1 b_1$), onde $q_1, q_2, q_3, \ldots$ são outros primos.

Então,

$$k - a_1 b_1 = a_1 b_1 q_1 q_2 q_3 \ldots$$

$$k = a_1 b_1 + a_1 b_1 q_1 q_2 q_3 \ldots$$

Ou seja,

$$a_1 a_2 a_3 \ldots = a_1 b_1 + a_1 b_1 q_1 q_2 q_3 \ldots$$

Logo,

$$a_2 a_3 \ldots = b_1 + b_1 q_1 q_2 q_3 \ldots$$

$$a_2 a_3 \ldots = b_1 (1 + q_1 q_2 q_3 \ldots)$$

e vemos que b_1 é um fator primo comum do produto de primos $a_2 a_3 \ldots$, portanto, b_1 é igual a um desses primos. Mas, por $C_1, b_1 \notin (a_1, a_2, a_3 \ldots)$, porque os conjuntos $(a_1, a_2, a_3, \ldots)$ e $(b_1, b_2, b_3, \ldots)$ são disjuntos. Essa contradição, veio do fato de considerar $k - a_1 b_1 < k$ como um número que obedece ao TFA. Desse modo, não existe o menor número natural k, para o qual não vale o TFA e, por conseguinte o TFA vale para qualquer inteiro positivo.

Agora podemos identificar uma propriedade de $\mathbb{N}$ que foi necessária nesta prova, mas que não é válida para $\mathcal{L}$. Na prova, foi preciso examinar o número natural $k - a_1 b_1 -$ que é a diferença entre dois números naturais. Se tentássemos usar esta prova em $\mathcal{L}$, teríamos que considerar a diferença entre dois números $\mathcal{L}$, o que não seria um $\mathcal{L} - número$.

Conclusão

A prova do TFA deu respostas a questionamentos fundamentais para a Aritmética no campo dos inteiros positivos. Mas, a história envolvendo esse teorema seguiu caminhos inesperados. A ampliação do estudo do TFA para o campo dos Números Complexos trouxe, para a Matemática, uma nova Aritmética.

Na tentativa de demonstrar o *Último Teorema de Fermat*[7], o matemático alemão Ernst Eduard Kummer (1810-1893) criou o método dos divisores complexos, a que chamou *números complexos ideais*, contribuindo para o desenvolvimento da teoria dos números. As dificuldades que surgiram em seus trabalhos se deviam a não validade do TFA em alguns domínios importantes de números e foram superadas com sucesso pelo próprio Kummer, bem como por outros matemáticos como Richard Dedekind (1831-1916), Ivanovich Zolotarev (1847-1878) e Leopold Kronecker (1823-1891). Assim, a não validade do TFA em outros campos da Matemática fez surgir um novo e vasto ramo, chamado de *Teoria Algébrica dos Números*, que é um fértil campo de pesquisa atualmente.

[7]O Último Teorema de Fermat é um famoso teorema conjecturado pelo francês Pierre de Fermat em 1637. Fermat afirmou que a equação $x^n + y^n = z^n$, não tem solução, se n for um natural maior do que 2 e (x, y, z) naturais.

Referências

AGARGÜN, A.; FLETCHER, C.. Al-Farisi and the Fundamental Theorem of Arithmetic. **Historia Mathematica**, 21, p. 162-173, 1994.

AGARGÜN, A.; FLETCHER, C.. The fundamental theorem of arithmetic dissected. **The Mathematical Gazette**, 81(490), p. 53-57, 1997.

DUREN, P. Changing Faces: the mistaken portrait of Legendre. **Notices of the AMS.** 56 (11), 1440–1443, 1455, 2009

GOLDSTEIN, C. On a seventeenth century version of the fundamental theorem of arithmetic. **Historia Mathematica**, 19, p. 177-187, 1992.

BICUDO, I. **EUCLIDES. Os Elementos**. Tradução de Irineu Bicudo. São Paulo: UNESP, 2009.

BRASIL. **Base Nacional Comum Curricular** (2ª versão). Brasília: MEC, 2016. Disponível em: http://basenacionalcomum.mec.gov.br/historico/ Acesso em: 13 jul. 2021.

EULER, L. **Elements of Algebra**. Translated from the French, with the notes of Bernoulli and the additions of De La Grange. 3 ed., carefully rev. and corr. by John Hewlett, 1822. New York: Springer, 2011.

GAUSS, C. F.; WATERHOUSE, W.; CLARKE. A. **Disquisitiones Arithmeticae (1801)**. New York: Springer, 1986.

HENDY, M. D.. Euclid and the Fundamental Theorem of Arithmetic. **Historia Mathematica**, 2, p. 189-191. 1975.

HOGENDIJK, J. Thabit Ibn Qurra And The Pair Of Amicable Numbers 17296, 18416. **Historia Mathematica**, v.12, i. 3, p. 269-273, aug.1985.

KNORR, W. Problems in the interpretation of greek number theory: Euclid and the 'fundamental theorem of arithmetic'. **Studies in History and Philosophy of Science,** Part A 7 (4), p. 353-368, 1976.

LEGENDRE, A. M. **Essai sur la théorie des nombres (1798)**. Cambridge: University Press. 2009.

MICHÓN, Gerard P. The true face of Adrien-Marie Legendre.
Disponível em: http://www.numericana.com/answer/record.htm#legendre. Acesso em: 12 jul. 2021.

MULLIN, A. A. Mathematico-philosophical remarks on new theorems analogous to the fundamental theorem of arithmetic. **Notre Dame Journal of Formal Logic**. 6(3), p. 218-222, jul.1965.

RASHED, R.; MORELON, R. **Encyclopedia of the History of Arabic Science**. London: Routledge, 1996. v.2.

RASHED, R. **The Development of Arabic Mathematics:** between arithmetic and algebra. Transl. by A. F. W. Armstrong. New York: Springer, 2001.

SHAMEY, R.; KIRCHNER, E.; AMIRSHAHI, S.H. Farisi, Kamal al-Din 1267–1319. *In:* SHAMEY, R.; KUEHNI, R. G. **Pioneers of Color Science**. New York: Springer, 2020.