A aritmética

Praciano-Pereira, Tarcisio *

15 de outubro de 2021
preprints da Sobral Matemática
no. 2021.08
Editor Tarcisio Praciano-Pereira
tarcisio@sobralmatematica.org

Resumo

Inspirei-me num artigo da Mathematics Daily que é um blog hospedado no www.wordpress.com que faz uma afirmação falsa sobre os números primos, sugere que sejam finitos e cita o teorema de Zheng de 2014. Usei um texto clássico de Davenport sobre a aritmética para falar de dois teoremas fundamentais da aritmética, *algoritmo da divisão euclidiana* e da *fatoração dos números naturais* e da infinitude da sequência dos números primos e indução finita.

palavras chave: algoritmo da divisão euclidiana fatoração dos números naturais indução finita, números primos, teorema de Zhang sobre o salto entre primos.

I took inspiration from the blog Mathematics Daily hosted at www.wordpress.com which makes a false statement about prime number suggesting they are finite citing Zhang theorem of 2013. I have use the first chapter of the classic book of Davenport to construct construct a line of though from the *algorithm of Euclidean division* to the *factorization theorem* and *finite induction*.

keywords: algorithm of Euclidean division, factorization theorem, finite induction, prime numbers, Zhang theorem on the gap of prime numbers,

*tarcisio@sobralmatematica.org

1 O desenvolvimento

A minha motivação para este artigo partiu duma publicação do blog *Mathematics Daily* que é um blog hospedado no www.wordpress.com que termina com uma parágrafo errado, "In May 2013, Yitang Zhang published a paper (Link in citation), which proves that the value in between two primes cannot exceed 70 million. This discovery was a breakthrough in the field of number theory as the once assumed infinite series of prime numbers now had a limit. This research has helped mathematicians tremendously along the way."

A afirmação de que os números primos agora têm um limite é errada. O resultado de Yitang Zhang estabelece que existe uma p.a. de razão 70.000.000 que sempre encerra um número primo entre os seus elementos, ou seja, a cada 70.000.000 haverá um novo número primo a partir dum número primo conhecido. Este resultado de Zhang foi em seguida melhorado com o cálculo dum número menor para a razão da p.a.

O resultado de Zhang é muito importante para os que pesquisam novos números primos, pelo menos agora se sabem que basta rodar o programa pelos próximos 70.000.000 de inteiros para encontrar mais um número primo, com sorte, vários.

Neste artigo eu me basei no primeiro capítulo do livro *The Higher Arithmetic* de Davenport para traçar um roteiro entre dois teoremas importantes da *Aritmética* e corrigir o erro do *Mathematics Daily* para quem enviei uma mensagem comentando o erro.

2 O que é a Aritmética

O objeto da *Aritmética* é a descoberta das propriedades gerais dos números naturais $1, 2, 3, \ldots$. Esta é a frase inicial do livro de Davenport, um discípulo e continuador do trabalho de G. Hardy que junto com Littlewood foram os dois pioneiros da Matemática inglesa na área da teoria dos números dentro da qual se encontra a *Aritmética* como pedra fundamental. Numa tradução livre...

Os números naturais se dividem em duas classes, não disjuntas, os *números primos*, que, por definição, somente podem ser divididos por eles mesmos, e portanto não podem ser fatorados, e os demais números naturais.

É um defeito falar em *duas classes*, na verdade o conjunto dos números primos é uma parte do conjunto dos números naturais e não uma *classe* que subentende uma partição do conjunto.

A sequência dos números primos continua sendo, hoje, um dos mais *intrigantes segredos da Matemática*, se conhece muito sobre os números primos e também que há ainda muito o que descobrir sobre eles. Se trata duma sucessão infinita de números naturais, e isto é um dos *teoremas da Aritmética*. Um dos resultados mais recentes sobre os números primos, provado por um matemático chinês que vive na América, *Yitang Zhang* é que há um *salto dos números primos*. Zhang descobriu, [3]

Teorema 1 (salto) *de Zhang dos números primos*

Existe um número muito grande, s_0 *tal que se* p *for um número primo, então há um outro número primo no intervalo* $[p, p+s_0]$. $s_0 < 70.000.000$

em um pouco depois dois outros matemáticos conseguiram melhorar este teorema descobrindo s_1 que substitui s_0, mas a busca prossegue por $s_2 \ldots$

Não apresento a demonstração do *teorema de Zhang* porque não há conheço e é um dos resultados difíceis da *teoria dos números*. Mas não afasto a possibilidade de incluí-la aqui num certo futuro, confira [3].

O resultado de Zhang é uma outra formulação, com objetivo diferente, dum resultado fácil de ser demonstrado, que o conjunto dos números primos é infinito. O que fez Zhang foi estabelecer que existe uma p.a. que encerra os número primos entre os termos da mesma. Como dito anteriormente, agora se

tem certeza de que conhecido um número primo p então há outro no intervalo de inteiros $[p, p + s_0]$ em que s_0 é a razão duma p.a.

3 Dois teorema da Aritmética

Outro exemplo inicial, e dos mais conhecidos, é o *teorema da fatoração* dos números naturais.

Teorema 2 (da) *fatoração dos números naturais*
Todo número natural pode ser fatorado de maneira única num produto de números primos elevados a alguma potência. Esta fatoração é única.

Dem :
Se $n \in \mathbf{N}$ não for primo, então existe um número primo p_1 tal que

$$p_1|n; n = p_1 n_1 + r_1 \tag{1}$$

pelo algoritmo da divisão euclidiana Então

$$p_1, n_1, r_1 < n; p_1|n; n_1|n; r_1 = 0; \tag{2}$$

uma vez que tanto p_1, n_1 dividem n deixando o resto r_1, como, por hipótese n não é primo então $r_1 = 0$. Ou seja, se não for possível encontrar entre os números primos que forem menores que n de maneira que se possa escrever a equação (eq.2) então n é primo e a demonstração termina, porque descobrimos um novo número primo. Então supondo que a (eq.2) seja possível vou passar a verificar se n_1 é primo. Se for está terminada a demonstração com a fatoração expressa na equação (eq.2) porque $r_1 = 0$. Se n_1 não for primo então pode ser fatorado o que vai produzir uma sucessão finita

este é o método da b
números primos.

$$n_1, n_2, \cdots, n_k \tag{3}$$

de fatores primos para n. Como alguns dos números primos nesta sucessão podem ser iguais e foram obtidos em ordem decrescente, então a demonstração finaliza com a expressão

$$n = n_1^{m_1} \cdots n_j^{m_j}; j \leq k; \tag{4}$$

que é fatoração de n num produto de números primos. **q.e.d .**

Observe que para fazer referência ao *primeiro* e mais fundamental dos teoremas da *Aritmética* eu me vi forçado a passar por um teorema mais recente, o *teorema de Zhang*, que garante a infinitude da sequência dos números primos porque ele estabelece a existência duma progressão aritmética que entre cujos termos se encontram **todos os números primos**. É uma forma complicadíssima de provar que a sucessão dos números primos é infinita mas oferece outra vantagem na busca por números primos. O livro de Davenport afirma que a *Aritmética* é a mais pura das partes da Matemática e que praticamente não tem aplicações. É uma *afirmação errada* e lembra o ponto de vista de Hardy, certamente o mentor de Davenport, que dizia algo do tipo "*se eu souber que aquilo que estou estudando tem alguma aplicação, eu mudo imediatamente o rumo dos meus estudos*" mal sabia ele que *teoria dos números*, em particular o estudo dos números primos, seria a parte central da *criptografia* do mais alto interesse para os banqueiros e para o comércio eletrônico. Não esquecendo a vitória contra a Alemanha nazista em que o matemático inglês *Alan Turing* teve papel importante quebrando a criptografia dos nazistas e assim decifrando seus segredos de guerra, aplicações da *pura Aritmética*!

"primeiro", depende do a

Vou tratar na última seção do outro resultado que anunciei da *Aritmética*, a indução finita.

4 A Escola podia sair da Idade Média

A *Aritmética* é apresentada às crianças desde o começo quando a aprendem as quatro operações duas das quais são falhas, a *divisão* e *subtração* e não deveriam ser ensinadas, pelo menos da forma como o são. A *multiplicação*, na *Aritmética*, é uma soma repetida. Quando um dia os professores forem aqueles que organizem a Escola, então poderemos ver a *divisão* adquirir uma melhor funcionalidade e se tornando até divertida com uma compreensão do *algoritmo da divisão euclidiana* que até mesmo permite compreender melhor a *subtração*.

A *adição* tem quatro propriedades.

1. comutatividade, $a+b=b+a$,
2. associatividade, $(a+b)+c=a+(b+c)$, que incrivelmente importante porque é quem permite multiplicar n números e também permite tornar algumas contas mais fáceis.

$$17+14=(10+7)+14=(10+7)+(10+4)=20+(7+4)=20+11; \tag{5}$$

em que também usei a *comutatividade*. E isto poderiam ser jogos para avançar o entediamento das crianças no ensino da Matemática induzindo pelo uso o aprendizado da tabuada e evitando ter que decorá-la de forma abruta.

3. distributividade que permite que a gente conte rapidamente quantos ovos tem nas bandejas no mercado quando estas forem diferentes. Uma bandeja tem na lateral b ovos alinhados em a linhas, e a outra tem c ovos alinhados em a linhas, então

$$a\times(b+c)=ab+ac \tag{6}$$

é a quantidade de ovos nas duas bandejas.

4. o elemento neutro, o 0 da adição e do inverso aditivo que falha no conjunto $\mathbf{N}$

Numa Escola futurista vamos encontrar logo os professores mostrando que estas propriedades podem ser vistas num relógio e em seguida falar do resto na divisão para em seguida mostrar que há uma infinidade de sistemas aritméticos que são

$$\mathbf{Z}_2,\mathbf{Z}_3,\mathbf{Z}_4,\mathbf{Z}_5,\mathbf{Z}_6,\mathbf{Z}_7,\ldots \tag{7}$$

e levar a criançada a ver a diferença entre $\mathbf{Z}_2,\mathbf{Z}_3,\mathbf{Z}_5,\mathbf{Z}_7$ porque são os restos na divisão por um *número primo*. Devagar, com profundidade divertida, estarão levando as crianças à ciência da Matemática e tirando-as do horror habitual que a Matemática provoca. Nos conjuntos dos restos se tem as quatro propriedades todas funcionando com a adição, são exemplos de *Aritmética finita*. E no caso dos primos as duas operações, *adição e multiplicação* são completas.

Também é possível neste momento mostrar que os números naturais são defeituosos do ponto de vista da *multiplicação* que tem um elemento neutro mas não tem inverso. Isto pode sair do $\mathbf{Z}_p$ como comparação, e para corrigir $\mathbf{N}$ foram criados os números inteiros $\mathbf{Z}$.

E neste momento novo problema aparece que permite outro avanço, $(\mathbf{Z},\cdot)$, c a multiplicação, tem o mesmo defeito que $(\mathbf{N},+)$. Com isto termino de imaginar o Ensino de Matemática da Escola Fundamental com outra formatação que a leva para fora da Idader Média em que se encontra porque vai aparecer o conceito de *grupo* também levando a outra visão da geometria abrindo espaço para compreender um pouco de química. Claro nada disto é compatível com um *sinistro* na Educação.

Possivelmente esta metodologia introduz de forma natural o *conserto* de $\mathbf{Z}$ para chegar em $\mathbf{Q}$. Claro, esta crítica do ensino é incompleta, o ensino da geometria precisa ter lugar na Escola Fundamental apenas não cabe neste tópico, *Aritmética*, discutir uma forma evoluída de ensinar geometria que respeite a inteligência das crianças.

5 O segundo resultado, indução finita

Este exemplo eu tirei do livro de Davenport e modifiquei um pouco a demonstração dele.

O método do ensino pela solução de problemas é muito produtivo, ele induz o gosto pela pesquisa. Uma análise da aparência, como

$$1=1^2,1+3=2^2,1+3+5=3^2,1+3+5+7=4^2\ldots \tag{8}$$

será sempre verdade que a soma dos sucessivos números ímpares, seja uma sucessão de números naturais ao quadrado? Os números ímpares formam uma p.a. então eu posso descrever esta propriedade como

$$P(N) : \sum_{k=0}^{N} 2k + 1 = N^2; \tag{9}$$

Parece ser verdadeiro e inclusive uma linha de programação serve para ilustrar a sentença na equaçãao (eq.9)

```
S =0; print,'k', 'S';for(k=1;k<20;k+=2) {S+=k; print,k, S;}
 k S
 1 1
 3 4
 5 9
 7 16
 9 25
 11 36
 13 49
 15 64
 17 81
 19 100
```

e até programação pode ser introduzida na Escola, este é um comando de uma linguagem muito parecida com `Python, calc`, linguagens de domínio público que são muito fácil de ser introduzida nas Escolas e podem ser usada para fazer testes aritméticos como este. Esta linha de programação foi escrita em `calc`, mas a sintaxe é quase idêntica a do `Python`. Sugiro um programa escrito em `Python`, [2, programas], `convol.py` que pode escrever quantas linhas você quiser do *triângulo de Pascal*. No mesmo local você encontra dezenas de programas que podem ser baixados livremente.

Mas, é verdade a sentença na equação (eq.9)?

Deixe-me supor que seja, que até um certo número N seja verdadeiro, a listagem me diz que vale até $N = 10$, a soma dos 10 primeiros números ímpares. Que acontece com $N + 1$?

$$P(N+1) : \left(\sum_{k=0}^{N} 2k + 1\right) + 2N + 1 = \left(N^2\right) + 2N + 1 = (N+1)^2; \tag{10}$$

$$P(N) \quad \Rightarrow \quad P(N+1); \tag{11}$$

é o *Princípio da Indução Finita* que deve ser divertido ensinar numa Escola Futurista que tenha rompido com suas ligações medievais. E agora ficou provado que aquela listagem de computador revelou um *teorema* da *Aritmética*. .

Eu chamei a "*indução finita*" de "*princípio*" que é quase um sinônimo de "postulado" ou "axioma". De fato, este "*princípio equivale aos axiomas que o matemático italiano Peano construiu para definir os números naturais.*

Conceitos relacionados:

- Aritmétca modular, a aritmética dos $\mathbf{Z}_p$.
- Teorema fundamental da aritmética.
- Princípio da Indução Finita.

Índice Remissivo

Referências

[1] David I. Bell Landon Curt Noll and other. Calc - arbitrary precision calculator. Technical report, http://www.isthe.com/chongo/, 2011.

[2] Tarcisio Praciano-Pereira. *Cálculo Numérico Computacional*. Sobral Matematica, 2007.

[3] Yitang Zhang. Bounded gaps between primes. *Annals of Mathematics*, 2014.