UM PRELÚDIO À MAGNÍFICA TEORIA DOS NÚMEROS PRIMOS

Thiago Augusto Silva Dourado
Instituto de Matemática e Estatística da Universidade de São Paulo – IME/USP
thiago.dourado@ime.usp.br

“O problema de distinguir os números primos dos números compostos e de exprimir estes últimos à custa dos seus fatores primos deve ser considerado um dos mais importantes e dos mais úteis em aritmética... A própria dignidade da ciência requer que todos os meios possíveis sejam explorados para a resolução de um problema tão elegante e tão famoso.”

C.F. Gauss, *Disquisitiones Arithmeticae*, Art. 329

INTRODUÇÃO

No clássico livro de Edmund Landau, ele escreve: “Gordon dizia algo como: `A Teoria dos Números é útil porque afinal podemos doutorar-nos com ela'.” [4, p. 40]. Isso dá uma ideia da visão que se tinha da teoria dos números, algo belo e majestoso, mas pouco útil. No entanto, tudo isso mudou após os anos de 1940, com o advento da criptografia moderna, cuja base é essencialmente a teoria dos números e em especial a teoria dos números primos. Neste artigo apresentamos resultados e problemas em aberto da teoria dos números primos. Partimos do mais básico, como a infinitude e o deserto de primos e vamos de forma paulatina evoluindo até chegarmos aos problemas estudados nos nossos dias. São nossos objetos os números de Fermat e Mersenne e sobre estes a Conjetura de Bateman-Selfridge-Wagstaff; a famigerada Conjetura de Goldbach e os avanços feitos nela até aos nossos dias, passando por Ivan Vinogradov e chegando até Harald Helfgott; o Teorema de Dirichlet e a “recíproca” de Green-Tao; Primos Gémeos e o importante teorema de Zhang; o Teorema do Número Primo e a Hipótese de Riemann, onde apresentamos a Conjetura de Hardy-Littlewood e a forma equivalente usando a função de Möbius para a hipótese de Riemann; e, por fim, apresentamos algumas fórmulas para a obtenção de números primos. Buscamos apresentar o que há de mais recente em cada assunto.

1. INFINITUDE E DESERTO DE PRIMOS

Os números primos recebem este nome devido ao que diz o Teorema Fundamental da Aritmética: *Todo o inteiro $n \geqslant 1$ pode ser escrito de forma única (a menos da ordem dos fatores) como o produto de primos.* Já nos *Elementos* (Livro IX – Proposição 20), Euclides provou a infinidade dos números primos. Reproduzamos essa prova:

[Em todo o texto p_n indicará o n-ésimo número primo.]

Suponhamos que $p_1, \ldots, p_n$ sejam todos os números primos, e seja $N = p_1 p_2 \cdots p_n + 1$. Assim, devido ao Teorema Fundamental da Aritmética, existe ℓ, $1 \leqslant \ell \leqslant n$, tal que $p_\ell \mid N$, e como $p_\ell \mid p_1 p_2 \cdots p_n$, temos que $p_\ell \mid (N - p_1 p_2 \cdots p_n)$, isto é, $p_\ell \mid 1$, absurdo. □

Embora existam infinitos primos, pode ter-se um espaço tão grande quanto se queira entre dois primos subsequentes. Este *deserto primo* é dado pela sequência de um número n qualquer de números compostos:

$$(n+1)! + 2, (n+1)! + 3, \ldots, (n+1)! + n + 1.$$

(Note que $\ell \mid (n+1)! + \ell$ para $2 \leqslant \ell \leqslant n+1$).

2. NÚMEROS DE FERMAT E DE MERSENNE

Pierre de Fermat conjeturou que os números da forma $F_n = 2^{2^n} + 1$ ($n \geq 0$), hoje conhecidos como *números de Fermat*, eram todos primos. Os cinco primeiros números de Fermat, todos primos, são:

$$F_0 = 2^{2^0} + 1 = 3, \quad F_1 = 2^{2^1} + 1 = 5, \quad F_2 = 2^{2^2} + 1 = 17,$$
$$F_3 = 2^{2^3} + 1 = 257, \quad F_4 = 2^{2^4} + 1 = 65537.$$

Entretanto, em 1732, Euler mostrou que todo o fator primo de F_n é da forma $k2^{n+2} + 1$ e, testando tais números, mostrou que 641 divide F_5:

$$F_5 = 641 \cdot 6700417.$$

Com efeito, sabendo que $641 = 2^4 + 5^4 = 2^7 \cdot 5 + 1$, tem-se que $2^7 \cdot 5 \equiv -1 \pmod{641}$, elevando a quarta potência obtemos que $2^{28} \cdot 5^4 \equiv 1 \pmod{641}$ assim, usando que $641 = 2^4 + 5^4$, isto é, que $5^4 \equiv -2^4 \pmod{641}$, obtemos que $2^{28} \cdot 5^4 \equiv -2^{28} \cdot 2^4 \equiv 1 \pmod{641}$, isto é, $-2^{32} \equiv 1 \pmod{641}$, ou, equivalentemente,

$$2^{32} \equiv -1 \pmod{641}.$$

Portanto $2^{32} + 1 = 2^{2^5} + 1$ é divisível por 641. □

Em 1877, Pépin [7, p. 71] deu o seguinte teste envolvendo números de Fermat:

F_n é primo se, e somente se, $3^{\frac{F_n - 1}{2}} \equiv -1 \pmod{F_n}$.

Lucas (1877) [7, p. 72] utilizou este teste para mostrar que F_6 é composto e Landry (1880) [7, p. 72] fatorizou-o:

$$F_6 = 2^{64} + 1 = 18446744073709551617 \\ = 274177 \cdot 67280421310721.$$

Em 1970, Morrison e Brillhart [7, p. 72] deram a decomposição de F_7:

$$F_7 = 2^{128} + 1 = 340282366920938463463374607431768211457 \\ = 59649589127497217 \cdot 5704689200685129054721.$$

A maior fatorização completa de um número de Fermat que se conhece é a de F_{11} [7, p. 73]:

$$F_{11} = 319489 \cdot 974849 \cdot 167988556341760475137 \\ \cdot 3560841906445833920513 \cdot [\text{número primo de 564 algarismos}].$$

Os fatores 319489 e 974849 de F_{11} foram obtidos por Cunningham (1899) [7, p. 73], outros fatores foram obtidos por Brent (1988) [7, p. 73] e a primalidade do último fator por Morain (1988) [7, p. 73].

Além dos primeiros cinco, listados acima, não se conhece nenhum outro número de Fermat que seja primo.

Em 1730, Goldbach deu uma prova da infinitude dos números primos usando números de Fermat. Ele provou que $\text{mdc}\,(F_n, F_m) = 1$ para $n \neq m$. Isto de facto prova a infinitude dos primos, pois sendo infinita a sequência dos números de Fermat e não possuindo fatores primos em comum, isto não poderia ocorrer se o conjunto dos primos fosse finito.

Demonstração. *Mostremos inicialmente que a seguinte relação se verifica:*

$$F_0 F_1 \cdots F_{n-1} = F_n - 2.$$

Com efeito, para $n = 1$ temos que $F_0 = 3 = F_1 - 2$. Supondo então o resultado válido para n, temos que

$$F_0 F_1 \cdots F_n = (F_0 F_1 \cdots F_{n-1}) F_n = (F_n - 2) F_n \\ = (2^{2^n} + 1 - 2)(2^{2^n} + 1) = (2^{2^n} - 1)(2^{2^n} + 1) \\ = 2^{2^{n+1}} - 1 = 2^{2^{n+1}} + 1 - 2 = F_{n+1} - 2.$$

Tomando $n < m$ temos, pela relação acima, que $F_0 F_1 \cdots F_n \cdots F_{m-1} = F_m - 2$, donde segue que $F_m - F_0 F_1 \cdots F_n \cdots F_{m-1} = 2$. Assim, se um número d divide F_n e F_m então d também divide 2, mas como F_n é ímpar, d não pode ser 2, portanto $\text{mdc}\,(F_n, F_m) = 1$. □

Os números da forma $b^{2^m} + 1$ com $m \geq 1$ e $b \geq 2$ são chamados *números de Fermat generalizados*. Em 1985, Dubner [7, p. 239] conseguiu descobrir números de Fermat generalizados bastante grandes que são primos, como, por exemplo, $150^{2^{11}} + 1$. Num artigo publicado em 2002, Dubner e Gallot [7, p. 240] descreveram um método computacional para determinar a primalidade desses números. Com este processo já se conhecem mais de 200 números de Fermat generalizados que são primos. É de setembro de 2018 o maior primo generalizado de Fermat conhecido: $1059094^{2^{20}} + 1$ (com 6317602 dígitos) [12].

Se $a^n - 1$ é primo, $n > 1$ e $a > 1$, então $a = 2$ e n é primo. Com efeito, como

$$a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \cdots + a + 1),$$

e o fator da direita é maior do que 1 ($a > 1$) concluímos que $a - 1$ deve ser igual 1, pois $a^n - 1$ é primo, logo a deve ser igual 2. Assim sendo, suponha que $n = rs, 1 < r, s < n$, logo $2^{rs} - 1 = (2^r - 1)(2^{r(s-1)} + 2^{r(s-2)} + \cdots + 2^r + 1)$, o que contradiz o facto de $2^{rs} - 1$ ser primo. □

Em 1974, Ligh e Neal [7, p. 76] mostraram que se $2^n - 1$ é uma potência de um número primo, ele próprio deve ser um primo e então n é primo, isto é, se $2^n - 1 = p^m$ (m natural e p primo), então $m = 1$. Os números $M_n = 2^n - 1$ (com n primo) são chamados *números de Mersenne* e a sua introdução foi motivada pelo estudo dos números perfeitos.

Um número inteiro positivo é dito *perfeito* se é a soma dos seus divisores próprios. Tem este nome porque todos os números perfeitos são triangulares e hexagonais. Os seis primeiros números perfeitos são: 6, 28, 496, 8128, 33550336, 8589869056. Euclides (*Elementos*, Livro IX – Proposição 36) mostrou que se $2^n - 1$ é um número primo, então $2^{n-1}(2^n - 1)$ é um número perfeito. Em 1747, Euler provou que todo o número perfeito par é da forma $2^{n-1}(2^n - 1)$. Portanto, todo o primo de Mersenne gera um número perfeito par, numa correspondência unívoca entre ambos os conjuntos. Até ao presente momento, conhecemos 51 números primos de Mersenne, logo 51 números perfeitos. O maior número primo conhecido, que também é o maior primo de Mersenne conhecido, é devido a Patrick Laroche (dezembro de 2018): $2^{82589933} - 1$ (com 24862048 dígitos) [11].

Em relação aos números de Mersenne, o problema que naturalmente se apresenta é o de saber se são primos ou compostos e, neste último caso, determinar os seus fatores primos. Em 1878, Lucas [7, p. 78] deu o seguinte resultado: *M_n é primo se, e somente se, $M_n \mid S_{n-2}$, onde S_ℓ é definida por recorrência: $S_0 = 4$ e $S_\ell = S_{\ell-1}^2 - 2$.* Um resultado clássico sobre os fatores primos de M_n foi enunciado por Euler em 1750 e demonstrado por Lagrange em 1775 e também por Lucas em 1878 [7, p. 76]: *Se p é um número primo e*

$p \equiv 3 \pmod 4$, *então* $2p+1$ *divide* M_p *se e somente se* $2p+1$ *é primo; neste caso, se* $p > 3$, *então* M_p *é composto.*

Conjetura de Bateman–Selfridge–Wagstaff (1989) [7, p. 83]. *Seja* n *um natural ímpar. Se duas das condições abaixo forem satisfeitas, então a terceira também o será:*

(i) n *é igual a* $2^k \pm 1$ *ou a* $4^k \pm 3$ *(para alguma* $k \geq 1$*).*

(ii) M_n *é primo.*

(iii) $\frac{2^n+1}{3}$ *é um número primo.*

3. CONJETURA DE GOLDBACH

Numa carta, datada de 7 de junho de 1742, Christian Goldbach escreveu a Leonhard Euler a seguinte afirmação:

(I) *Todo o inteiro* $n > 5$ *é a soma de três números primos.*

Euler respondeu-lhe que era fácil ver que a afirmação era equivalente à seguinte:

(II) *Todo o inteiro par* $2n \geq 4$ *é a soma de dois números primos.*

Esta é a famosa *Conjetura de Goldbach*. Muitos avanços foram feitos, conforme veremos, mas a conjetura em si segue aberta.

Provemos que de facto (I) e (II) são equivalentes.

Demonstração. *(I)* $\Rightarrow$ *(II), Se* $2n \geqslant 4$*, então* $2n+2 = p+p'+p''$*, onde* p*,* p' *e* p'' *são números primos. Um desses primos é então necessariamente par, por exemplo,* $p'' = 2$*; então* $2n = p+p'$*.*

(II) $\Rightarrow$ *(I), Para* $2n \geq 6$*, temos por hipótese que* $2n-2 = p+p'$*, onde* p *e* p' *são números primos; assim* $2n = 2+p+p'$ *e* $2n+1 = 3+p+p'$*.* □

Em 1930, Lev Schnirelmann [7, p. 213] provou que qualquer número natural maior do que 1 pode ser escrito como a soma de, no máximo, C números primos, onde C é uma constante efetivamente computável. A constante C de Schnirelmann é o menor número com essa propriedade. O próprio Schnirelmann obteve $C < 800\,000$. Esse resultado foi posteriormente aprimorado por muitos autores, como Olivier Ramaré, que em 1995 mostrou que todo o número par $n \geq 4$ é de facto a soma de, no máximo, 6 números primos.

Um resultado menos exigente, conhecido como *Conjetura Fraca de Goldbach* diz o seguinte: Todo o número ímpar $n \geq 5$ é a soma de três números primos. Em 1937, Ivan Matveevich Vinogradov [7, p. 212] provou que todos os números ímpares suficientemente grandes podem ser expressos como a soma de três números primos. A prova original de Vinogradov, que usava o ineficaz teorema de Siegel-Walfisz, não dava um limite para "suficientemente grande"; o seu aluno K. Borozdkin (1956) [7, p. 212] deduziu que $e^{e^{16\,038}} \approx 3^{3^{15}}$ é grande o suficiente. A parte inteira deste número possui 4 008 660 dígitos decimais, portanto, verificar todos os números abaixo desse número seria completamente inviável. Em 2002, Liu Ming-Chit e Wang Tian-Ze [6] reduziram o limitante de Borozdkin para aproximadamente $n > e^{3100} \approx 2 \times 10^{1346}$. O expoente ainda era demasiado grande para admitir verificação computacional de todos os números menores. Em 2012 e 2013, o matemático peruano Harald Helfgott [5, p. 321] divulgou um par de trabalhos melhorando as estimativas de arco maior e menor o suficiente para provar incondicionalmente a Conjetura Fraca de Goldbach. O resultado de Helfgott implica diretamente que todo o número par $n \geqslant 4$ é a soma de, no máximo, 4 primos.

O teorema, devido a Jingrun Chen [2] e publicado em 1966, afirma que todo o número par suficientemente grande pode ser escrito como a soma de dois primos, ou um primo e um semiprimo (o produto de dois primos). Em 2002, Ying Chun Cai [1] provou que: *Existe um número natural* N *tal que todo o inteiro par* N *maior do que* N *é a soma de um primo menor ou igual a* $n^{0,95}$ *e um número com, no máximo, dois fatores primos.* Em 2015, Tomohiro Yamada provou a seguinte versão explícita do Teorema de Chen: *Todo o número par maior do que* $e^{e^{36}} \approx 1,7 \times 10^{1872344071119348}$ *é a soma de um primo e um produto de, no máximo, dois primos.*

4. TEOREMA DE DIRICHLET

Um teorema clássico e muito importante foi provado por Dirichlet em 1837:

Se $d \geqslant 2$ *e* $a \neq 0$ *são números inteiros que são primos entre si, então a progressão aritmética*

$$a, \quad a+d, \quad a+2d, \quad a+3d, \quad \ldots$$

contém uma infinidade de números primos.

Muitos casos especiais desse teorema já eram conhecidos, incluindo, é claro, o Teorema de Euclides sobre a infinidade de primos (quando $a = 2$ e $d = 1$). Provemos o caso particular em que $a = 5$ e $d = 6$ (que é bastante similar à prova de Euclides):

Dividindo um número qualquer por 6, os possíveis restos são 0, 1, 2, 3, 4 e 5 o que significa que um inteiro pode ser escrito numa das seguintes formas: $6\ell, 1+6\ell, 2+6\ell, 3+6\ell, 4+6\ell, 5+6\ell$. Logo, se p é um primo ímpar diferente de 3, então p é da forma $1+6\ell$ ou

$5+6\ell$. Para mostrarmos que existem infinitos primos da forma $5+6\ell$ vamos supor o contrário, isto é, que existe apenas um número finito deles. Sejam $p_0=5, p_1, p_2, \ldots, p_r$ estes números. Consideremos então o número

$$N = 5 + 6p_1p_2\cdots p_r.$$

É claro que este número não é divisível por nenhum dos números primos $p_0, p_1, p_2, \ldots, p_r$. Afirmamos que n possui um fator primo da forma $5+6\ell$, pois, caso contrário, seriam da forma $1+6\ell$, o que não é possível, uma vez que o produto de dois números da $1+6\ell$ é sempre desta mesma forma. Isto mostra que, ou n é primo e portanto da forma $5+6\ell$, ou n possui um fator primo da forma $5+6\ell$ que não está lista acima. Portanto, existem infinitos primos da forma $5+6\ell$. □

Em 2004, Ben Green e Terence Tao [5, p. 323] apresentaram uma "recíproca" do Teorema de Dirichlet. Eles mostraram que a sequência de números primos contém progressões aritméticas arbitrariamente longas, isto é, para cada número natural k, existe uma progressão aritmética formada por k números primos. Este resultado, entre outros, rendeu a Terence Tao a Medalha Fields de 2006.

Por exemplo, se $k=3$, temos: 7, 13, 19. A 12 de abril de 2010, Benoãt Perichon [5, p. 232], encontrou uma sequência contendo 26 primos:

$$43142746595714191 + 23681770\cdot 223092870\cdot n,$$

para n variando de 0 a 25. Este é o maior exemplo conhecido do Teorema de Green-Tao.

5. PRIMOS GÉMEOS

Números onde p e $p+2$ são ambos primos são ditos *primos gémeos*. Conjetura-se, mas não se sabe demonstrar até agora, que existem infinitos pares de primos gémeos. Os maiores primos gémeos conhecidos, devido a Chris Cal-dwell (setembro de 2018) são: $2996863034895\cdot 2^{1290000}\pm 1$ [12].

Em 1737, Euler provou que

$$\sum_{p \text{ primo}} \frac{1}{p} = \infty,$$

demonstrando assim, como consequência, a infinitude dos números primos. Assim, um caminho na tentativa de provar a infinitude dos primos gémeos seria provar a divergência da série destes números. Entretanto, em 1919, Viggo Brun [5, p. 311] provou que

$$\sum_{p,p+2 \text{ primos}} \left(\frac{1}{p}+\frac{1}{p+2}\right) = B \approx 1,902160583104.$$

Em 1949, P. A. Clement [5, p. 312] demonstrou que $(p, p+2)$ é um par de números primos gémeos se, e somente se, $4((p-1)!+1) \equiv -p \pmod{p(p+2)}$.

O matemático francês Alphonse de Polignac [7, p. 215] conjeturou, em 1849, de forma mais geral, que para cada natural k há infinitos pares de primos p e q tais que $q-p=2k$. O caso $k=1$ é a conjetura dos primos gémeos. A 17 de Abril de 2013, Yitang Zhang [5, p. 322] anunciou uma prova de que para algum inteiro n menor do que 70 milhões, há infinitos pares de primos cuja diferença é n. O artigo de Zhang foi aceite pela *Annals of Mathematics* no início de maio de 2013, sendo a sua primeira publicação desde o seu último artigo em 2001. Terence Tao, em sequência, propôs o *Polymath8* com a intenção de melhorar colaborativamente a cota de Zhang. Em abril de 2014, um ano após o anúncio inicial, a melhor cota provada é de 246, que melhora substancialmente a estimativa inicial de 70 milhões.

A conjetura de Andrica (1986) [7, p. 191], verificada numericamente para $2^{42} \approx 4,39\times 10^{12}$, afirma que

$$\sqrt{p_{n+1}} - \sqrt{p_n} < 1.$$

Em 2005, Goldston, Pintz e Yldirin demonstraram que

$$\liminf_{n\to\infty} \frac{p_{n+1}-p_n}{\log p_n} = 0.$$

6. TEOREMA DO NÚMERO PRIMO E A HIPÓTESE DE RIEMANN

Seja x um número real positivo, definimos $\pi(x)$ como o número de primos menores ou iguais a x. O Teorema do Número Primo [5, Apêndice A] afirma que

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1.$$

Isto é, $\pi(x)$ é assintótica a $x/\log x$. Este resultado é fundamental pois mostra como se distribuem os números primos. Na tabela 1 apresentamos alguns resultados numéricos deste quociente. O Teorema do Número Primo só foi demonstrado em 1896, de forma independente, por Jacques Hadamard e Charles Jean de la Vallée Poussin. Para demonstrar este resultado, ambos utilizaram a função zeta de Riemann, definida por

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s},$$

em que s é um número complexo e a parte real de s é maior do que 1.

Tabela 1. Valores numéricos de $\frac{\pi(x)}{x/\log x}$.

x	$\frac{\pi(x)}{x/\log x}$
10	0,9210340372
100	1,151292546
1000	1,160502887
10000	1,131950832
100000	1,104319811
1000000	1,084489948

A função ζ de Riemann pode ser estendida a outros limites do plano complexo para além do indicado $\operatorname{Re} s > 1$. De facto, ζ pode ser estendida analiticamente a todo o plano complexo, com exceção de $s = 1$.

Se s é um inteiro negativo par, então $\zeta(s) = 0$, porém se s não está neste caso e $\zeta(s) = 0$, existe uma conjetura que afirma que se isto ocorre tem-se necessariamente que $\operatorname{Re} s = 1/2$. Esta conjetura é conhecida como *Hipótese de Riemann*, um dos Problemas do Milénio e vale um milhão de dólares!

Em 1914, G. H. Hardy [3] provou que existem infinitos zeros na função ζ na reta $\operatorname{Re} s = 1/2$. Levinson [7, p. 174], em 1974, mostrou que pelo menos um terço dos zeros da função ζ encontram-se na reta $\operatorname{Re} s = 1/2$.

Definimos a função de Möbius da seguinte forma:

$$\mu(n) = \begin{cases} 1 & \text{se } n = 1, \\ (-1)^r & \text{se } n \text{ é o produto de } r \text{ primos distintos}, \\ 0 & n \text{ tem um fator quadrado.} \end{cases}$$

Em posse desta função, apresentamos uma formulação equivalente da Hipótese de Riemann [5, p. 192]:

$$\lim_{n\to\infty} \frac{\sum_{k=1}^{n} \mu(k)}{n} = 0.$$

Na figura 1 apresentamos um gráfico desta razão.

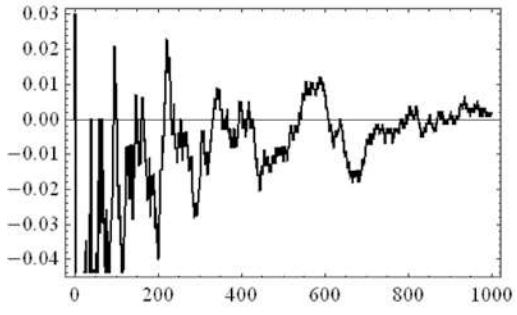

Figura 1. Gráfico de $f(n) = \frac{\sum_{k=1}^{n} \mu(k)}{n}$, $0 \leqslant n \leqslant 1000$.

Na secção 1, apresentamos o deserto de primos. Em 1845, Joseph Bertrand, baseado em observações numéricas, afirmou que os primos não são tão "esparsos" assim [5, p. 201]:

Entre os inteiros $n \geq 2$ e $2n$, há sempre um número primo.

De maneira equivalente, a afirmação pode ser expressa pela desigualdade

$$\pi(2n) - \pi(n) \geqslant 1 \text{ (para } n \geqslant 2),$$

ou ainda por

$$p_{n+1} < 2p_n \text{ (para } n \geqslant 1).$$

Em 1923, Hardy e Littlewood [7, p. 182] apresentaram a seguinte conjetura que todavia segue em aberto:

$$\pi(x+y) \leqslant \pi(x) + \pi(y) \text{ para todo } x \geqslant 2, y \geqslant 2.$$

Em 1975, Rosser e Schoenfeld [7, p. 182] mostraram que

$$\pi(2x) < 2\pi(x) \text{ para } x \geqslant 5.$$

Também em 1975, Udrescu [7, p. 183] provou que: *Para todo o $\varepsilon > 0$, se $x, y \geqslant 17$ e $x + y \geqslant 1 + e^{4(1+1/\varepsilon)}$, então*

$$\pi(x+y) < (1+\varepsilon)(\pi(x) + \pi(y)).$$

Em 2002, Dusart [7, p. 183] provou que: *Se $2 \leqslant x \leqslant y \leqslant \frac{7}{5} x \log x \log\log x$, então*

$$\pi(x+y) \leqslant \pi(x) + \pi(y).$$

7. FÓRMULAS PARA NÚMEROS PRIMOS

Em 1964, C. P. Willians [7, p. 133] apresentou a seguinte fórmula para o n-ésimo número primo:

$$p_n = 1 + \sum_{m=1}^{2^n} \left\lfloor \sqrt[n]{\frac{n}{1+\pi(m)}} \right\rfloor.$$

Demonstração. Para $n \geqslant 1$ temos $2^n > n$, donde

$$0 < \frac{n}{1+\pi(m)} \leqslant n < 2^n,$$

e logo

$$0 < \sqrt[n]{\frac{n}{1+\pi(m)}} < 2.$$

Assim, a parte inteira do radical só pode ser 0 ou 1, e é 1 se e só se $n/(1+\pi(m)) \geqslant 1$, ou seja, se e só se $1 + \pi(m) \leqslant n$, o que equivale a $\pi(m) < n$, e vale se e só se $m < p_n$.

Como $p_n \leqslant 2^n$ para todo o n (isso segue do postulado de Bertrand), a soma

$$\sum_{m=1}^{2^n} \left\lfloor \sqrt[n]{\frac{n}{1+\pi(m)}} \right\rfloor$$

vale exatamente $p_n - 1$, o que prova o resultado. □

O Teorema de Miná̂c-Ribenboim [7, p. 129] dá-nos uma fórmula explícita para o número de primos:

$$\pi(m) = \sum_{j=2}^{m} \left\lfloor \frac{(j-1)!+1}{j} - \left\lfloor \frac{(j-1)!}{j} \right\rfloor \right\rfloor .$$

Gandhi [7, p. 134], em 1971, também apresentou uma fórmula para o n-ésimo número primo:

$$p_n = \left\lfloor 1 - \frac{1}{\log 2} \log \left(-\frac{1}{2} + \sum_{d \mid p_1 p_2 \cdots p_{n-1}} \frac{\mu(d)}{2^d - 1} \right) \right\rfloor .$$

Em 1947, Mills [7, p. 137] demonstrou que existe um número real $\theta > 1$ tal que para todo o inteiro $n \geqslant 1$ o número

$$\left\lfloor \theta^{3^n} \right\rfloor$$

é primo. Mills determinou que θ é aproximadamente igual a 1,3064. Um estudo mais aprofundado do trabalho de Mills permitiu mostrar que se $c > 2,106$, existe um conjunto não enumerável de números reais $\theta > 0$ tais que para todo o inteiro $n \geq 1$ o número

$$\left\lfloor \theta^{c^n} \right\rfloor$$

é primo. Wright [7, p. 137], em 1951, mostrou que

$$g(n) = \left\lfloor 2^{2^{2^{\cdot^{\cdot^{\cdot^{2^{\omega}}}}}}} \right\rfloor ,$$

com uma sucessão de n expoentes e $\omega \approx 1,9287800\ldots$, é um número primo.

Como foi visto no texto, o estudo dos números primos pode ser bastante frutífero e empolgante. Resultados novos e surpreendentes continuam a surgir. O que foi apresentado aqui não passa de um prelúdio a esta magnífica teoria.

REFERÊNCIAS

[1] Cai, Y. C., "Chen's Theorem with Small Primes". *Acta Mathematica Sinica*, 18, (2002), 597-604.

[2] Chen, J., "Sobre a representação de um grande número inteiro par como a soma de um primo e um produto de, no máximo, dois primos." [em chinês] *Kexue Tongbao.* 17, (1966), 385-386.

[3] Hardy, G. H., "Sur les zéros de la fonction $\zeta(s)$ de Riemann". *Comptes Rendus Acad. Sci. Paris*, 158, 1012-1014.

[4] Landau, E., *Teoria Elementar dos Números.* Tradução de Paulo Henrique Viana de Barros, Ciência Moderna, Rio de Janeiro, 2002.

[5] Martinez, F. B.; Moreira, C. G. T. A.; Saldanha, N. C.; Tengan, E., *Teoria dos Números: Um Passeio com Primos e Outros Números Familiares pelo Mundo Inteiro.* 4ª. edição, Projeto Euclides, IMPA, Rio de Janeiro, 2018.

[6] Ming-Chit, L.; Tian-Ze, W., "Distribution of zeros of Dirichlet L-functions and an explicit formula for $\psi(t, \chi)$". *Acta Arithmetica* 102 (2002), 261-293.

[7] Ribenboim, P., *The Little Book of Bigger Primes.* Second Edition, Springer-Verlag New York, 2004.

[8] Santos, J. P. O., *Introdução à Teoria dos Números.* 3ª. edição, Coleção Matemática Universitário, IMPA, Rio de Janeiro, 2011.

[9] Vieira, V. L., *Um Curso Básico em Teoria dos Números.* 2ª. Edição, Coleção Textuniversitários, 7, Editora Livraria da Física, São Paulo, 2020.

[10] Yamada, T., *Explicit Chen's theorem.* arXiv:1511.03409, (2015-11-11).

[11] *GIMPS - Great Internet Mersenne Prime Search. https://www.mersenne.org/primes/?press=M82589933*

[12] *Top Twenty's Home Page. https://primes.utm.edu/top20/home.php.*

SOBRE O AUTOR

Thiago Augusto Silva Dourado é formado em Matemática Pura pela Universidade Federal de Mato Grosso do Sul – UFMS, um estado do centro-oeste brasileiro onde se localiza o Pantanal. Atualmente integra o corpo académico da Universidade de São Paulo – USP. As suas principais áreas de interesse são a álgebra e a teoria dos números, isto principalmente devido à influência de seus precetores e amigos Paulo Ribenboim, Carlos Gustavo Moreira - Gugu e César Polcino Milies, mas também nutre um enorme apreço pela filosofia e pela história da matemática.