MAT^2
MATerials MATemàtics
Volum 2025, treball no. 6, 62 pp. ISSN: 1887-1097
Publicació electrònica de divulgació del Departament de Matemàtiques
de la Universitat Autònoma de Barcelona
www.mat.uab.cat/web/matmat

Um Passeio Pelos Números Primos*

Luis Fernando Mello

Conteúdo

1 Introdução

Este artigo é uma organização dos estudos realizados no primeiro semestre de 2022, mais precisamente de março a junho, pela turma do Programa de Iniciação Científica e Mestrado - PICME - da Universidade Federal de Itajubá. As atividades foram desenvolvidas de forma remota, em função da pandemia de COVID-19 que existia à época. Semanalmente foi feita uma reunião de sessenta minutos para discussão do assunto selecionado, além de uma reunião extra também semanal para discussão das dúvidas e dos exercícios propostos para estudo.

*Dedicado à Edinita, Larissa e Luis Gustavo, com amor e gratidão.

Como a rotação dos alunos do PICME é grande, uma vez que cada aluno pode participar de, no máximo, quatro semestres, e, de um modo geral, esses alunos estão no início de seus estudos universitários e têm formações muitos distintas, é um desafio grande encontrar um tema para estudo que seja suficientemente interessante e cientificamente significativo. Para aquele semestre, o tema selecionado foi "números primos", uma vez que, de acordo com Albert Einstein: "If Euclid failed to kindle your youthful enthusiasm, then you were not born to be a scientific thinker."

Escolhido o tema de estudo, uma tarefa igualmente difícil é selecionar os assuntos que serão estudados. Foram escolhidos os assuntos que são os títulos das seções deste artigo. Muitos outros não foram selecionados por motivos diversos, os principais deles foram o tempo que tínhamos para estudo (15 semanas) e a maturidade da turma.

Este artigo segue exatamente os registros das atividades desenvolvidas. Cada seção corresponde ao material estudado em uma reunião semanal. A maioria dos teoremas têm suas demonstrações apresentadas em um nível bastante elementar. No final de cada seção são colocados um ou dois exercícios. Alguns deles são utilizados em seções seguintes.

2 Número primo

Nesta seção serão fixadas as nomenclaturas e os símbolos que serão utilizados ao longo do texto. Os assuntos aqui tratados podem ser encontrados nos excelentes livros [10], [12] e [14].

Assumiremos conhecidos os seguintes conjuntos:

(i) O conjunto dos *número naturais*

$$\mathbb{N} = \{1, 2, 3, \ldots\}.$$

(ii) O conjunto dos *número inteiros*

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

O conjunto dos números naturais $\mathbb{N}$ também será chamado de *o conjunto dos números inteiros positivos.*

Assumiremos, ainda, os seguintes princípios.

Princípio 2.1 (Princípio da Boa Ordem)**.** *Todo conjunto não vazio de inteiros positivos contém um elemento mínimo.*

Princípio 2.2 (Princípio da Indução Finita–Primeira Forma)**.** *Considere $B \subset \mathbb{N}$. Se B possui as seguintes duas propriedades*

- $1 \in B$,

- $k+1 \in B$, *sempre que* $k \in B$,

então $B = \mathbb{N}$.

Princípio 2.3 (Princípio da Indução Finita–Segunda Forma)**.** *Considere* $B \subset \mathbb{N}$. *Se* B *possui as seguintes duas propriedades*

- $1 \in B$,
- $k+1 \in B$, *sempre que* $1, 2, \ldots, k \in B$,

então $B = \mathbb{N}$.

Vejamos um exemplo simples da utilização do Princípio da Indução Finita–Primeira Forma.

Exemplo 2.1. *Para cada* $n \in \mathbb{N}$, *defina*

$$S(n) = 1 + 2 + \cdots + n. \tag{1}$$

Considere o conjunto

$$B = \left\{ n \in \mathbb{N} : S(n) = \frac{n(n+1)}{2} \right\}.$$

Queremos mostrar que $B = \mathbb{N}$. *Para isto, utilizaremos o Princípio da Indução Finita–Primeira Forma. É imediato que* $1 \in B$, *pois* $S(1) = 1 = 1(1+1)/2$.
Hipótese de Indução (HI): $k \in B$, *isto é,*

$$S(k) = 1 + 2 + \cdots + k = \frac{k(k+1)}{2}.$$

Analisaremos, sob a HI, se $k+1 \in B$, *isto é, se*

$$S(k+1) = 1 + 2 + \cdots + k + (k+1) = \frac{(k+1)((k+1)+1)}{2} = \\ = \frac{(k+1)(k+2)}{2}.$$

Da HI, resulta

$$S(k+1) = (1 + 2 + \cdots + k) + (k+1) = \\ = \left(\frac{k(k+1)}{2} \right) + (k+1) = (k+1)\left(\frac{k}{2} + 1 \right) \\ = (k+1)\left(\frac{k+2}{2} \right) = \frac{(k+1)(k+2)}{2}.$$

Concluímos, assim, que $k+1 \in B$. *Pelo Princípio da Indução Finita–Primeira Forma,*

$$B = \mathbb{N},$$

ou seja,

$$S(n) = 1 + 2 + \cdots + n = \frac{n(n+1)}{2},$$

para todo $n \in \mathbb{N}$.

Considere $a, b \in \mathbb{Z}$. Dizemos que a *divide* b, denotando por

$$a|b,$$

se existe $c \in \mathbb{Z}$ tal que

$$b = ac.$$

Se a não divide b escrevemos

$$a \nmid b.$$

Para dar um gostinho de como utilizar a definição acima, vejamos a seguinte proposição.

Proposição 2.1. *Considere* $a, b, c \in \mathbb{Z}$. *Se* $a|b$ *e* $b|c$, *então* $a|c$.

Demonstração. Como $a|b$ e $b|c$, existem $k_1, k_2 \in \mathbb{Z}$ tais que

$$b = k_1 a, \qquad c = k_2 b.$$

Assim,

$$c = k_2 b = k_2(k_1 a) = (k_1 k_2)a, \quad \text{com} \quad k_1 k_2 \in \mathbb{Z},$$

o que implica que $a|c$, terminando a prova da proposição. □

O teorema a seguir é fundamental nas discussões ao longo deste texto.

Teorema 2.1 (Algoritmo da Divisão)**.** *Dados* $a, b \in \mathbb{Z}$, *com* $b > 0$, *existe um único par* $q, r \in \mathbb{Z}$ *tais que*

$$a = q\,b + r, \quad \textit{com} \quad 0 \leq r < b.$$

O número inteiro q é chamado *quociente* e o número inteiro r é o *resto* da divisão de a por b. Note que

$$r = 0 \iff b|a.$$

Considere $a, b \in \mathbb{Z}$ com a ou b diferente de zero. O *máximo divisor comum* de a e b, denotado por (a, b), é o maior inteiro que divide a e b.

Pode-se mostrar que o máximo divisor comum de a e b é o divisor positivo de a e b o qual é divisível por todo divisor comum.

Os números inteiros a e b são chamados *relativamente primos* se

$$(a, b) = 1.$$

Um número inteiro $p > 1$ é um número *primo* se os únicos divisores positivos de p são os números 1 e o próprio p. Se $p > 1$ não é primo dizemos que ele é *composto*.

Os números

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17$$

são primos, enquanto que

$$4,\ 15,\ 3375$$

são compostos.

Exercício 2.1. *Considere $a, b \in \mathbb{Z}$ com a ou b diferente de zero e suponha que*

$$d = (a, b).$$

Mostre que existem $n_0, m_0 \in \mathbb{Z}$ tais que

$$d = n_0 a + m_0 b.$$

Exercício 2.2. *Defina os números de Fermat*

$$F_n = 2^{2^n} + 1, \quad com \quad n = 0, 1, 2, \ldots.$$

Mostre que, para todo número natural $m \geq 1$, vale

$$F_m - 2 = F_0\, F_1 \cdots F_{m-1}.$$

3 Números primos: Não finitude e Teorema de Euclides

Uma primeira pergunta natural a respeito dos números primos é a seguinte.

Pergunta 3.1. *Considere $\mathcal{P} \subset \mathbb{N}$ o conjunto dos números primos. O conjunto $\mathcal{P}$ é finito ou infinito?*

A primeira resposta a essa pergunta apareceu há cerca de 2300 anos em "Os Elementos" de Euclides [7]. Em sua homenagem, o teorema da não finitude dos números primos é chamado de Teorema de Euclides.

Teorema 3.1 (Teorema de Euclides)**.** *O conjunto $\mathcal{P}$ é infinito.*

Na prova do Teorema de Euclides, utilizaremos o Teorema Fundamental da Aritmética - TFA. O TFA afirma que todos os números inteiros positivos maiores que 1 podem ser decompostos num produto de números primos, sendo esta decomposição única a menos de permutações dos fatores. O TFA também é conhecido como Teorema da Fatoração Única.

Teorema 3.2 (Teorema Fundamental da Aritmética)**.** *Todo inteiro $n > 1$ pode ser escrito unicamente da forma*

$$n = p_1^{n_1} \, p_2^{n_2} \, \cdots \, p_k^{n_k},$$

sendo

$$p_1 < p_2 < \cdots < p_k$$

primos e $n_i > 0$ para todo $i \in \{1, 2, \ldots, k\}$.

Prova do Teorema de Euclides. Suponha que $\mathcal{P}$ é finito. Considere

$$\mathcal{P} = \{p_1, p_2, \ldots, p_n\}.$$

Defina o número inteiro positivo

$$a = p_1 \, p_2 \, \cdots \, p_n + 1.$$

Por construção, a não é divisível por nenhum $p_i \in \mathcal{P}$ e, claramente, $a > p_i$, $i \in \{1, 2, \ldots, n\}$. Assim, pelo TFA, ou a é primo ou possui um fator primo. Em ambos os casos, temos a existência de um número primo diferente de p_i, $i \in \{1, 2, \ldots, n\}$. Portanto, $\mathcal{P}$ não pode ser finito. □

A seguir serão apresentadas mais duas provas do Teorema de Euclides que são, na verdade, pequenas variantes da prova apresentada acima. A primeira variante é devida a Ernst Eduard Kummer e foi feita em 1878. A segunda variante foi apresentada por Pierre René Jean Baptiste Henri Brocard em 1915.

Prova do Teorema de Euclides: Variante 1. Assuma que $\mathcal{P}$ é finito e considere

$$\mathcal{P} = \{p_1, p_2, \ldots, p_n\}.$$

Defina o número inteiro positivo

$$b = p_1 \, p_2 \, \cdots \, p_n > 2.$$

Pelo TFA, existe $p_j \in \mathcal{P}$ que divide $b - 1 > 1$. Ora, por construção, esse mesmo p_j também divide b e, portanto, também divide a diferença

$$b - (b - 1) = 1,$$

um absurdo. □

Prova do Teorema de Euclides: Variante 2. O teorema estará demonstrado se demonstrarmos que, dado $n \in \mathbb{N}$, existe um número primo $p > n$. Fixe $n \in \mathbb{N}$ arbitrário, $n > 3$. Defina o número natural

$$a_n = n! + 1 = 1 \cdot 2 \cdot 3 \cdots n + 1.$$

Note que $a_n > n$. Se a_n é primo, acabou a prova. Se a_n não é primo, pelo TFA, existe um primo p tal que $p|a_n$. Afirmamos que $p > n$. De fato, se $p \leq n$, então p é um fator de $n!$, de onde p divide

$$a_n - n! = 1,$$

um absurdo. □

A seguir, analisaremos a prova do Teorema de Euclides apresentada por Christian Goldbach. Essa prova apareceu em uma carta enviada a Euler em 1730. A ideia é bastante simples. Basta encontrar um sequência infinita de números naturais a_i

$$1 < a_0 < a_1 < \cdots < a_n < a_{n+1} < \cdots,$$

dois a dois primos entre si, isto é, sem fator primo comum. Assim, se p_i é um fator primo de a_i (TFA), $i \in \{0, 1, 2, \ldots\}$, então todos os números primos da sequência infinita

$$p_0, p_1, \ldots, p_n, \ldots$$

serão distintos.

Prova do Teorema de Euclides: Variante 3. Considere os números de Fermat

$$F_n = 2^{2^n} + 1, \quad \text{com} \quad n = 0, 1, 2, \ldots.$$

É claro que os números de Fermat formam um sequência crescente e infinita de números naturais ímpares

$$1 < F_0 < F_1 < \cdots < F_n < F_{n+1} < \cdots.$$

Basta, portanto, mostrarmos que esses números são dois a dois primos entre si. Do Exercício 2.2, para todo número natural $m \geq 1$, vale

$$F_m - 2 = F_0\, F_1 \cdots F_{m-1}. \tag{2}$$

Considere números inteiros $0 \leq n < m$, arbitrários. De (2), F_n é um fator de $F_m - 2$, logo divide $F_m - 2$. Suponha a existência de um número primo p que divida simultaneamente F_n e F_m. Ora, esse primo p divide também $F_m - 2$, pois F_n é um fator de $F_m - 2$. Portanto, esse primo p divide a diferença

$$F_m - (F_m - 2) = 2.$$

Concluímos que $p = 2$, o que é um absurdo, pois F_m é ímpar. □

Exercício 3.1. *Mostre que o número 3 divide*

$$a_n = n^3 + 2n, \qquad \forall n \in \mathbb{N}.$$

Exercício 3.2. *Considere os números de Fibonacci f_i, $i \in \mathbb{N}$, sendo*

$$f_1 = 1, \quad f_2 = 1, \quad f_{n+1} = f_n + f_{n-1}, \quad \forall n \geq 2.$$

Prove que:

- $f_1 + f_2 + \cdots + f_n = f_{n+2} - 1$, *para todo* $n \in \mathbb{N}$.
- $f_1^2 + f_2^2 + \cdots + f_n^2 = f_n f_{n+1}$, *para todo* $n \in \mathbb{N}$.

4 Teorema Fundamental da Aritmética

Em algumas das provas do Teorema de Euclides usamos de maneira essencial o Teorema Fundamental da Aritmética (veja Teorema 3.2). Sua prova será apresentada a seguir.

Prova do Teorema Fundamental da Aritmética. Considere um inteiro $n > 1$, arbitrário. Se n é um número primo, a prova acabou. Suponha, então, que n é composto. Considere o conjunto

$$S_n = \{m \in \mathbb{N} : m > 1 \text{ e } m|n\}$$

dos divisores positivos, maiores do que um, de n. O conjunto S_n é não vazio, pois n é composto. Pelo Princípio da Boa Ordem (veja Princípio 2.1), existe p_1 o menor elemento de S_n. Note que $p_1 > 1$ e é um divisor de n.
Afirmação. p_1 é um número primo.
Suponha que p_1 não é primo, isto é, p_1 é composto. Assim, existe $1 < a_1 < p_1$ que divide p_1. Ora, nesse caso, a_1 divide n, de onde $a_1 \in S_n$. Isto é um absurdo, pois p_1 é o menor elemento de S_n. Em resumo: $p_1 > 1$ é um número primo que divide n, ou seja

$$n = p_1\, n_1, \qquad n_1 \in \mathbb{N}.$$

Se n_1 é primo, a prova está completa. Se n_1 é composto, considere S_{n_1} o conjunto dos divisores positivos, maiores do que um, de n_1. Repetindo os argumentos anteriores, considere p_2 o menor elemento de S_{n_1}. Segue que p_2 é primo e

$$n = p_1\, n_1 = p_1\, p_2\, n_2, \qquad n_2 \in \mathbb{N}.$$

Repetindo este procedimento, obtemos uma sequência decrescente de inteiros positivos

$$n_1 > n_2 > \cdots > n_r > 1.$$

Como todos esses números são inteiros maiores do que um, esse procedimento termina depois de um número finito de etapas, resultando em

$$n = p_1\, p_2\, \cdots\, p_r.$$

Como os números primos na escrita acima não são necessariamente distintos, existirão

$$\alpha_1,\, \alpha_2,\, \ldots,\, \alpha_k > 0,$$

tais que

$$n = p_1^{\alpha_1}\, p_2^{\alpha_2}\, \cdots\, p_k^{\alpha_k}.$$

Com isto, está completa a prova da parte da existência. Falta mostrarmos a unicidade (a menos da ordenação) da decomposição.
A prova da unicidade (a menos da ordenação) será feita por indução. Mais precisamente, utilizaremos o Princípio da Indução - Segunda Forma (veja Princípio 2.3). Para $n = 2$ (caso base) a unicidade é imediata.
Hipótese de Indução: A unicidade (a menos da ordenação) da decomposição em um produto de números primos é verdadeira para todos os inteiros positivos n maiores do que um e menores do que k.
Queremos mostrar que a unicidade (a menos da ordenação) da decomposição em um produto de números primos é verdadeira para $n = k$.
Se k é um número primo não temos nada a provar. Suponha que k é composto e que tenha duas decomposições

$$p_1\, p_2\, \cdots\, p_s = k = q_1\, q_2\, \cdots\, q_r. \tag{3}$$

Provaremos que $s = r$ e que cada p_i no membro esquerdo é igual a algum q_j no membro direito. Isto implicará no término da prova do TFA. De (3), como p_1 divide $q_1\, q_2\, \cdots\, q_r$, segue que p_1 divide pelos menos um dos fatores q_j. Sem perda de generalidade, podemos assumir que p_1 divide q_1. Como ambos são primos, segue que $p_1 = q_1$. Como p_1 divide k, segue que $k = p_1\, \overline{k}$, com $1 < \overline{k} < k$. Podemos reescrever (3) da forma

$$p_1\, p_2\, \cdots\, p_s = k = p_1\, \overline{k} = p_1\, q_2\, \cdots\, q_r, \tag{4}$$

ou, equivalentemente

$$p_2\, \cdots\, p_s = \overline{k} = q_2\, \cdots\, q_r. \tag{5}$$

Como $1 < \overline{k} < k$, a Hipótese de Indução nos informa que as duas decomposições em (5) são idênticas (a menos da ordenação). Em particular, $s = r$. Isto implica que as duas decomposições em (4) e, portanto, em (3), são idênticas (a menos da ordenação). □

Como reconhecer que o número inteiro 337 é primo? Mais geralmente, como reconhecer que um número inteiro $n > 1$ é primo?

A maneira direta de atacar esta questão é fazer a divisão de n por inteiros menores que n. Se n for divisível por algum inteiro m, com $1 < m < n$, então n é composto. Caso contrário será primo.

Observe que, se um número primo p divide n, isto é, $n = a\,p$, com $p \leq a$, então

$$p^2 \leq a\,p = n.$$

Portanto,

$$p \leq \sqrt{n}\,.$$

Assim, para verificar se n é primo ou não basta examinar a divisibilidade de n por números primos menores ou iguais a $\sqrt{n}$.

Surge, assim, a seguinte questão: Como encontrar todos os primos menores que um dado inteiro $m > 1$?

Uma resposta a essa questão é obtida pelo Crivo ou Algoritmo de Eratóstenes. Eratóstenes foi um dos dirigentes da antiga biblioteca de Alexandria e contribuiu com descobertas em vários campos da ciência, como Astronomia, Geografia e Matemática. Seu mais famoso feito foi determinar um valor aproximado para o raio da Terra utilizando Geometria Euclidiana. Daremos a ideia do Crivo de Eratóstenes exibindo um exemplo [8].

Queremos listar os números primos menores que $m = 100$. Isto é feito eliminando os números inteiros maiores que 1 com divisores primos até

$$\sqrt{m} = \sqrt{100} = 10,$$

ou seja, múltiplos de

$$2,\ 3,\ 5 \text{ e } 7.$$

Os números restantes depois desse processo iterativo são exatamente os números primos menores que $m = 100$. Veja a sequência das Figuras 1 a 6.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Figura 1: Listar os números de 2 a 100.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Figura 2: Retirar os múltiplos de 2 (amarelo).

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Figura 3: Retirar os múltiplos de 3 ainda não retirados (verde).

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Figura 4: Retirar os múltiplos de 5 ainda não retirados (rosa).

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Figura 5: Retirar os múltiplos de 7 ainda não retirados (azul).

	2	3		5		7			
11		13				17		19	
		23						29	
31						37			
41		43				47			
		53						59	
61						67			
71		73						79	
		83						89	
						97			

Figura 6: Os números restantes são primos.

Voltemos à pergunta anterior: Como reconhecer que 337 é primo?

Para saber se o número inteiro 337 é primo, basta encontrar os números primos menores ou iguais a $\sqrt{337}$ e verificar se algum deles divide 337. Como

$$18^2 = 324 < 337 < 361 = 19^2,$$

devemos analisar os primos menores que 18. Do exemplo anterior, a lista dos números primos menores que 18 (veja a Figura 6) é

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17.$$

Como nenhum deles divide 337, segue que este número é primo.

Exercício 4.1. *Uma sequência ou progressão aritmética (de números inteiros positivos) é uma sequência, finita ou não, de números inteiros positivos que aumenta a cada passo por uma diferença comum. Por exemplo, os números primos*

$$3,\ 7,\ 11,$$

formam uma sequência aritmética de três primos. A diferença comum, neste caso, é 4. *Dê um exemplo de uma sequência aritmética de* 5 *primos.*

Exercício 4.2. *Definição de número primo em $\mathbb{Z}$: um número inteiro n é primo se n é diferente de 0, 1 e -1 e os seus únicos fatores inteiros são n, seu oposto $-n$, 1 e -1. Com esta definição, pode-se mostrar que todo número inteiro diferente de 0, 1 e -1 pode ser fatorado num produto de números primos. Mostre, no entanto, que, neste caso, essa fatoração pode não ser única, ou seja, fatores primos em duas fatorações podem ser distintos.*

5 Números primos em conjuntos de termos de progressões aritméticas

Nesta seção, discutiremos a existência de números primos em conjuntos de termos de progressões aritméticas. Para fixar as ideias e as notações, considere o seguinte conjunto

$$\begin{aligned} S &= \{n \in \mathbb{N} : n = 4k + 3,\ k \in \mathbb{N} \cup \{0\}\} \\ &= \{3,\ 7,\ 11,\ 15,\ 19,\ 23,\ 27,\ 31,\ 35, \ldots\}, \end{aligned}$$

ou seja, S é o conjunto dos termos da progressão arimética de razão 4 e de primeiro termo $n = 3$.

Notemos que os números

$$3,\ 7,\ 11,\ 19,\ 23,\ 31 \in S$$

são números primos. Considere o seguinte conjunto

$$\mathcal{P}_S = \{n \in S : n \text{ é número primo}\}.$$

A seguinte pergunta é imediata.

Pergunta 5.1. *O conjunto $\mathcal{P}_S$ é finito ou infinito?*

Mostraremos que $\mathcal{P}_S$ é infinito, ou seja, existem infinitos números primos dentre os termos da progressão aritmética $4k + 3$, $k \in \mathbb{N} \cup \{0\}$.

Esse resultado, aparentemente simples, é surpreendente: mostra a existência de infinitos números primos que são escritos em uma forma especial.

Teorema 5.1. *O conjunto $\mathcal{P}_S$ é infinito.*

Demonstração. Queremos provar que existem infinitos primos da forma $4k+3$. Dado um inteiro positivo m, pelo Algoritmo da Divisão (Teorema 2.1), os possíveis restos da divisão de m por 4 são: 0, 1, 2 e 3. Segue que um número primo $p \neq 2$ é da forma $4q + 1$ ou $4q + 3$, visto que os números da forma $4q = 4q + 0$ e $4q + 2$ são pares.

Suponha a existência de somente um número finito de primos da forma $4k+3$. Sejam $p_1, p_2, \ldots, p_r$ esses primos, ou seja,

$$p_1 = 4k_1 + 3,\ p_2 = 4k_2 + 3,\ \ldots,\ p_r = 4k_r + 3,$$

sendo $k_1,\ k_2, \ldots,\ k_r$ inteiros positivos. Defina

$$N = 4\,p_1\,p_2 \cdots p_r - 1.$$

É imediato que cada p_i, $i = 1, 2, \ldots, r$ não divide N. Note que

$$\begin{aligned} N &= 4\,p_1\,p_2 \cdots p_r - 1 + (-3+3) = 4(p_1\,p_2 \cdots p_r - 1) + 3 \\ &= 4q + 3. \end{aligned}$$

Por construção, $N > p_i$, para todo $i = 1, 2, \ldots, r$. Temos duas possibilidades: N é primo ou N é composto. Se N é primo, acabou, pois N é da forma $N = 4q + 3$, com $q \in \mathbb{N}$, ou seja, $N \in S$, mas é diferente de p_i, para todo $i = 1, 2, \ldots, r$. Se N é composto, pelo TFA, N possui um divisor primo. Afirmamos que algum divisor primo de N tem que ser da forma $4s + 3$, $s \in \mathbb{N}$. De fato, se todo divisor primo de N for da forma $4j + 1$, $j \in \mathbb{N}$, segue que N terá a forma $N = 4t + 1$, $t \in \mathbb{N}$, contrariando a escrita de N. Assim, esse divisor primo $p = 4s+3 \in S$ e é diferente de p_i, para todo $i = 1, 2, \ldots, r$, terminando a prova do teorema. □

Imitando a demonstração acima, podemos provar que existem infinitos primos da forma

$$6k + 5, \qquad k \in \mathbb{N} \cup \{0\},$$

ou seja, o conjunto

$$T = \{n \in \mathbb{N} : n = 6k + 5,\ k \in \mathbb{N} \cup \{0\}\}$$

dos termos da progressão aritmética acima contém infinitos números primos. De fato, pode-se provar o seguinte teorema, devido ao matemático Peter Gustav Lejeune Dirichlet (1805-1859).

Teorema 5.2 (Dirichlet)**.** *Considere a e b inteiros positivos primos entre si, isto é, $(a, b) = 1$. O conjunto*

$$L = \{n \in \mathbb{N} : n = ak + b,\ k \in \mathbb{N} \cup \{0\}\}$$

contém infinitos números primos.

O Teorema de Dirichlet sobre "números primos em progressões aritméticas" é uma jóia da Teoria dos Números. Grande parte de sua beleza está na simplicidade do seu enunciado. Um estudante do ensino médio conhece matemática suficiente para entender a formulação do teorema. No entanto, muitas idéias profundas de Álgebra e Análise são necessárias para prová-lo. Veja uma prova em [10].

O estudo dos "números primos em progressões aritméticas" motivou o nascimento da Teoria Analítica dos Números, ramo de prestígio e em desenvolvimento na Teoria dos Números.

Progressão aritmética	Os 10 primeiros de infinitos números primos
$2n+1$	$3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \ldots$
$4n+1$	$5, 13, 17, 29, 37, 41, 53, 61, 73, 89, \ldots$
$4n+3$	$3, 7, 11, 19, 23, 31, 43, 47, 59, 67, \ldots$
$6n+1$	$7, 13, 19, 31, 37, 43, 61, 67, 73, 79, \ldots$
$6n+5$	$5, 11, 17, 23, 29, 41, 47, 53, 59, 71, \ldots$
$8n+1$	$17, 41, 73, 89, 97, 113, 137, 193, 233, 241, \ldots$
$8n+3$	$3, 11, 19, 43, 59, 67, 83, 107, 131, 139, \ldots$
$8n+5$	$5, 13, 29, 37, 53, 61, 101, 109, 149, 157, \ldots$
$8n+7$	$7, 23, 31, 47, 71, 79, 103, 127, 151, 167, \ldots$
$10n+1$	$11, 31, 41, 61, 71, 101, 131, 151, 181, 191, \ldots$
$10n+3$	$3, 13, 23, 43, 53, 73, 83, 103, 113, 163, \ldots$
$10n+7$	$7, 17, 37, 47, 67, 97, 107, 127, 137, 157, \ldots$
$10n+9$	$19, 29, 59, 79, 89, 109, 139, 149, 179, 199, \ldots$
$12n+1$	$13, 37, 61, 73, 97, 109, 157, 181, 193, 229, \ldots$
$12n+5$	$5, 17, 29, 41, 53, 89, 101, 113, 137, 149, \ldots$
$12n+7$	$7, 19, 31, 43, 67, 79, 103, 127, 139, 151, \ldots$
$12n+11$	$11, 23, 47, 59, 71, 83, 107, 131, 167, 179, \ldots$

Tabela 1: Dez primeiros números primos em algumas progressões aritméticas.

Na Tabela 1 são apresentados os dez primeiros números primos em algumas progressões aritméticas. Esta tabela pode ser acessada em: https://en.wikipedia.org/wiki/Dirichlet%27s_theorem_on_arithmetic_progressions.

Utilizaremos o Teorema de Euclides e o Teorema de Dirichlet para demonstrar o teorema seguinte devido ao matemático polonês Waclaw Franciszek Sierpinski (1882-1969).

Teorema 5.3 (Sierpinski). *Dado um inteiro $m > 1$, existe um número primo p^* tal que*

$$p^* \pm 1, p^* \pm 2, \ldots, p^* \pm m$$

são números inteiros compostos.

Em outras palavras, dado $m > 1$, existe um número primo p^* "isolado" por m números compostos de "cada lado".

Demonstração. Fixe $m > 1$ arbitrário. Pelo Teorema de Euclides, existe um número primo q maior do que m. Defina o número inteiro positivo

$$a = (q+1) \cdot (q+2) \cdots (q+m).$$

Afirmação 1. *Os números a e q são relativamente primos, isto é, $(a, q) = 1$.*

De fato, como $a > q$ e q é primo, se q divide a, então q divide $q + i$, para algum $1 \leq i \leq m < q$. Ora, mas neste caso, q divide i, o que é um

absurdo. Isto completa a prova da Afirmação 1. Pelo Teorema de Dirichlet, a progressão aritmética

$$\{n \in \mathbb{N} : n = a\,k + q,\ k \in \mathbb{N} \cup \{0\}\},$$

contém infinitos números primos. Considere um desses números primos, ou seja, tome $k_0 \in \mathbb{N} \cup \{0\}$ tal que

$$p = a\,k_0 + q = ((q+1)\cdot(q+2)\cdots(q+m))\cdot k_0 + q$$

é um número primo. Segue da nossa construção que

$$\begin{aligned} p+1 &= (q+1)\cdot(q+2)\cdots(q+m)\cdot k_0 + (q+1),\\ p+2 &= (q+1)\cdot(q+2)\cdots(q+m)\cdot k_0 + (q+2),\\ &\vdots\\ p+m &= (q+1)\cdot(q+2)\cdots(q+m)\cdot k_0 + (q+m), \end{aligned}$$

são números compostos. Como $q > m$, considere, agora, o número inteiro positivo

$$a^* = (q-m)\cdot(q-(m-1))\cdots(q-1)\cdot\underbrace{(q+1)\cdot(q+2)\cdots(q+m)}_{a}.$$

Afirmação 2. *Os números a^* e q são relativamente primos.*

A prova da Afirmação 2 é exatamente a mesma da Afirmação 1. Pelo Teorema de Dirichlet, a progressão aritmética

$$\{n \in \mathbb{N} : n = a^*\,k + q,\ k \in \mathbb{N} \cup \{0\}\},$$

contém infinitos números primos. Considere um desses números primos, ou seja, tome $k^* \in \mathbb{N} \cup \{0\}$ tal que

$$p^* = a^*\,k^* + q$$

é um número primo. Por construção, os números

$$\begin{aligned} p^* - m &= a^*\,k^* + (q-m),\\ &\vdots\\ p^* - 1 &= a^*\,k^* + (q-1),\\ p^* + 1 &= a^*\,k^* + (q+1),\\ &\vdots\\ p^* + m &= a^*\,k^* + (q+m), \end{aligned}$$

são compostos, terminando a prova do teorema. □

Exercício 5.1. *Prove que existem infinitos primos da forma*

$$6k+5, \qquad k \in \mathbb{N} \cup \{0\},$$

ou seja, o conjunto

$$T = \{n \in \mathbb{N} : n = 6k+5,\ k \in \mathbb{N} \cup \{0\}\}$$

dos termos da progressão aritmética acima contém infinitos números primos.

Exercício 5.2. *Pode-se mostrar (Teorema de Fermat) que os números primos da forma*

$$p = 4k+1, \quad k \in \mathbb{N},$$

podem ser escritos como a soma de dois quadrados de números inteiros positivos, isto é,

$$p = a^2 + b^2, \quad a, b \in \mathbb{N}.$$

Assumindo o Teorema de Fermat, mostre que um tal primo é a hipotenusa de um triângulo retângulo cujos catetos são números inteiros positivos.

6 Distribuição e espaçamento de números primos

Nesta seção, discutiremos um pouco mais sobre a distribuição e o espaçamento de números primos, além de discutirmos um pouco a respeito dos primos gêmeos.

O primeiro resultado informa que existem "saltos" arbitrariamente grandes na sequência dos números primos.

Teorema 6.1. *Para qualquer inteiro $m > 1$, existem m inteiros positivos compostos consecutivos.*

A prova a seguir é construtiva, no sentido de exibirmos quais são os m inteiros positivos compostos consecutivos, para cada $m > 1$ dado.

Demonstração. Fixe, arbitrariamente, um inteiro $m > 1$. Considere os m números inteiros consecutivos:

$$(m+1)!+2,\ (m+1)!+3,\ (m+1)!+4, \ldots,\ (m+1)!+m+1.$$

É simples verificar que

- $(m+1)!+2$ é divisível por 2, logo é um número composto,
- $(m+1)!+3$ é divisível por 3, logo é um número composto,
- $\vdots$
- $(m+1)!+m+1$ é divisível por $m+1$, logo é um número composto.

Assim, os m números inteiros acima são compostos, terminando a prova do teorema. □

Exemplo 6.1. *Considere $m = 6$. Os números inteiros consecutivos*

$$(6+1)!+2,\ (6+1)!+3,\ (6+1)!+4,\ (6+1)!+5,\ (6+1)!+6,\ (6+1)!+7,$$

ou seja,

$$5042,\ 5043,\ 5044,\ 5045,\ 5046,\ 5047,$$

são divisíveis, respectivamente, por

$$2,\ 3,\ 4,\ 5,\ 6,\ 7,$$

são números compostos.

Mais à frente, discutiremos com mais profundidade o conhecido Postulado de Bertrand. Em 1845, Bertrand postulou que, para todo $n \geq 1$, existe um número primo entre n e $2n$. Ele verificou essa afirmação para todo $n < 3 \times 10^6$. Em 1850, Tchebychev deu uma prova para esse postulado.

Teorema 6.2. *Para todo inteiro $n \geq 1$, existe um número primo p tal que*

$$n \leq p \leq 2n.$$

Um par de números primos cuja diferença é igual a 2 é chamado de *primos gêmeos*. Denotaremos esse par por

$$\{p, p+2\}.$$

Alguns exemplos de primos gêmeos:

$$\{3,5\},\ \{5,7\},\ \{11,13\},\ \{17,19\},\ \{29,31\},\ \{41,43\}.$$

Examinemos com mais atenção os primos gêmeos acima.

Observe que

$$\begin{aligned}
5 &= 6\cdot 1 - 1 \quad \text{e} \quad 7 = 6\cdot 1 + 1,\\
11 &= 6\cdot 2 - 1 \quad \text{e} \quad 13 = 6\cdot 2 + 1,\\
17 &= 6\cdot 3 - 1 \quad \text{e} \quad 19 = 6\cdot 3 + 1,\\
29 &= 6\cdot 5 - 1 \quad \text{e} \quad 31 = 6\cdot 5 + 1,\\
41 &= 6\cdot 7 - 1 \quad \text{e} \quad 43 = 6\cdot 7 + 1.
\end{aligned}$$

Coincidência? É claro que não.

Considere um número inteiro positivo n. Pelo Teorema da Divisão (Teorema 2.1), os possíveis restos da divisão de n por 6 são:

$$0,\ 1,\ 2,\ 3,\ 4,\ 5.$$

Segue, imediatamente, que, se o resto da divisão de n por 6 for

$$0,\ 2,\ \text{ou } 4,$$

então n é par e, se o resto da divisão de n por 6 for 3, então n é múltiplo de 3. Deste modo, se $p > 3$ é um número primo, então as únicas possibilidades dos restos da divisão de p por 6 são: 1 e 5, ou seja,

$$p = 6 \cdot k + 1, \qquad k \in \mathbb{N},$$

ou

$$p = 6 \cdot \overline{k} + 5 = 6 \cdot \overline{k} + 5 + (1 - 1) = 6 \cdot \overline{k} + 6 - 1 = 6 \cdot (\overline{k} + 1) - 1 \\ = 6 \cdot \hat{k} - 1, \quad \hat{k} \in \mathbb{N}.$$

Portanto, todo par de números primos gêmeos, diferente de $\{3, 5\}$, tem a forma

$$\{6 \cdot k - 1, 6 \cdot k + 1\}, \quad \text{para algum} \quad k \in \mathbb{N},$$

ou seja, o número composto entre dois primos gêmeos é múltiplo de 6.

Uma das importantes questões em aberto na Teoria dos Números é a seguinte.

Conjectura 6.1 (Conjectura dos primos gêmeos)**.** *Existem infinitos pares de números primos gêmeos.*

Uma conjectura mais geral é a seguinte.

Conjectura 6.2 (Conjectura de Polignac)**.** *Para todo número inteiro positivo k, existem infinitos números primos p tais que $p + 2k$ também é primo.*

Se $k = 1$, então as duas conjecturas coincidem. As duas conjecturas continuam sendo conjecturas, embora alguns avanços tenham ocorrido.

No artigo [4] foi provado que existem infinitos números primos p tais que $p + 2$ tem no máximo dois fatores primos. Em [17] foi publicada a prova de que, para algum inteiro positivo n menor que 70 milhões, existem infinitos pares de primos que diferem por n. Posteriormente, num esforço conjunto liderado por Terence Tao e James Maynard, essa cota baixou para 246, veja [11] e [13].

Algumas curiosidades. Até setembro de 2018, o maior par de primos gêmeos conhecido era

$$2.996.863.034.895 \times 2^{1.290.000} \pm 1.$$

Existem

$$808.675.888.577.436$$

números primos gêmeos menores que 10^{18}.

Finalizaremos esta seção com mais uma prova de que o conjunto dos números primos é infinito.

Considere os números de Fibonacci f_i, $i \in \mathbb{N}$, sendo

$$f_1 = 1,\ f_2 = 1,\ f_{n+1} = f_n + f_{n-1}, \quad \forall n \geq 2.$$

Veja Exercício 3.2. Os vinte primeiros números de Fibonacci são:

$$\begin{array}{lllll} f_1 = 1, & f_2 = 1, & f_3 = 2, & f_4 = 3, & f_5 = 5, \\ f_6 = 8, & f_7 = 13, & f_8 = 21, & f_9 = 34, & f_{10} = 55, \\ f_{11} = 89, & f_{12} = 144, & f_{13} = 233, & f_{14} = 377, & f_{15} = 610, \\ f_{16} = 987, & f_{17} = 1597, & f_{18} = 2584, & f_{19} = 4181, & f_{20} = 6765. \end{array}$$

Pode-se mostrar que

$$(f_m, f_n) = f_{(m,n)}, \quad \forall m, n \in \mathbb{N}, \tag{6}$$

sendo (a, b) o máximo divisor comum dos números inteiros positivos a e b.

Prova do Teorema de Euclides. Suponha que o conjunto dos números primos é finito. Sejam

$$p_1,\ p_2, \ldots,\ p_k$$

esses k números primos. Construa os correspondentes k números de Fibonacci

$$f_{p_1},\ f_{p_2}, \ldots,\ f_{p_k}. \tag{7}$$

Considere $i, j \in \{1, 2, \ldots, k\}$ com $i \neq j$. Utilizando (6), vem

$$\left(f_{p_i}, f_{p_j}\right) = f_{(p_i, p_j)} = f_1 = 1.$$

Desta última análise, segue que os números de Fibonacci em (7) são 2 a 2 relativamente primos. Como temos k números primos e k números de Fibonacci 2 a 2 relativamente primos, segue que cada um desses números de Fibonacci tem exatamente um fator primo. No entanto, o número de Fibonacci

$$f_{19} = 4181 = 37 \cdot 113,$$

sendo 37 e 113 números primos, um absurdo. □

Exercício 6.1. *Use o Teorema de Dirichlet (Teorema 5.2) para provar que existem infinitos números primos que não pertencem a qualquer par de primos gêmeos. Em outras palavras, existem infinitos números primos p tais que $p + 2$ e $p - 2$ não são números primos.*

7 Algumas fórmulas para números primos

As questões que serão discutidas nesta seção são as seguintes.

Pergunta 7.1. *Existem fórmulas que fornecem só números primos? Existem fórmulas que fornecem todos os números primos? Existem fórmulas que fornecem todos os números primos e somente números primos?*

Certamente estas perguntas são importantes e merecem nossa atenção. Uma das fórmulas estudadas para fornecer números primos é a que aparece no polinômio de Euler

$$P(n) = n^2 - n + 41, \qquad n \in \mathbb{N}. \tag{8}$$

É imediato que

- $P(1) = 1^2 - 1 + 41 = 41$ é um número primo,
- $P(2) = 2^2 - 2 + 41 = 43$ é um número primo,
- $P(3) = 3^2 - 3 + 41 = 47$ é um número primo,
- $\vdots$
- $P(40) = (40)^2 - 40 + 41 = 1601$ é um número primo.

No entanto,

$$P(41) = (41)^2 - 41 + 41 = (41)^2$$

não é um número primo.

É comum lermos ou escutarmos que não existe um fórmula que forneça todos os números primos e somente os números primos. O próximo teorema informa-nos que a afirmação acima é falsa [16].

Denotaremos por $\mathbb{Z}_{\geq 0}$ o conjunto dos inteiros não negativos, por $\mathbb{N}$ o conjunto dos inteiros positivos e por $\mathcal{P}$ o conjunto dos números primos.

Teorema 7.1. *Considere $n \in \mathbb{Z}_{\geq 0}$ e $m \in \mathbb{N}$. Defina o número inteiro*

$$a = n(m+1) - (m! + 1)$$

e considere $f : \mathbb{Z}_{\geq 0} \times \mathbb{N} \longrightarrow \mathcal{P}$, dada por

$$f(n,m) = \frac{m-1}{2}\Big(\big|a^2 - 1\big| - \big(a^2 - 1\big)\Big) + 2. \tag{9}$$

Então, as seguintes afirmações são verdadeiras:

(i) *A função f está bem definida.*

(ii) *A função f é sobrejetora.*

Na prova abaixo do Teorema 7.1 faremos uso do seguinte resultado, conhecido como Teorema de Wilson:

$$p > 1 \text{ é primo} \iff p \,|\, (p-1)! + 1.$$

Demonstração. **Afirmação (i).** A função f está bem definida, ou seja, o número $f(n,m)$ é um número primo, para todo n inteiro não negativo e para todo m inteiro positivo. Sendo a um número inteiro, então a^2 é um número inteiro. Separaremos em dois casos: $a^2 \geq 1$ e $a^2 = 0$.

Caso 1. Se $a^2 \geq 1$, então $\left|a^2 - 1\right| = a^2 - 1$, o que implica que $f(n,m) = 2$, que é um número primo.

Caso 2. Se $a^2 = 0$, então, $a = 0$ e, da definição de a, vem

$$n(m+1) = m! + 1. \tag{10}$$

Tomando $a = 0$ na definição de f resulta

$$f(n,m) = m + 1. \tag{11}$$

Ora, das equações (10) e (11) resulta que

$$f(n,m) = m + 1 \,|\, m! + 1.$$

Utilizando o Teorema de Wilson, com $p = f(n,m) = m+1$, concluímos que $f(n,m)$ é um número primo. Dos Casos 1 e 2, concluimos que f está bem definida.

Afirmação (ii). A função f é sobrejetora. Considere um número primo $p \in \mathcal{P}$ arbitrário e fixado. Queremos mostrar que existem $n \in \mathbb{Z}_{\geq 0}$ e $m \in \mathbb{N}$ tais que $f(n,m) = p$. Como p é primo, pelo Teorema de Wilson, existe $n \in \mathbb{N}$ tal que

$$(p-1)! + 1 = n\,p.$$

Denote

$$n = \frac{(p-1)! + 1}{p}$$

e considere $m = p - 1$. Com essas escolhas,

$$\begin{aligned} a = n(m+1) - (m! + 1) &= \frac{(p-1)! + 1}{p}(p - 1 + 1) - ((p-1)! + 1) \\ &= (p-1)! + 1 - ((p-1)! + 1) = 0. \end{aligned}$$

Assim,

$$f(n,m) = m - 1 + 2 = m + 1 = (p-1) + 1 = p.$$

Isso conclui a prova da Afirmação (ii), terminando a demonstração do teorema. □

Embora a expressão de f seja relativamente simples e o Teorema 7.1 tenha lá o seu charme, na verdade esse tipo de resultado não ajuda em nada, pois, por um lado, a "fórmula" f não é "eficiente", no sentido de gerar números primos "distintos", nem ajuda a responder questões teóricas importantes, como, por exemplo, questões sobre distribuições de números primos.

A título de curiosidade, faça o seguinte exercício: fixe $n \in \mathbb{Z}_{\geq 0}$ e calcule os valores de $f(n,m)$ para uma sequência arbitrária de valores de m, por exemplo, $m \in \{2,\ 4,\ 6,\ \ldots,\ 30\}$. Alguma surpresa?

No próximo teorema utilizaremos técnicas da Análise Real para obtermos informações sobre números primos, veja [6].

Para $x \in \mathbb{R}$, denotaremos por

$$\lfloor x \rfloor$$

a parte inteira do número x. Denotaremos por p_n, $n \in \mathbb{N}$, o n-ésimo número primo. Deste modo,

$$p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ p_4 = 7,\ \ldots.$$

Faremos uso, ainda, do seguinte resultado: existe uma constante $k > 0$ tal que

$$p_{n+1} - p_n < k\, p_n^{5/8}, \qquad \forall n \in \mathbb{N}. \tag{12}$$

Teorema 7.2. *Existe $\theta \in \mathbb{R}$ tal que*

$$\left\lfloor \theta^{3^n} \right\rfloor \tag{13}$$

é um número primo, para todo $n \in \mathbb{N}$.

Demonstração. Se $N \in \mathbb{N}$ é tal que

$$N > k^8 \tag{14}$$

e p_n é o maior número primo menor que N^3, então

$$p_n < N^3 < p_{n+1} \overset{(12)}{<} p_n + k\, p_n^{5/8} \overset{(14)}{<} N^3 + N^{1/8}(N^3)^{5/8} < N^3 + N^2 < (N+1)^3 - 1.$$

Da análise anterior, concluímos: dado um inteiro $N > k^8$, existe um número primo p tal que

$$N^3 < p < (N+1)^3 - 1.$$

Construa, recursivamente, uma sequência de números primos $(q_n)_{n \in \mathbb{N}}$ da seguinte forma:

- q_1 é um número primo satisfazendo $q_1 > k^8$.
- Para $n \geq 1$, q_{n+1} é um número primo satisfazendo

$$q_n^3 < q_{n+1} < (q_n + 1)^3 - 1, \tag{15}$$

sendo, por definição, q_{n+1} o menor número primo satisfazendo essas desigualdades.

Da sequência $(q_n)_{n\in\mathbb{N}}$ construímos outras duas sequências, denotadas por $(u_n)_{n\in\mathbb{N}}$ e $(v_n)_{n\in\mathbb{N}}$, definidas por:

$$u_n = q_n^{3^{-n}}, \; v_n = (q_n + 1)^{3^{-n}}, \quad \forall n \in \mathbb{N}. \tag{16}$$

Afirmação. A sequência $(u_n)_{n\in\mathbb{N}}$ é crescente e a sequência $(v_n)_{n\in\mathbb{N}}$ é decrescente.

De fato, para todo $n \in \mathbb{N}$, valem

$$\begin{aligned} u_{n+1} &= (q_{n+1})^{3^{-n-1}} \overset{(15)}{>} \left(q_n^3\right)^{3^{-n-1}} = q_n^{3^{-n}} = u_n, \\ v_{n+1} &= (q_{n+1} + 1)^{3^{-n-1}} \overset{(15)}{<} \left(\left((q_n + 1)^3 - 1\right) + 1\right)^{3^{-n-1}} \\ &= (q_n + 1)^{3^{-n}} = v_n. \end{aligned}$$

Das definições das sequências $(u_n)_{n\in\mathbb{N}}$ e $(v_n)_{n\in\mathbb{N}}$ seguem que

$$u_n < v_n, \qquad \forall n \in \mathbb{N}.$$

Dessa desigualdade e das desigualdades das monotonicidades das sequências $(u_n)_{n\in\mathbb{N}}$ e $(v_n)_{n\in\mathbb{N}}$, resulta, finalmente

$$u_n < u_{n+1} < v_{n+1} < v_n, \qquad \forall n \in \mathbb{N}.$$

Logo, ambas as sequências são monótonas e limitadas, portanto, convergentes. Denote por

$$\theta = \lim_{n\to\infty} u_n \quad \text{e} \quad \phi = \lim_{n\to\infty} v_n.$$

Das nossas análises, resulta

$$u_n < \theta \leq \phi < v_n, \quad \forall n \in \mathbb{N},$$

de onde

$$u_n^{3^n} < \theta^{3^n} \leq \phi^{3^n} < v_n^{3^n}, \quad \forall n \in \mathbb{N},$$

ou seja,

$$q_n < \theta^{3^n} < q_n + 1, \quad \forall n \in \mathbb{N}.$$

Isto implica que

$$\left\lfloor \theta^{3^n} \right\rfloor = q_n, \quad \forall n \in \mathbb{N},$$

como queríamos demonstrar. □

Exercício 7.1. *Prove a seguinte implicação no Teorema de Wilson:*

$$p > 1,\ p \,|\, (p-1)! + 1 \quad \Longrightarrow \quad p \text{ é primo.}$$

Exercício 7.2. *Considere p, p_1, p_2 e p_3 números primos. Suponha que*

$$p = (p_1)^2 + (p_2)^2 + (p_3)^2.$$

Mostre que um dos primos p_1, p_2 ou p_3 é igual a 3.

8 Postulado de Bertrand, parte 1

Em 1845, Bertrand postulou que, para todo $n \geq 1$, existe um número primo entre n e $2n$. Ele verificou essa afirmação para todo $n < 3 \times 10^6$. Em 1850, Tchebychev deu uma prova para esse postulado [2].

Teorema 8.1 (Postulado de Bertrand)**.** *Para todo inteiro $n \geq 1$, existe um número primo p tal que*

$$n \leq p \leq 2n.$$

Para a prova do Teorema 8.1 precisamos de alguns preliminares. Recordemos, primeiramente, o coeficiente binomial. Considere $m, n \in \mathbb{N}$ com $m \geq n$. O *coeficiente binomial* definido por m e n é o número inteiro positivo

$$\binom{m}{n} = \frac{m!}{n!\,(m-n)!}.$$

Dado um numero real $x > 0$, denotaremos por

$$\prod_{p \leq x} p$$

o produto dos números primos $p \leq x$.

Lema 8.1. *Para todo $n \in \mathbb{N}$, temos*

$$\binom{2n}{n} > \frac{2^{2n}}{2n}. \tag{17}$$

Demonstração. A prova deve ser feita por indução. Aqui, daremos uma ideia de que a desigualdade (17) é verdadeira. Observe que

$$\begin{aligned}
\binom{2n}{n} = \frac{(2n)!}{n!\,n!} &= \frac{1 \cdot 2 \cdot 3 \cdot 4 \cdots n \cdot (n+1) \cdots (2n-1) \cdot (2n)}{1 \cdot 2 \cdot 3 \cdot 4 \cdots n \cdot n!} \\
&= 2^n \frac{3 \cdot 5 \cdots (2n-1)}{n!} > 2^n \frac{2 \cdot 4 \cdots (2n-2)}{n!} \\
&= 2^n \frac{2 \cdot 4 \cdots (2n-2)}{1 \cdot 2 \cdots (n-1) \cdot n} \\
&= \frac{2^n (2^{n-1})}{n} = \frac{2^{2n-1}}{n} = \frac{2^{2n}}{2n}.
\end{aligned}$$

□

Lema 8.2. *Para todo número real $x > 1$, vale*

$$\prod_{p \leq x} p \leq 4^x. \tag{18}$$

Demonstração. É suficiente mostrarmos que, para todo $n \in \mathbb{N}$, vale

$$\prod_{p \leq n} p \leq 4^n. \tag{19}$$

De fato, suponha (19) verdadeira. Dado $x > 1$, tome $n = \lfloor x \rfloor$. Assim,

$$\prod_{p \leq x} p = \prod_{p \leq n} p \leq 4^n \leq 4^x.$$

Faremos a prova de (19) por indução em n. Note que ela é imediata para $n = 1$ e $n = 2$.
Fixe arbitrariamente $n \geq 3$ e considere a seguinte Hipótese de Indução (HI): A desigualdade (19) é verdadeira para todo $k < n$. Queremos mostrar que ela é verdadeira para n.
Caso 1. n é par. Assim,

$$\prod_{p \leq n} p = \prod_{p \leq n-1} p \overset{(HI)}{\leq} 4^{n-1} < 4^n.$$

Caso 2. n é ímpar, ou seja, $n = 2k + 1$. Como $k + 1 < n$, pela HI, temos

$$\prod_{p \leq k+1} p \leq 4^{k+1}. \tag{20}$$

Observe que

$$\binom{2k+1}{k} = \frac{(2k+1)!}{k!\,(k+1)!} = \frac{(k+2)\cdots(2k)\cdot(2k+1)}{1 \cdot 2 \cdots k},$$

implicando em

$$\prod_{k+2 \leq p \leq 2k+1} p \leq \binom{2k+1}{k}. \tag{21}$$

$$\begin{aligned}
\binom{2k+1}{k} = \frac{(2k+1)!}{k!\,(k+1)!} &= \frac{1 \cdot 2 \cdot 3 \cdot 4 \cdots (2k) \cdot (2k+1)}{1 \cdot 2 \cdot 3 \cdot 4 \cdots k \cdot (k+1)!} \\
&= 2^k \frac{3 \cdot 5 \cdots (2k+1)}{(k+1)!} < 2^k \frac{4 \cdot 6 \cdots (2k+2)}{(k+1)!} \\
&= 2^k \frac{4 \cdot 6 \cdots (2k+2)}{1 \cdot 2 \cdots k \cdot (k+1)} \\
&= 2^k \cdot 2^k = 4^k.
\end{aligned} \tag{22}$$

Deste modo,

$$\prod_{p\leq n=2k+1} p = \prod_{p\leq k+1} p \cdot \prod_{k+2\leq p\leq 2k+1} p$$

$$\overset{(20)}{<} 4^{k+1} \cdot \prod_{k+2\leq p\leq 2k+1} p$$

$$\overset{(21)}{\leq} 4^{k+1} \cdot \binom{2k+1}{k} \overset{(22)}{<} 4^{k+1} \cdot 4^k = 4^{2k+1}.$$

Dos Casos 1 e 2, concluímos a prova do lema. □

A prova do próximo lema será omitida e ficará como exercício. Veja a Figura 7.

Lema 8.3. *Para todo número real $x \geq 10$, vale*

$$2^x > x^3. \tag{23}$$

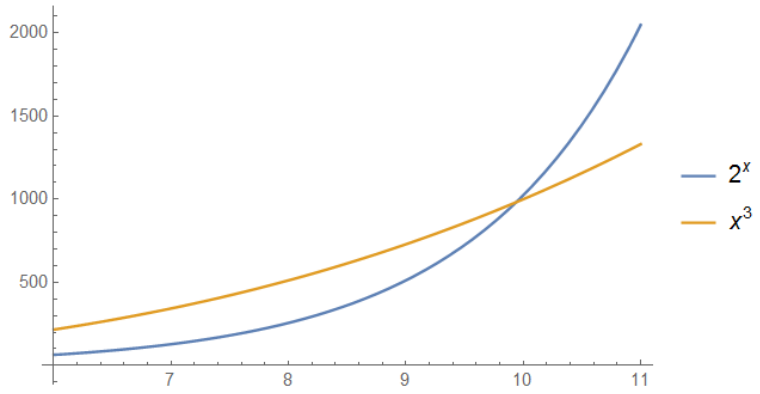

Figura 7: Ilustração dos gráficos de 2^x e x^3.

A prova do próximo lema também será omitida.

Lema 8.4. *Considere $n \in \mathbb{N}$ e p um número primo. Suponha que exista $\theta_p \in \mathbb{Z}_{\geq 0}$ tal que*

$$p^{\theta_p} \leq 2n < p^{\theta_p+1}.$$

Então, o expoente da maior potência de p que divide o coeficiente binomial

$$\binom{2n}{n}$$

é menor ou igual a θ_p.

Em particular, se $p > \sqrt{2n}$, então o expoente dessa máxima potência de p é menor ou igual a 1. De fato,

$$\sqrt{2n} < p \implies 2n < p^2 \implies \theta_p + 1 = 2 \implies \theta_p = 1. \tag{24}$$

Prova do Teorema 6.2. A prova estará concluída se mostrarmos que

$$\prod_{n+1 \leq p \leq 2n} p > 1.$$

Como

$$\binom{2n}{n} = \frac{(2n)!}{n!\,n!} = \frac{(n+1)\cdot(n+2)\cdots 2n}{1\cdot 2\cdots n}, \tag{25}$$

segue que os números primos entre $n+1$ e $2n$, se existirem, dividem o coeficiente binomial (25). Além disto, qualquer primo divisor deste coeficiente binomial é menor que $2n$. Pelo Teorema Fundamental da Aritmética, podemos escrever

$$\binom{2n}{n} = f_1 \cdot f_2 \cdot f_3, \tag{26}$$

sendo

$$f_1 = \prod_{p_i \leq \sqrt{2n}} p_i^{\alpha_i}, \quad f_2 \overset{(24)}{=} \prod_{\sqrt{2n} < p_j \leq n} p_j, \quad f_3 \overset{(24)}{=} \prod_{n < p_k \leq 2n} p_k.$$

Para todo número real $x > 0$, defina $\Pi(x)$ como o número de primos menores que x. Deste modo,

$$f_1 \leq (2n)^{\Pi(\sqrt{2n})}. \tag{27}$$

Considere um número primo p satisfazendo

$$\frac{2n}{3} < p \leq n.$$

Então,

$$\frac{4n}{3} < 2p \leq 2n \quad \text{e} \quad 2n < 3p \leq 3n.$$

Assim, p é um fator do denominador de (25), mas $2p$ não é, enquanto que $2p$ é um fator do numerador de (25), mas $3p$ não é. Ou seja, o número primo p aparece no numerador e no denominador de (25) e, portanto, é cancelado. Assim,

$$f_2 = \prod_{\sqrt{2n} < p_j \leq n} p_j = \prod_{\sqrt{2n} < p_j \leq 2n/3} p_j \overset{(18)}{\leq} 4^{2n/3}. \tag{28}$$

Em resumo,

$$\frac{2^{2n}}{2n} \overset{(17)}{<} \binom{2n}{n} = f_1 \cdot f_2 \cdot f_3 \overset{(27)(28)}{\leq} (2n)^{\Pi(\sqrt{2n})} \cdot 4^{2n/3} \cdot f_3,$$

de onde

$$f_3 > \frac{2^{2n/3}}{(2n)^{\Pi(\sqrt{2n}\,)+1}}. \tag{29}$$

Hipótese. Considere $n \geq 113$.

Assim, $\sqrt{2n} > 15$. Como $\Pi(\sqrt{2n}\,)$ é menor que o número de números inteiros positivos ímpares menores do que $\sqrt{2n}$ e considerando que 9 e 15 são números compostos, temos

$$\Pi(\sqrt{2n}\,)+1 \leq \left(\frac{\sqrt{2n}+1}{2}-2\right)+1 = \frac{\sqrt{2n}+1}{2}-1$$

$$= \frac{\sqrt{2n}}{2}-\frac{1}{2} < \frac{\sqrt{2n}}{2}.$$

Substituindo a desigualdade acima em (29), obtemos

$$f_3 > \frac{2^{2n/3}}{(2n)^{\Pi(\sqrt{2n}\,)+1}} > \frac{2^{2n/3}}{(2n)^{\sqrt{2n}/2}} = \frac{2^{2n/3}}{(\sqrt{2n}\,)^{\sqrt{2n}}} = \left(\frac{2^{\sqrt{2n}}}{(\sqrt{2n}\,)^3}\right)^{\sqrt{2n}/3}. \tag{30}$$

Considerando $x = \sqrt{2n} > 15$ (Hipótese), segue de (23) que

$$2^{\sqrt{2n}} = 2^x > x^3 = (\sqrt{2n}\,)^3 \quad \Longrightarrow \quad \frac{2^{\sqrt{2n}}}{(\sqrt{2n}\,)^3} > 1,$$

a qual aplicada em (30) resulta em

$$f_3 = \prod_{n<p_k\leq 2n} p_k > 1, \text{ pois } \frac{\sqrt{2n}}{3} > 5 > 1.$$

Em outras palavras, o teorema está demonstrado para $n \geq 113$ (Hipótese). Por exaustão, verificando os casos possíveis, prova-se o teorema para $1 \leq n < 113$, terminando, assim, a sua prova. □

Exercício 8.1. *Encontre todos os números $n \in \mathbb{N}$ tais que os números*

$$n+1,\ n+3,\ n+7,\ n+9,\ n+13,\ n+15,$$

são números primos.

Exercício 8.2. *Por exaustão, verificando os casos possíveis, prove o Teorema 6.2 para $1 \leq n < 113$.*

9 Postulado de Bertrand, parte 2

Nesta seção serão estudadas algumas consequências do Postulado de Bertrand.

As estimativas que aparecem no Postulado de Bertrand podem ser melhoradas se $n \geq 2$. De fato, como vimos na demonstração do Postulado de Bertrand, existe um número primo p, tal que $n < p < 2n$.

A primeira utilização do Postulado de Bertrand aparecerá na generalização da seguinte construção. Considere $k = 2$ e $n = 5$. Note que $n > 2^k$. Procuremos os $k = 2$ primeiros números inteiros que são *maiores* que $n = 5$ e *relativamente primos* com $n! = 120$.

O número inteiro 6 não serve, pois, 6 e 120 não são relativamente primos. O número inteiro 7 serve, pois, 7 e 120 são relativamente primos. Os números inteiros 8, 9 e 10 não servem, pois, cada um deles e 120 não são relativamente primos. O número inteiro 11 serve, pois, 11 e 120 são relativamente primos.

Assim, os $k = 2$ primeiros números inteiros que são maiores que $n = 5$ e relativamente primos com $n! = 120$ são 7 e 11.

Note que eles são *números primos*. De fato, a construção acima pode ser generalizada, resultando na seguinte proposição.

Proposição 9.1. *Considere $k \in \mathbb{N}$ e $n > 2^k$. Então, os k primeiros números inteiros que são maiores que n e relativamente primos com $n!$ são números primos.*

Demonstração. Como, por hipótese,

$$n > 2^k, \quad \text{então} \quad n^2 > 2^k n.$$

Considere a sequência com $k + 1$ termos de números inteiros positivos

$$n,\ 2n,\ 4n,\ 8n,\ \ldots,\ 2^k n \quad (< n^2).$$

Pelo Teorema de Bertrand, existe um número primo entre quaisquer dois termos consecutivos desta sequência. Portanto, entre n e n^2 existem, pelo menos, k números primos. Em particular, os k primeiros números inteiros que são maiores que n e relativamente primos com $n!$ estão entre n e n^2. Suponha que um de tais números, denotado por a, não é um número primo. Assim, a é composto. Sem perda de generalidade, considere

$$a = b\,c, \quad \text{com} \quad 1 < b \leq c.$$

Assim,

$$b^2 \leq b\,c = a \leq n^2,$$

de onde

$$b \leq n,$$

ou seja, b divide a e também divide $n!$, um absurdo. □

Considere um conjunto A não vazio, de natureza qualquer. Uma *partição* do conjunto A é uma coleção $A_1, A_2, \ldots, A_k$ de subconjuntos de A tais que

$$A = \bigcup_{i=1}^{k} A_i, \quad A_j \cap A_n = \emptyset, \quad j \neq n, \quad j, n \in \{1, 2, \ldots, k\}.$$

Exemplo 9.1. *Uma partição do conjunto*

$$A = \{1, 2, 3, 4, 5, 6\}$$

é dada por

$$A_1 = \{1, 3, 5\} \quad e \quad A_2 = \{2, 4, 6\}.$$

Dado $n \in \mathbb{N}$, considere o conjunto

$$I_{2n} = \{1, 2, \ldots, 2n\}.$$

Procuramos uma partição do conjunto I_{2n} com as seguintes características:

- Cada conjunto da partição tem dois elementos;
- A soma dos dois elementos de cada conjunto da partição é um número primo.

Em outras palavras, procuramos uma partição do conjunto I_{2n} com as seguintes características

$$\{a_i, b_i\} \subset I_{2n}, \quad \forall i \in \{1, 2, \ldots, n\},$$
$$I_{2n} = \bigcup_{i=1}^{n} \{a_i, b_i\},$$
$$\{a_i, b_i\} \bigcap \{a_j, b_j\} = \emptyset, \ i \neq j, \ i, j \in \{1, 2, \ldots, n\},$$
$$a_i + b_i = p_i,$$

sendo p_i um número primo, para todo $i \in \{1, 2, \ldots, n\}$.

Uma tal partição, se existir, é chamada de *partição de I_{2n} por pares cujas somas são números primos.*

Exemplo 9.2. *Considere $n = 10$. Assim,*

$$I_{20} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20\}.$$

Uma possível partição de I_{20} por pares cujas somas são números primos é dada na Figura 8, ou seja,

$$\{1, 12\}, \quad \{2, 11\}, \quad \{3, 20\}, \quad \{4, 19\}, \quad \{5, 18\},$$
$$\{6, 17\}, \quad \{7, 16\}, \quad \{8, 15\}, \quad \{9, 14\}, \quad \{10, 13\}.$$

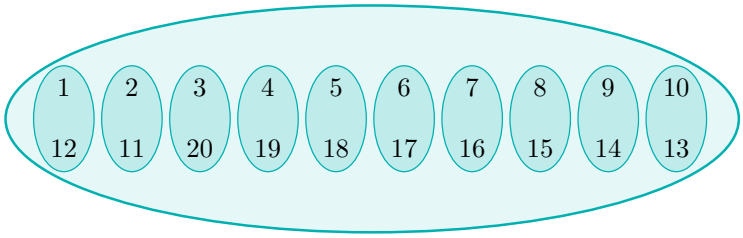

Figura 8: Partição de I_{20} por pares cujas somas são números primos.

A proposição a seguir garante que, para cada $n \in \mathbb{N}$, I_{2n} possui uma partição por pares cujas somas são números primos.

Proposição 9.2. *Considere $n \in \mathbb{N}$ e o conjunto $I_{2n} = \{1, 2, \ldots, 2n\}$. Então, existe uma partição de I_{2n} por pares cujas somas são números primos.*

Como veremos, na demonstração da Proposição 9.2 utilizaremos de maneira essencial o Postulado de Bertrand.

Demonstração. Faremos a prova por indução em $n \in \mathbb{N}$. Para $n = 1$, temos $I_2 = \{1, 2\}$, que tem partição trivial $\{1, 2\}$, cuja soma dos elementos é 3, que é um número primo. Para $n = 2$, temos $I_4 = \{1, 2, 3, 4\}$, que tem a seguinte partição

$$I_4 = \{1, 4\} \cup \{2, 3\},$$

cujas somas dos elementos é 5, um número primo. Fixe arbitrariamente $n > 2$.

Hipótese de Indução. O teorema tem uma prova para todo $m < n$, ou seja, existe uma partição do conjunto I_{2m} por pares cujas somas são números primos.

Queremos mostrar, utilizando a Hipótese de Indução, que existe uma partição do conjunto I_{2n} por pares cujas somas são números primos. Pelo Postulado de Bertrand, existe um número primo p tal que

$$2n < p < 4n.$$

Escreva $p = 2n + k$, para algum k ímpar satisfazendo $1 \leq k < 2n$. Defina o seguinte conjunto

$$I_{k,2n} = \{k, k + 1, \ldots, 2n - 1, 2n\}.$$

Afirmação. Existe uma partição de $I_{k,2n}$ por pares cujas somas são números primos.

De fato, considere a seguinte partição de $I_{k,2n}$:

$$I_{k,2n} = \{k, 2n\} \bigcup \{k + 1, 2n - 1\} \bigcup \cdots \bigcup \left\{ n + \left\lfloor \frac{k}{2} \right\rfloor, n + \left\lceil \frac{k}{2} \right\rceil \right\}.$$

Esta partição está bem definida (verifique!) e as somas em cada um dos pares é

$$2n + k = p,$$

portanto, um número primo. Como k é ímpar, então $k - 1$ é par, ou seja $k - 1 = 2m$. Assim,

$$2m = k - 1 < 2n \quad \Longrightarrow \quad m < n.$$

Pela Hipótese de Indução, existe uma partição do conjunto

$$I_{2m} = \{1, 2, \ldots, 2m\} = \{1, 2, \ldots, k - 1\}$$

por pares cujas somas são números primos. Como

$$\begin{aligned} I_{2n} &= \underbrace{\{1, 2, \ldots, k-1\}}_{I_{2m}} \bigcup \underbrace{\{k, k+1, \ldots, 2n-1, 2n\}}_{I_{k,2n}} \\ &= I_{2m} \bigcup I_{k,2n}, \end{aligned}$$

segue que existe uma partição do conjunto I_{2n} por pares cujas somas são números primos. □

A conjectura a seguir pode ser encontrada em [5].

Conjectura 9.1. *Para cada inteiro $n \geq 2$, o conjunto $I_{2n} = \{1, 2, \ldots, 2n\}$ pode ser arranjado em um ciclo tal que a soma de quaisquer números adjacentes é um número primo.*

Exercício 9.1. *Considere $n = 20$. Exiba uma partição do conjunto I_{40} por pares cujas somas são números primos.*

Exercício 9.2. *Pode-se provar o seguinte teorema.*

Teorema 9.1. *Para todo inteiro $n > 1$, existe um número primo p tal que*

$$2n < p < 3n.$$

Use o Teorema 9.1 para provar o seguinte teorema.

Teorema 9.2. *Para todo inteiro $n \geq 1$, existe um número primo p tal que*

$$n < p < \frac{3(n+1)}{2}.$$

Como

$$\frac{3(n+1)}{2} < 2n, \quad \forall n > 3,$$

segue que o Teorema 9.2 é um refinamento do Postulado de Bertrand.

10 Primos como a soma de dois quadrados

O objetivo desta seção é estudar alguns números primos que são escritos como a soma de dois quadrados. Em particular, demonstraremos o Teorema de Fermat. Mais detalhes podem ser encontrados em [1]. Começamos com um esboço da solução do Exercício 5.2.

Solução 10.1. *Considere um número primo da forma $p = 4k + 1$, para algum $k \in \mathbb{N}$. Assim, pelo Teorema de Fermat,*

$$p = a^2 + b^2, \quad a, b \in \mathbb{N}.$$

Sem perda de generalidade, podemos assumir $a > b$. Considere

$$p^2 = \left(a^2 + b^2\right)^2 = \left(a^2 - b^2\right)^2 + (2\,a\,b)^2 = c^2 + d^2,$$

sendo $c = a^2 - b^2 \in \mathbb{N}$ e $d = 2\,a\,b \in \mathbb{N}$.

Teorema 10.1 (Teorema de Fermat)**.** *Todo número primo da forma*

$$p = 4k + 1, \quad k \in \mathbb{N},$$

pode ser escrito como a soma de dois quadrados de números inteiros positivos, isto é,

$$p = a^2 + b^2, \quad a, b \in \mathbb{N}.$$

Considere A um conjunto não vazio e uma função $f : A \longrightarrow A$. Dizemos que a função f é uma *involução* se $f \circ f = \mathrm{Id}$. Um *ponto fixo* de f é um ponto $x_0 \in A$ tal que $f(x_0) = x_0$.

Prova do Teorema 10.1. Fixe, arbitrariamente, um número primo $p = 4k+1$, $k \in \mathbb{N}$. Queremos mostrar que p é a soma de dois quadrados de números inteiros positivos. Defina o conjunto

$$S_p = \left\{(x, y, z) \in \mathbb{Z}^3 : 4\,x\,y + z^2 = p,\ x \geq 1,\ y \geq 1\right\}.$$

Afirmação. S_p é um conjunto finito. De fato,

$$4\,x\,y + z^2 = p \quad \Longrightarrow \quad 0 \leq z^2 = p - 4\,x\,y \quad \Longrightarrow \quad 4\,x\,y \leq p,$$

de onde

$$1 \leq x \leq \frac{p}{4} \quad \text{e} \quad 1 \leq y \leq \frac{p}{4},$$

ou seja, apenas uma quantidade finita de valores de x e de y são possíveis e, consequentemente apenas uma quantidade finita de valores de z também é possível, de onde S_p é finito.

Parte 1. Defina

$$f : S_p \longrightarrow S_p, \quad f(x, y, z) = (y, x, -z).$$

A função f está bem definida. De fato,

$$f(x,y,z) = (y,x,-z) \in S_p,$$

uma vez que

$$4(y)(x) + (-z)^2 = 4\,x\,y + z^2 = p, \quad \text{pois } (x,y,z) \in S_p.$$

A função f é uma involução. De fato,

$$f(f(x,y,z)) = f(y,x,-z) = (x,y,z), \quad \forall (x,y,z) \in S_p.$$

A função f não tem ponto fixo. Um ponto fixo de f satisfaz

$$(x,y,z) = f(x,y,z) = (y,x,-z) \quad \Longrightarrow \quad x = y \text{ e } z = 0,$$

de onde,

$$p = 4\,x\,y + z^2 = 4x^2,$$

o que não pode acontecer, pois, p é um número primo. Considere o conjunto

$$T = \{(x,y,z) \in S_p : z > 0\}.$$

Tome $(x,y,z) \in T$. Como $f(x,y,z) = (y,x,-z) \in S_p$, segue que a terceira coordenada de $f(x,y,z)$ é negativa, de onde $f(x,y,z) \notin T$, ou seja, f aplica o conjunto T em $S_p \setminus T$. Os pontos $(x,y,z) \in \mathbb{Z}^3$ tais que $x - y + z = 0$ não pertencem a S_p. De fato, se um deles pertencesse a S_p teríamos

$$p = 4\,x\,y + z^2 = 4\,x\,y + (x-y)^2 = (x+y)^2,$$

o que não é possível, pois, p é um número primo. Da afirmação anterior e, como f reverte os sinais de $x - y$ e de z, então f aplica o conjunto

$$U = \{(x,y,z) \in S_p : x - y + z > 0\}$$

no conjunto $S_p \setminus U$. Como f aplica os conjuntos T e U nos seus complementares em S_p, então f aplica $T \setminus U$ em $U \setminus T$ e reciprocamente. Veja a Figura 9.

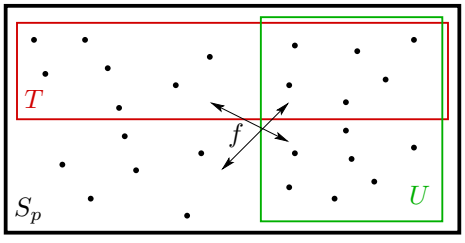

Figura 9: A função f.

Deste modo, os conjuntos T e U são finitos e têm a mesma cardinalidade.

Parte 2. Defina

$$g : U \longrightarrow U, \quad g(x, y, z) = (x - y + z, y, 2y - z).$$

A função g está bem definida (verifique!). A função g é uma involução. De fato,

$$\begin{aligned} g(g(x, y, z)) &= g(x - y + z, y, 2y - z) \\ &= ((x - y + z) - y + (2y - z), y, 2y - (2y - z)) \\ &= (x, y, z), \quad \forall (x, y, z) \in U. \end{aligned}$$

A função g tem um único ponto fixo. Veja a Figura 10.

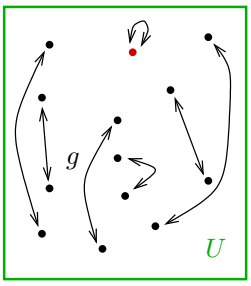

Figura 10: A função g.

Um ponto fixo de g satisfaz

$$(x, y, z) = g(x, y, z) = (x - y + z, y, 2y - z) \quad \Longrightarrow \quad y = z.$$

Assim,

$$p = 4\,x\,y + z^2 = 4\,x\,y + y^2 = y(4x + y).$$

Como p é primo, a única possibilidade é

$$y = z = 1 \quad \text{e} \quad x = \frac{p - 1}{4} \in \mathbb{N},$$

o que está de acordo com a hipótese de que $p = 4k + 1$, $k \in \mathbb{N}$. Em resumo, a função g é uma involução em U com exatamente um ponto fixo. Isto implica que a cardinalidade de U é ímpar.

Parte 3. Defina

$$h : T \longrightarrow T, \quad h(x, y, z) = (y, x, z).$$

A função h está bem definida e é uma involução (verifique!). Como a cardinalidade de T é igual à cardinalidade de U e a cardinalidade de U é ímpar,

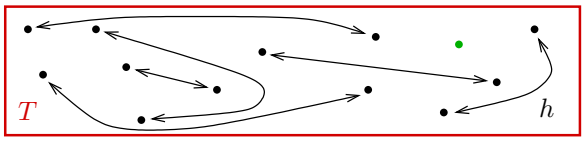

Figura 11: A função h.

segue que a cardinalidade de T é ímpar. Sendo h uma involução em T e tendo T cardinalidade ímpar, segue que h tem um ponto fixo em T. Veja a Figura 11.

Portanto, existe $(x, y, z) \in T$ tal que

$$(x, y, z) = h(x, y, z) = (y, x, z) \quad \Longrightarrow \quad x = y \text{ e } z > 0.$$

Assim,

$$p = 4\,x\,y + z^2 = 4x(x) + z^2 = 4x^2 + z^2 = (2x)^2 + z^2,$$

com $x \geq 1$ e $z \geq 1$, terminando a prova do teorema. □

Por outro lado, pode-se mostrar que nenhum número primo da forma $p = 4k + 3$, $k \in \mathbb{N}$, pode ser escrito como a soma de dois quadrados de números inteiros positivos.

Combinando o Teorema de Fermat e o parágrafo acima, pode-se demonstrar o seguinte teorema.

Teorema 10.2. *Um número $n \in \mathbb{N}$ pode ser escrito como a soma de dois quadrados de números inteiros não negativos se, e somente se, na decomposição de n como um produto de números primos, cada fator primo da forma $4k + 3$ aparece com uma potência par.*

Exercício 10.1. *Mostre que a função g na prova do Teorema 10.1 está bem definida. Mostre, ainda, que a função h está bem definida e é uma involução.*

Exercício 10.2. *Suponha que os números $n, m \in \mathbb{N}$ podem ser escritos como a soma de dois quadrados de números inteiros não negativos. Mostre que o produto $mn \in \mathbb{N}$ também pode ser escrito como a soma de dois quadrados de números inteiros não negativos. Mostre ainda que o número $n\,z^2$, sendo z um número inteiro não negativo, também pode ser escrito como a soma de dois quadrados de números inteiros não negativos.*

11 Teorema de Euclides: Algum primo foi esquecido?

Na Seção 3 discutimos a seguinte questão.

Pergunta 11.1. *Considere $\mathcal{P} \subset \mathbb{N}$ o conjunto dos números primos. O conjunto $\mathcal{P}$ é finito ou infinito?*

A primeira resposta a esta pergunta apareceu há cerca de 2300 anos na Proposição 20 do Livro IX de "Os Elementos" de Euclides [7]. Em sua homenagem, o teorema da não finitude dos números primos é chamado de Teorema de Euclides.

Na prova do Teorema de Euclides, utilizamos o Teorema Fundamental da Aritmética (TFA), estudado nas Seções 3 e 4. O TFA afirma que todos os números inteiros positivos maiores que 1 podem ser decompostos num produto de números primos, sendo essa decomposição única a menos de permutações dos fatores.

Prova do Teorema de Euclides. Suponha que $\mathcal{P}$ é finito. Considere

$$\mathcal{P} = \{p_1, p_2, \ldots, p_n\}.$$

Defina o número inteiro positivo

$$a = p_1 \cdot p_2 \cdots p_n + 1.$$

Por construção, a não é divisível por nenhum $p_i \in \mathcal{P}$ e $a > p_i$, $i \in \{1, 2, \ldots, n\}$. Assim, ou a é primo ou possui um fator primo (TFA). Em ambos os casos, temos a existência de um número primo p diferente de p_i, $i \in \{1, 2, \ldots, n\}$. Portanto, $\mathcal{P}$ não pode ser finito. □

O teorema apresentado acima é na verdade um pouco diferente do teorema que Euclides escreveu. Como os gregos antigos não tinham a noção moderna de infinito, Euclides não poderia ter escrito "há infinitos primos" ou o "conjuntos dos números primos é infinito".

Ele escreveu: "a quantidade de números primos é maior do que qualquer quantidade atribuida de números primos", ou seja, existem mais números primos do que em qualquer lista finita de números primos.

Como os primos são a matéria prima com a qual temos que construir a Aritmética, o Teorema de Euclides nos garante que temos bastante material para a tarefa.

A prova do Teorema de Euclides é muito simples. Entretanto, ela não nos fornece informação alguma a respeito do número primo p, a não ser que ele é, no máximo, igual a

$$a = p_1 \cdot p_2 \cdots p_n + 1.$$

Denote por $\mathcal{P}^E$ o conjuntos dos número primos que podem ser obtidos pelo "método" de Euclides, ou seja, o conjunto dos números primos obtidos segundo a "ideia" apresentada na prova do Teorema de Euclides. Por construção, $\mathcal{P}^E$ é um conjunto infinito.

Pergunta 11.2. *Considere $\mathcal{P}^E \subset \mathcal{P}$. O conjunto $\mathcal{P}^E$ coincide com o conjunto $\mathcal{P}$, ou seja, $\mathcal{P}^E = \mathcal{P}$?*

Em outras palavras, terá Euclides "esquecido" algum número primo? Para tentar entender a Pergunta 11.2 precisamos, antes de mais nada, entender o que significa "método" de Euclides ou "ideia" apresentada na prova do Teorema de Euclides.

Dado um número primo p, defina

$$p^* = \prod_{q \leq p} q, \text{ sendo } q \text{ um número primo,}$$

isto é, p^* é o produto dos números primos q menores ou iguais a p.

Defina o seguinte subconjunto do conjunto dos números primos

$$\mathcal{P}^* = \{p \in \mathcal{P} : p^* + 1 \text{ é um número primo}\}.$$

Afirmação 1. O conjunto $\mathcal{P}^*$ é não vazio.

De fato, os números primos $p = 2$, $p = 3$, $p = 5$ e $p = 7$ pertencem ao conjunto $\mathcal{P}^*$, pois

$$2^* + 1 = 2 + 1 = 3 \in \mathcal{P}, \quad 3^* + 1 = 2 \cdot 3 + 1 = 7 \in \mathcal{P},$$
$$5^* + 1 = 2 \cdot 3 \cdot 5 + 1 = 31 \in \mathcal{P}, \quad 7^* + 1 = 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211 \in \mathcal{P}.$$

Afirmação 2. O conjunto $\mathcal{P}^*$ é diferente de $\mathcal{P}$.

De fato, o número primo $p = 13$ não pertence a $\mathcal{P}^*$, pois

$$13^* + 1 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509 \notin \mathcal{P}.$$

Coloca-se, assim, a seguinte questão.

Pergunta 11.3. *Considere $\mathcal{P}^* \subset \mathcal{P}$. O conjunto $\mathcal{P}^*$ é finito ou infinito?*

Não se tem, até o momento, uma resposta a esta pergunta.

Considere, agora, a seguinte sequência $(p_n)_{n \in \mathbb{N}}$, definida recursivamente por: $p_1 = 2$ e, para todo $n \in \mathbb{N}$, $n \geq 2$, p_n é o maior divisor primo de

$$p_1 \cdot p_2 \cdots p_{n-1} + 1.$$

Denote por $\mathcal{P}^M \subset \mathcal{P}$ o conjunto dos termos dessa sequência. Por construção, $\mathcal{P}^M$ é um conjunto infinito.

Podemos colocar as seguintes questões com relação ao conjunto $\mathcal{P}^M$ e à sequência $(p_n)_{n \in \mathbb{N}}$.

Pergunta 11.4. *Considere $\mathcal{P}^M \subset \mathcal{P}$. O conjunto $\mathcal{P}^M$ coincide com o conjunto $\mathcal{P}$, ou seja, $\mathcal{P}^M = \mathcal{P}$? Se $\mathcal{P}^M \subsetneq \mathcal{P}$, $\mathcal{P}^M$ omite uma quantidade finita ou infinita de números primos?*

Pergunta 11.5. *A sequência $(p_n)_{n \in \mathbb{N}}$ é monótona crescente?*

Começaremos nossa análise pela última pergunta. Por definição, $p_1 = 2$ e p_2 é o maior divisor primo de

$$p_1 + 1 = 2 + 1 = 3 \quad \Longrightarrow \quad p_2 = 3.$$

p_3 é o maior divisor primo de

$$p_1 \cdot p_2 + 1 = 2 \cdot 3 + 1 = 7 \quad \Longrightarrow \quad p_3 = 7.$$

p_4 é o maior divisor primo de

$$p_1 \cdot p_2 \cdot p_3 + 1 = 2 \cdot 3 \cdot 7 + 1 = 43 \quad \Longrightarrow \quad p_4 = 43.$$

p_5 é o maior divisor primo de

$$p_1 \cdot p_2 \cdot p_3 \cdot p_4 + 1 = 2 \cdot 3 \cdot 7 \cdot 43 + 1 = 1807 = 13 \cdot 139 \quad \Longrightarrow \quad p_5 = 139.$$

Repetindo esse procedimento, obtemos

$$p_6 = 50207, \quad p_7 = 340999, \quad p_8 = 2365347734339,$$
$$p_9 = 4680225641471129, \quad p_{10} = 1368845206580129, \quad \ldots.$$

Observe que $p_{10} < p_9$, de onde a sequência $(p_n)_{n\in\mathbb{N}}$ não é monótona crescente.

Vale comentar que os termos p_5, p_6, p_7, p_8, p_9 e p_{10}, listados acima, da sequência $(p_n)_{n\in\mathbb{N}}$ foram obtidos com o software Mathematica.

Observe que o número primo 5 não apareceu entre os termos iniciais da sequência $(p_n)_{n\in\mathbb{N}}$. Assim, $5 \in \mathcal{P}^M$? Como a sequência $(p_n)_{n\in\mathbb{N}}$ não é monótona, não podemos, pelos argumentos anteriores, decidir essa questão.

Afirmação 3. $5 \notin \mathcal{P}^M$.

Como vimos acima, $p_1 = 2$, $p_2 = 3$ e $p_3 = 7$. Dos dois primeiros termos, para $n \geq 3$,

$$p_1 \cdot p_2 \cdot p_3 \cdots p_{n-1} = 2 \cdot 3 \cdot p_3 \cdots p_{n-1}$$

é múltiplo de 2 e também é múltiplo de 3. Portanto,

$$p_1 \cdot p_2 \cdot p_3 \cdots p_{n-1} + 1 = 2 \cdot 3 \cdot p_3 \cdots p_{n-1} + 1$$

não é múltiplo de 2 e também não é múltiplo de 3. Segue ainda que p_n é ímpar.

Dessa discussão,

$$p_1 \cdot p_2 \cdot p_3 \cdots p_{n-1}$$

não é múltiplo de 4.

Suponha que exista $n \geq 4$ tal que $p_n = 5$, ou seja, o maior divisor primo de

$$p_1 \cdot p_2 \cdot p_3 \cdots p_{n-1} + 1$$

é 5. Como 2 e 3 não dividem

$$p_1 \cdot p_2 \cdot p_3 \cdots p_{n-1} + 1,$$

segue que existe $k \in \mathbb{N}$, tal que

$$p_1 \cdot p_2 \cdot p_3 \cdots p_{n-1} + 1 = 5^k.$$

Portanto,

$$p_1 \cdot p_2 \cdot p_3 \cdots p_{n-1} = 5^k - 1 = (5-1)\left(5^{k-1} + 5^{k-2} + \cdots + 5 + 1\right).$$

Portanto, 4 divide

$$p_1 \cdot p_2 \cdot p_3 \cdots p_{n-1},$$

o que é uma contradição, pelo que vimos acima.

Pode-se mostrar que

$$11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,\ 47 \notin \mathcal{P}^M.$$

Pelo que vimos, $\mathcal{P}^M \subsetneq \mathcal{P}$.

A resposta à Pergunta 11.4, se $\mathcal{P}^M$ omite uma quantidade finita ou infinita de números primos, é dada pelo seguinte teorema, veja [3].

Teorema 11.1. *O conjunto $\mathcal{P}^M$ omite uma quantidade infinita de números primos. De modo mais preciso, o conjunto $\mathcal{P} \setminus \mathcal{P}^M$ é infinito.*

Podemos alterar a definição da sequência $(p_n)_{n\in\mathbb{N}}$, de modo a obter uma outra sequência. Considere, agora, a sequência $(q_n)_{n\in\mathbb{N}}$, definida recursivamente da seguinte maneira: $q_1 = 2$ e, para todo $n \in \mathbb{N}$, $n \geq 2$, q_n é o menor divisor primo de

$$q_1 \cdot q_2 \cdots q_{n-1} + 1.$$

Denote por $\mathcal{P}^m \subset \mathcal{P}$ o conjunto dos termos dessa sequência. Por construção, $\mathcal{P}^m$ é um conjunto infinito.

Podemos colocar a seguinte questão com relação ao conjunto $\mathcal{P}^m$.

Pergunta 11.6. *Considere $\mathcal{P}^m \subset \mathcal{P}$. O conjunto $\mathcal{P}^m$ coincide com o conjunto $\mathcal{P}$, ou seja, $\mathcal{P}^m = \mathcal{P}$? Se $\mathcal{P}^m \subsetneq \mathcal{P}$, $\mathcal{P}^m$ omite uma quantidade finita ou infinita de números primos?*

Por definição, $q_1 = 2$ e q_2 é o menor divisor primo de

$$q_1 + 1 = 2 + 1 = 3 \quad \Longrightarrow \quad q_2 = 3.$$

q_3 é o menor divisor primo de

$$q_1 \cdot q_2 + 1 = 2 \cdot 3 + 1 = 7 \quad \Longrightarrow \quad q_3 = 7.$$

q_4 é o menor divisor primo de

$$q_1 \cdot q_2 \cdot q_3 + 1 = 2 \cdot 3 \cdot 7 + 1 = 43 \quad \Longrightarrow \quad q_4 = 43.$$

q_5 é o menor divisor primo de

$$q_1 \cdot q_2 \cdot q_3 \cdot q_4 + 1 = 2 \cdot 3 \cdot 7 \cdot 43 + 1 = 1807 = 13 \cdot 139 \quad \Longrightarrow \quad q_5 = 13.$$

Da análise acima, segue que a sequência $(q_n)_{n\in\mathbb{N}}$ não é monótona crescente.

O que poder ser dito a respeito da Pergunta 11.6? Muito pouco! Na referência [15] são apresentados argumentos probabilísticos de que $\mathcal{P}^m = \mathcal{P}$. No entanto, ainda não se tem uma prova dessa afirmação. Se essa afirmação for provada, concluiremos que Euclides não esqueceu primo algum!

Exercício 11.1. *Um quadrado mágico é uma matriz quadrada cujas entradas são números inteiros positivos e tal que as somas dos números em cada linha, em cada coluna e nas duas diagonais são as mesmas. Essa soma comum é chamada soma mágica. Complete a matriz abaixo com números primos de modo que ela seja um quadrado mágico com soma mágica* 111.

	1	

12 A Conjectura de Goldbach

Em 1742, em carta enviada a Euler, Goldbach escreveu

Afirmação 1. Todo número inteiro $n > 5$ é a soma de três números primos.

Euler respondeu que a afirmação feita por Goldbach era equivalente à seguinte afirmação.

Afirmação 2. Todo número inteiro par $2n \geq 4$ é a soma de dois números primos.

A Afirmação 2 ficou conhecida como a Conjectura de Goldbach.

Conjectura 12.1 (Conjectura de Goldbach)**.** *Todo número inteiro par maior ou igual a quatro é a soma de dois números primos.*

A seguir, será apresentada uma prova da equivalência das Afirmações 1 e 2.

Demonstração.
Parte 1: Suponha a Afirmação 2 verdadeira, ou seja, todo número inteiro par $2n \geq 4$ é a soma de dois números primos.
Queremos mostrar que a Afirmação 1 é verdadeira, ou seja, que todo número inteiro $n > 5$ é a soma de três números primos. Considere $k \geq 3$. Assim, $2k-2$ é par e é maior ou igual a quatro. Pela Afirmação 1, existem números primos p_1 e p_2 tais que

$$2k-2 = p_1 + p_2 \quad \Longrightarrow \quad 2k = 2 + p_1 + p_2 \quad \text{e} \quad 2k+1 = 3 + p_1 + p_2,$$

provando, assim, a Afirmação 1 para $n \geq 7$. Para $n = 6$ é imediato.

Parte 2: Suponha que a Afirmação 1 é verdadeira, ou seja, todo número inteiro $n > 5$ é a soma de três números primos. Queremos mostrar que a Afirmação 2 verdadeira, ou seja, que todo número inteiro par $2n \geq 4$ é a soma de dois números primos. Considere $2n \geq 4$. Pela Afirmação 1, existem números primos q_1, q_2 e q_3, tais que

$$2n + 2 = q_1 + q_2 + q_3.$$

Como $2n+2$ é par, segue da igualdade anterior que um dos números primos q_1, q_2 ou q_3 é par. Suponha $q_3 = 2$. Assim,

$$2n + 2 = q_1 + q_2 + q_3 = q_1 + q_2 + 2 \quad \Longrightarrow \quad 2n = q_1 + q_2,$$

provando a Afirmação 2. □

Na correspondência entre Goldbach e Euler, este último escreveu: "Que todo inteiro par é uma soma de dois primos, considero um teorema completamente certo, embora não possa prová-lo."

A Conjectura de Goldbach foi verificada verdadeira para números inteiros pares até 10^8, mas ela permanece sem uma prova para todo número inteiro par.

Suponha, por um momento, que a Conjectura de Goldbach é verdadeira. Considere $n \geq 2$. Assim, existem números primos $p \leq q$ tais que

$$2n = p + q \quad \Longrightarrow \quad n = \frac{p+q}{2},$$

ou seja,

$$p = n - k \quad \text{e} \quad q = n + k,$$

para algum número inteiro $0 \leq k \leq n-2$. Deste modo,

$$p\,q = (n-k)(n+k) = n^2 - k^2.$$

Suponha, agora, que para cada número inteiro $n \geq 2$, exista um número inteiro k satisfazendo $0 \leq k \leq n-2$ e números primos $p \leq q$ tais que

$$n^2 - k^2 = p\,q.$$

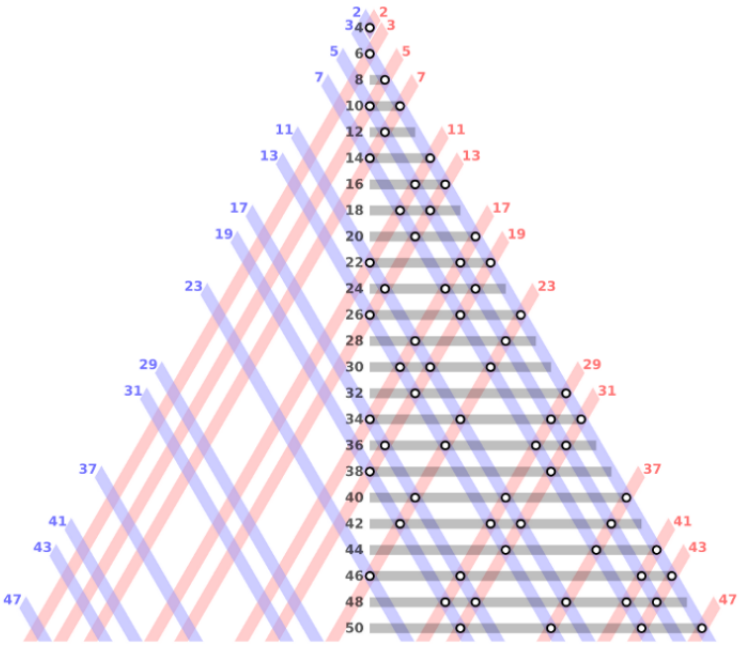

Figura 12: Números pares como a soma de dois primos.

Deste modo,

$$p\,q = n^2 - k^2 = (n-k)(n+k),$$

de onde, pelo TFA,

$$p = n - k \quad \text{e} \quad q = n + k,$$

implicando que

$$2n = p + q.$$

O que acabamos de mostrar é que a Conjectura de Goldbach é equivalente à seguinte afirmação.

Afirmação 3. Para todo número inteiro $n \geq 2$, existem números inteiros k, p e q, com $0 \leq k \leq n-2$, p e q números primos e tais que

$$n^2 - k^2 = p\,q.$$

Considerando $k = 1$ na Afirmação 3, colocamos a seguinte conjectura.

Conjectura 12.2. *Existem infinitos números inteiros $n \geq 2$ para os quais existem números primos p e q tais que*

$$n^2 - 1 = p\,q. \tag{31}$$

Recordemos a Conjectura dos Primos Gêmeos, discutida na Seção 6.

Conjectura 12.3 (Conjectura dos Primos Gêmeos)**.** *Existem infinitos números primos p para os quais $p+2$ é um número primo.*

Suponha, por um momento, que a Conjectura 12.3 é verdadeira. Considere p e $q = p+2$ números primos. Assim,

$$p\,q + 1 = p(p+2) + 1 = p^2 + 2p + 1 = (p+1)^2,$$

o que implica que

$$p\,q = (p+1)^2 - 1 = n^2 - 1, \quad \text{sendo} \quad n = p+1.$$

Concluimos, assim, que existem infinitos números inteiros $n \geq 2$ para os quais existem números primos p e $q = p+2$, tais que

$$n^2 - 1 = p\,q,$$

ou seja, a Conjectura 12.2 é verdadeira.

Por outro lado, suponha que a Conjectura 12.2 é verdadeira e fixe um tal número inteiro n satisfazendo-a. Assim,

$$n^2 - 1 = p\,q \quad \text{e} \quad n^2 - 1 = (n-1)(n+1).$$

Logo,

$$p = n-1 \quad \text{e} \quad q = n+1,$$

implicando que

$$q - p = (n+1) - (n-1) = 2 \quad \Longrightarrow \quad q = p+2.$$

Em resumo, a Conjectura 12.3 é verdadeira.

O que acabamos de provar é que a Conjectura 12.2 é equivalente à Conjectura 12.3.

Como a Conjectura 12.2 está relacionada com a Conjectura 12.1 (Goldbach), mostramos que existe uma estreita ligação entre ela e a Conjectura 12.3 (Primos Gêmeos).

Recordemos o conteúdo da Afirmação 1: Todo número inteiro $n > 5$ é a soma de três números primos. Considere a seguinte conjectura.

Conjectura 12.4 (Conjectura Fraca de Goldbach)**.** *Todo número inteiro ímpar $n > 5$ é a soma de três números primos.*

É imediato que a sua veracidade decorre da eventual veracidade da Conjectura 12.1 (Goldbach). Suponha, por um momento, que a Conjectura 12.4 (Fraca de Goldbach) é verdadeira.

Tome, arbitrariamente, $n \geq 5$ e assim, $2n \geq 10$. Considere o número inteiro ímpar $2n-3$. Da veracidade da Conjectura 12.4, existem números primos p_1, p_2 e p_3, tais que

$$2n - 3 = p_1 + p_2 + p_3 \quad \Longrightarrow \quad 2n = p_1 + p_2 + p_3 + 3,$$

ou seja, o número inteiro par $2n$ é a soma de quatro números primos. Podemos, então, concluir que todo número inteiro par maior ou igual a oito é a soma de quatro números primos.

Há fortes indícios de que essa afirmação seja, de fato, um teorema, em virtude da seguinte afirmação.

Afirmação 4. [Helfgott] A Conjectura Fraca de Goldbach é verdadeira.

THE TERNARY GOLDBACH CONJECTURE IS TRUE

H. A. HELFGOTT

ABSTRACT. The ternary Goldbach conjecture, or three-primes problem, asserts that every odd integer n greater than 5 is the sum of three primes. The present paper proves this conjecture.

Both the ternary Goldbach conjecture and the binary, or strong, Goldbach conjecture had their origin in an exchange of letters between Euler and Goldbach in 1742. We will follow an approach based on the circle method, the large sieve and exponential sums. Some ideas coming from Hardy, Littlewood and Vinogradov are reinterpreted from a modern perspective. While all work here has to be explicit, the focus is on qualitative gains.

The improved estimates on exponential sums are proven in the author's papers on major and minor arcs for Goldbach's problem. One of the highlights of the present paper is an optimized large sieve for primes. Its ideas get reapplied to the circle method to give an improved estimate for the minor-arc integral.

Figura 13: http://arxiv.org/pdf/1312.7748.pdf.

O que sabemos até o momento com relação aos estudos de Helfgott [9]: Em 2013 e 2014, Helfgott divulgou a sua prova da Conjectura Fraca de Goldbach, mas ela ainda não foi publicada em um periódico revisado por pares. A prova vem passando por mais revisões desde então.

Exercício 12.1. *Escreva cada um dos números inteiros pares abaixo como uma soma de números primos:*

$$10,\ 20,\ 50,\ 992,\ 1382,\ 1856,\ 1928.$$

Exercício 12.2. *Defina a função* $f : \mathbb{R}^2 \longrightarrow \mathbb{R}$, *por* $f(x, y) = x^2 - y^2$. *Dados* p *e* q *números primos ímpares com* $p \leq q$, *mostre que os dois pares abaixo são duas soluções com coordenadas inteiras não negativas da equação* $f(x, y) = p\,q$*:*

$$(x_1, y_1) = \left(\frac{p+q}{2}, \frac{q-p}{2}\right), \quad (x_2, y_2) = \left(\frac{p\,q+1}{2}, \frac{p\,q-1}{2}\right).$$

13 Números perfeitos e primos de Mersenne

Considere os primeiros números primos

$$2,\ 3,\ 5 \text{ e } 7.$$

Com eles, contruimos os seguintes números primos

$$\begin{aligned} M_2 &= 2^2 - 1 = 4 - 1 = 3, \\ M_3 &= 2^3 - 1 = 8 - 1 = 7, \\ M_5 &= 2^5 - 1 = 32 - 1 = 31, \\ M_7 &= 2^7 - 1 = 128 - 1 = 127. \end{aligned}$$

O que podemos afirmar sobre os números inteiros positivos da forma abaixo?

$$M_p = 2^p - 1, \quad p \text{ é primo.} \tag{32}$$

A primeira afirmação é que p ser um número primo é uma condição necessária para M_p ser um número primo.

Proposição 13.1. *Se M_p é um número primo, então p é um número primo.*

Demonstração. Faremos a prova pela contrapositiva, ou seja, mostraremos que se p é um número composto, então M_p é um número composto. Sendo p um número composto, existem $a, b \in \mathbb{N}$, $a, b > 1$, tais que $p = a\,b$. Em particular, $2^a - 1 > 1$. Agora,

$$\begin{aligned} M_p &= 2^p - 1 = 2^{a\,b} - 1 = (2^a)^b - 1 \\ &= (2^a - 1)\left((2^a)^{b-1} + (2^a)^{b-2} + \cdots + 2^a + 1\right). \end{aligned}$$

Desta última expressão, inferimos que $2^a - 1 > 1$ divide M_p o que implica que M_p é um número composto, como queríamos demonstrar. □

Observamos, agora, que p ser um número primo, embora seja uma condição necessária, não é suficiente para M_p ser um número primo. De fato, considere o número primo $p = 11$ e o número M_{11}. Por definição

$$M_{11} = 2^{11} - 1 = 2048 - 1 = 2047 = 23 \cdot 89,$$

o qual é um número composto. Se o número M_p é um número primo ele é chamado de *primo de Mersenne*.

Tabela 2 lista os números primos de Mersenne conhecidos até o momento. Esses números só puderam ser conhecidos devido ao grande esforço coletivo do "Grupo de Busca dos Números Primos de Mersenne", *Great Internet Mersenne Prime Search - GIMPS*.

#	n	M_n	Digitos	Data de descobrimento	Descobridor
1	2	3	1	Antiguidade	Antiguidade
2	3	7	1	Antiguidade	Antiguidade
3	5	31	2	Antiguidade	Antiguidade
4	7	127	3	Antiguidade	Antiguidade
5	13	8.191	4	1456	Anônimo
6	17	131.071	6	1588	Cataldi
7	19	524.287	6	1588	Cataldi
8	31	2.147.483.647	10	1772	Euler
9	61	2.305.843.009.213.693.951	19	1883	Pervushin
10	89	618970019...449.562.111	27	1911	Powers
11	107	162259276...010.288.127	33	1914	Powers
12	127	170141183...884.105.727	39	1876	Lucas
13	521	686479766...115.057.151	157	30 de janeiro de 1952	Robinson
14	607	531137992...031.728.127	183	30 de janeiro de 1952	Robinson
15	1.279	104079321...168.729.087	386	25 de junho de 1952	Robinson
16	2.203	147597991...697.771.007	664	7 de outubro de 1952	Robinson
17	2.281	446087557...132.836.351	687	9 de outubro de 1952	Robinson
18	3.217	259117086...909.315.071	969	8 de setembro de 1957	Riesel
19	4.253	190797007...350.484.991	1.281	3 de novembro de 1961	Hurwitz
20	4.423	285542542...608.580.607	1.332	3 de novembro de 1961	Hurwitz
21	9.689	478220278...225.754.111	2.917	11 de maio de 1963	Gillies
22	9.941	346088282...789.463.551	2.993	16 de maio de 1963	Gillies
23	11.213	281411201...696.392.191	3.376	2 de junho de 1963	Gillies
24	19.937	431542479...968.041.471	6.002	4 de março de 1971	Tuckerman
25	21.701	448679166...511.882.751	6.533	30 de outubro de 1978	Noll e Nickel
26	23.209	402874115...779.264.511	6.987	9 de fevereiro de 1979	Noll
27	44.497	854509824...011.228.671	13.395	8 de abril de 1979	Nelson e Slowinski
28	86.243	536927995...433.438.207	25.962	25 de setembro de 1982	Slowinski
29	110.503	521928313...465.515.007	33.265	25 de setembro de 1988	Colquitt e Welsh
30	132.049	512740276...730.061.311	39.751	20 de setembro de 1983	Slowinski
31	216.091	746093103...815.528.447	65.050	6 de setembro de 1985	Slowinski
32	756.839	174135906...544.677.887	227.832	19 de setembro de 1992	Slowinski e Gage
33	859.433	129498125...500.142.591	258.716	10 de janeiro de 1994	Slowinski e Gage
34	1.257.787	412245773...089.366.527	378.632	3 de setembro de 1996	Slowinski e Gage
35	1.398.269	814717564...451.315.711	420.921	13 de novembro de 1996	GIMPS/Joel Armengaud
36	2.976.221	623340076...729.201.151	895.932	24 de agosto de 1997	GIMPS/Gordon Spence
37	3.021.377	127411683...024.694.271	909.526	27 de janeiro de 1998	GIMPS/Roland Clarkson
38	6.972.593	437075744...924.193.791	2.098.960	1 de junho de 1999	GIMPS/Nayan Hajratwala
39	13.466.917	924947738...256.259.071	4.053.946	14 de novembro de 2001	GIMPS/Michael Cameron
40	20.996.011	125976895...855.682.047	6.320.430	17 de novembro de 2003	GIMPS/Michael Shafer
41	24.036.583	299410429...733.969.407	7.235.733	15 de maio de 2004	GIMPS/Josh Findley
42	25.964.951	122164630...577.077.247	7.816.230	18 de fevereiro de 2005	GIMPS/Martin Nowak
43	30.402.457	315416475...652.943.871	9.152.052	15 de dezembro de 2005	GIMPS/Curtis Cooper&Steven Boone
44	32.582.657	124575026...053.967.871	9.808.358	4 de setembro de 2006	GIMPS/Curtis Cooper&Steven Boone
45	37.156.667	202254406...308.220.927	11.185.272	6 de setembro de 2008	GIMPS/Hans-Michael Elvenich
46	42.643.801	169873516...562.314.751	12.837.064	12 de abril de 2009	GIMPS/Odd M. Strindmo
47	43.112.609	316470269...697.152.511	12.978.189	23 de agosto de 2008	GIMPS/Edson Smith
48	57.885.161	581887266...724.285.951	17.425.171	25 de janeiro de 2013	GIMPS/Curtis Cooper
49	74.207.281	300376418084...391086436351	22.338.618	7 de janeiro de 2016	GIMPS/Curtis Cooper
50	77.232.917	467333183359...069762179071	23.249.426	26 de dezembro de 2017	GIMPS/Jonathan Pace
51	82.589.933	148894445742...325217902591	24.862.048	7 de dezembro de 2018	GIMPS/Patrick Laroche
52	136.279.841	881694327503...219486871551	41.024.320	21 de outubro de 2024	GIMPS/Luke Durant

Tabela 2: http://pt.wikipedia.org/wiki/Primo_de_Mersenne.

Analisemos os números inteiros positivos 6 e 28. As somas dos divisores próprios de 6 e de 28 são:

$$6 : 1 + 2 + 3 = 6,$$
$$28 : 1 + 2 + 4 + 7 + 14 = 28,$$

ou seja, em ambos os casos, as somas dos divisores próprios desses números resultam nos próprios números. Dizemos que um número inteiro positivo n é um *número perfeito* se as somas dos seus divisores próprios é n. Equivalentemente, um número inteiro positivo n é um *número perfeito* se as somas dos seus divisores é $2n$.

Dado um número inteiro positivo n, denotamos por $\sigma(n)$ a soma dos divisores de n, e por $\sigma_0(n)$ a soma dos divisores próprios de n. Resulta que

$\sigma_0(n) = \sigma(n) - n$. Também resulta, imediatamente, que $\sigma(1) = 1$ e que $\sigma(p) = p + 1$, se, e somente se, p é um número primo.

O lema a seguir dá importante informação a respeito da $\sigma(n)$ no caso em que n é um número composto, produto de fatores relativamente primos.

Lema 13.1. *Considere um número inteiro positivo $n = a\,b$, sendo $(a, b) = 1$. Então,*

$$\sigma(n) = \sigma(a\,b) = \sigma(a)\,\sigma(b).$$

Demonstração. Como $n = a\,b$ e $(a, b) = 1$, segue que qualquer divisor d de n tem a forma $d = a_i b_i$, sendo a_i um divisor de a e b_i um divisor de b. Denotando os divisores de a e de b, respectivamente, por

$$1,\ a_1,\ \ldots,\ a, \quad 1,\ b_1,\ \ldots,\ b,$$

então

$$\sigma(a) = 1 + a_1 + \cdots + a \quad \text{e} \quad \sigma(b) = 1 + b_1 + \cdots + b.$$

Fixe um divisor de a da forma a_k. Considere todos os divisores de n da forma $d_k = a_k b_i$. Assim,

$$\sum_i d_k = \sum_i a_k b_i = a_k\,1 + a_k\,b_1 + \cdots + a_k b = a_k\,\sigma(b).$$

Variando os possíveis valores de a_k, obtemos

$$\begin{aligned}\sigma(n) &= \sum_k \sum_i d_k = \sum_k a_k\,\sigma(b) = 1\,\sigma(b) + a_1\,\sigma(b) + \cdots + a\,\sigma(b)\\ &= \sigma(a)\sigma(b),\end{aligned}$$

como queríamos demonstrar. □

A prova do próximo teorema, utilizando-se o Princípio da Indução, é imediata e ficará como exercício.

Teorema 13.1. *Considere um inteiro positivo $n \geq 2$ e sua fatoração única (TFA)*

$$n = p_1^{\alpha_1} \cdots p_m^{\alpha_m},$$

como um produto de números primos. Então,

$$\sigma(n) = \sigma\left(p_1^{\alpha_1}\right) \cdots \sigma\left(p_m^{\alpha_m}\right). \tag{33}$$

Calculemos $\sigma\left(p_j^{\alpha_j}\right)$ para $j \in \{1, 2, \ldots, m\}$ em (33). Como os divisores de $p_j^{\alpha_j}$ são

$$1,\ p_j,\ p_j^2, \ldots,\ p_j^{\alpha_j},$$

segue que, para cada $j \in \{1, 2, \ldots, m\}$,

$$\sigma\left(p_j^{\alpha_j}\right) = 1 + p_j + p_j^2 + \cdots + p_j^{\alpha_j} = \frac{p_j^{\alpha_j+1} - 1}{p_j - 1}.$$

Substituindo em (33), obtemos

$$\sigma(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdots \frac{p_m^{\alpha_m+1} - 1}{p_m - 1}. \tag{34}$$

Exemplo 13.1. *Utilizando (34), obtemos*

$$\sigma(6) = \sigma(2 \cdot 3) = \frac{2^{1+1} - 1}{2 - 1} \cdot \frac{3^{1+1} - 1}{3 - 1} = \frac{4 - 1}{1} \cdot \frac{9 - 1}{2} = 12 = 2 \cdot 6,$$

ou seja, $n = 6$ é um número perfeito.

Exemplo 13.2. *Utilizando (34), obtemos*

$$\sigma(45) = \sigma(3^2 \cdot 5) = \frac{3^{2+1} - 1}{3 - 1} \cdot \frac{5^{1+1} - 1}{5 - 1} = 13 \cdot 6 = 78 \neq 90 = 2 \cdot 45.$$

Concluimos que $n = 45$ não é um número perfeito.

O próximo teorema estabelece uma relação entre números perfeitos e primos de Mersenne.

Teorema 13.2. *Se M_p é um número primo de Mersenne, então*

$$n = 2^{p-1} M_p \tag{35}$$

é um número perfeito par. Além disso, todo número perfeito par é da forma

$$2^{p-1} M_p,$$

para algum número primo p e M_p um número primo de Mersenne.

Antes de demonstrarmos o teorema acima, observamos: não se conhece um número perfeito ímpar.

Prova do Teorema 13.2. Supondo que (35) é válida, segue que p é primo e, portanto, $p - 1 \geq 1$, de onde 2^{p-1} é múltiplo de 2 e, assim, n é par. Por hipótese, M_p é um primo de Mersenne, de onde 2^{p-1} e $M_p = 2^p - 1$ são relativamente primos. Do Lema 13.1,

$$\begin{aligned}\sigma(n) &= \sigma\left(2^{p-1}\right)\, \sigma\left(2^p - 1\right) = \frac{2^{p-1+1} - 1}{2 - 1}\left(2^p - 1 + 1\right) = \left(2^p - 1\right) 2^p \\ &= 2 \cdot 2^{p-1}\left(2^p - 1\right) = 2\, n,\end{aligned}$$

ou seja, n é um número perfeito, como queríamos demonstrar.

Seja n um número perfeito par, ou seja, $\sigma(n) = 2n$. Como n é par, tome 2^k a maior potência de 2 que divide n. Assim,

$$n = 2^k\, b, \tag{36}$$

sendo b ímpar. Como 2^k e b são relativamente primos, segue que

$$2^{k+1}b = 2n = \sigma(n) = \sigma(2^k)\,\sigma(b) = \frac{2^{k+1}-1}{2-1}\,\sigma(b)$$
$$= \left(2^{k+1}-1\right)\,\sigma(b),$$

ou seja,

$$2^{k+1}b = \left(2^{k+1}-1\right)\,\sigma(b).$$

Como

$$2^{k+1} \quad \text{e} \quad 2^{k+1}-1$$

são relativamente primos, segue que b divide $2^{k+1}-1$, ou seja,

$$b = \left(2^{k+1}-1\right)\,c, \tag{37}$$

para algum inteiro positivo c. Assim,

$$\sigma(b) = 2^{k+1}c. \tag{38}$$

Pelo que vimos acima,

$$1,\ 2^{k+1}-1,\ c,\ b$$

dividem b. Suponha que $c > 1$. Neste caso, de (37) e de (38), temos

$$b + c \overset{(37)}{=} 2^{k+1}c \overset{(38)}{=} \sigma(b) \geq 1 + \left(2^{k+1}-1\right) + b + c = 2^{k+1} + b + c,$$

o que resulta numa contradição. Logo,

$$c = 1,\ b = 2^{k+1}-1 \text{ e } \sigma(b) = 2^{k+1}.$$

Isso implica que $b = M_{k+1}$ é primo e, pela Proposição 13.1, segue que $p = k+1$ é primo. Em resumo, de (36), resulta

$$n \overset{(36)}{=} 2^k\, b = 2^{p-1}\, M_p,$$

como queríamos demonstrar. □

Exercício 13.1. *Dê uma prova para o Teorema 13.1.*

Exercício 13.2. *Dizemos que um número inteiro positivo n é um* número deficiente *se as somas dos seus divisores próprios é menor que n. De modo análogo, dizemos que um número inteiro positivo n é um* número abundante *se as somas dos seus divisores próprios é maior que n. Mostre que existem infinitos números deficientes. Mostre também que existem infinitos números abundantes. Decida se $n = 945$ é deficiente, perfeito ou abundante, justificando a sua resposta.*

14 Congruências e aplicações I: Teoremas de Wilson e de Fermat

Iniciamos esta seção estudando em exemplo.

Exemplo 14.1. *Este exemplo é uma questão do nível 1 da primeira etapa da Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP) de 2012 e pode ser encontrado em* http://www.obmep.org.br. *Um quadrado de lado* 1 *cm roda em torno de um quadrado de lado* 2 *cm, como na Figura 14, partindo da posição inicial e completando um giro cada vez que um de seus lados fica apoiado em um lado do quadrado maior.*

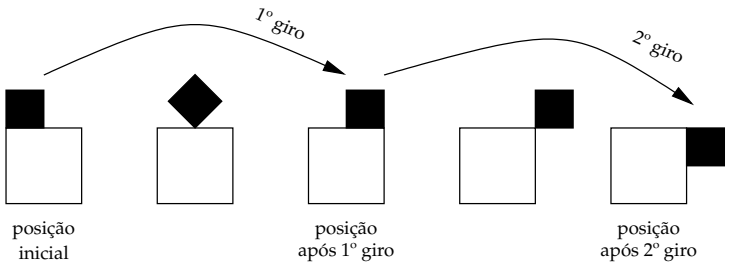

Figura 14: Posições do quadrado de lado 1 cm.

Qual das figuras esboçadas na Figura 15 representa a posição dos dois quadrados após 2012 giros?

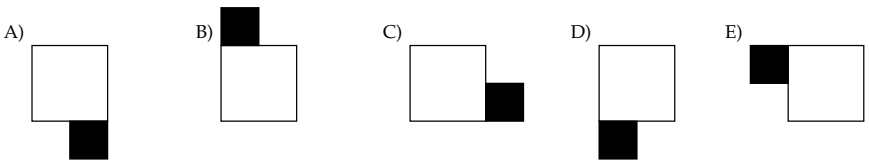

Figura 15: Possíveis posições dos dois quadrados após 2012 giros.

Verifica-se que após oito giros sucessivos o quadrado menor retorna à sua posição inicial. Deste modo, basta encontrar o resto da divisão de 2012 por 8,

$$2012 = 8 \cdot 251 + 4.$$

Assim, após 251 *voltas no quadrado maior, o quadrado menor retorna à posição inicial. Sobram, na análise, apenas* 4 *giros. Portanto, a resposta correta é a alternativa A.*

Daremos uma ideia da aritmética dos "restos" proposta por Gauss. Considere $a, b \in \mathbb{Z}$ e $m \in \mathbb{N}$. Dizemos que a *é congruente a* b *módulo* m se

$$m \mid (a - b).$$

Denotaremos isso por

$$a \equiv b \pmod{m}.$$

Se

$$m \nmid (a-b),$$

dizemos que a *é incongruente a* b *módulo* m ou a *é não congruente a* b *módulo* m e denotamos por

$$a \not\equiv b \pmod{m}.$$

Exemplo 14.2. $11 \equiv 3 \pmod{2}$, *pois* $2 \mid (11-3) = 8$.

Exemplo 14.3. $17 \not\equiv 11 \pmod{5}$, *pois* $5 \nmid (17-11) = 6$.

Veremos, a seguir, alguns resultados a respeito da ideia de congruência. Alguns serão demonstrados aqui, outros terão suas demonstrações deixadas como exercício.

Proposição 14.1. *Considere* $a, b \in \mathbb{Z}$ *e* $m \in \mathbb{N}$. *Assim,* $a \equiv b \pmod{m}$ *se, e somente se, existe* $k \in \mathbb{Z}$ *tal que* $a = b + k\,m$.

Demonstração. Se $a \equiv b \pmod{m}$, por definição, $m \mid (a-b)$, ou seja, existe $k \in \mathbb{Z}$ tal que $a - b = k\,m$, o que implica $a = b + k\,m$. Por outro lado, se existe $k \in \mathbb{Z}$ tal que $a - b = k\,m$, então $m \mid (a-b)$, ou seja, $a \equiv b \pmod{m}$. □

Proposição 14.2. *Considere* $a, b \in \mathbb{Z}$ *e* $m \in \mathbb{N}$. *As seguintes afirmações são verdadeiras:*

- $a \equiv a \pmod{m}$;
- *Se* $a \equiv b \pmod{m}$, *então* $b \equiv a \pmod{m}$;
- *Se* $a \equiv b \pmod{m}$ *e* $b \equiv c \pmod{m}$, *então* $a \equiv c \pmod{m}$.

A prova da Proposição 14.2 ficará como exercício. Por esta proposição verificamos que a relação de congruência é uma *relação de equivalência* no conjunto dos números inteiros.

Proposição 14.3. *Considere* $a, b, c \in \mathbb{Z}$ *e* $m \in \mathbb{N}$. *Suponha que* $a \equiv b \pmod{m}$. *As seguintes afirmações são verdadeiras:*

1. $a + c \equiv b + c \pmod{m}$;
2. $a - c \equiv b - c \pmod{m}$;
3. $a\,c \equiv b\,c \pmod{m}$.

Demonstração. Por hipótese, $a \equiv b \pmod{m}$, ou seja, existe $k \in \mathbb{Z}$, tal que $a - b = k\,m$. Agora,

$$(a + c) - (b + c) = a - b = k\,m,$$

o que implica que $a + c \equiv b + c \pmod{m}$, provando o item 1.

De modo análogo,

$$(a - c) - (b - c) = a - b = k\,m,$$

implicando que $a - c \equiv b - c \pmod{m}$, provando o item 2.

Por último,

$$a\,c - b\,c = c(a - b) = c\,k\,m,$$

o que implica que $m \mid (a\,c - b\,c)$ e, portanto, $a\,c \equiv b\,c \pmod{m}$. □

A prova da próxima proposição ficará como exercício.

Proposição 14.4. *Considere $a, b, c, d \in \mathbb{Z}$ e $m \in \mathbb{N}$. Suponha que*

$$a \equiv b \pmod{m} \quad e \quad c \equiv d \pmod{m}.$$

As seguintes afirmações são verdadeiras:

1. $a + c \equiv b + d \pmod{m}$);
2. $a - c \equiv b - d \pmod{m}$;
3. $a\,c \equiv b\,d \pmod{m}$.

Proposição 14.5. *Considere $a, b, c \in \mathbb{Z}$ e $m \in \mathbb{N}$. Suponha que $d = (c, m)$ e que $a\,c \equiv b\,c \pmod{m}$. Então, $a \equiv b \pmod{m/d}$. Em particular, se $(c, m) = d = 1$, então, $a \equiv b \pmod{m}$.*

Demonstração. Por hipótese, $a\,c - b\,c = c(a - b) = k\,m$. Dividindo ambos os membros por d, temos

$$(c/d)(a - b) = k(m/d), \quad \text{com} \quad c/d,\ m/d \in \mathbb{Z},$$

ou seja, $(m/d) \mid (c/d)(a - b)$. Como $(m/d, c/d) = 1$, segue que

$$(m/d) \mid (a - b) \implies a \equiv b \pmod{m}/d,$$

como queríamos provar. □

Considere $h, k \in \mathbb{Z}$ e $m \in \mathbb{N}$, com $h \equiv k \pmod{m}$. Neste caso, dizemos que k *é um resíduo de* h *módulo* m.

O conjunto de números inteiros

$$\{r_1,\ r_2, \ldots,\ r_s\}$$

é um *sistema completo de resíduos módulo* m se:

- $r_i \not\equiv r_j \pmod{m}$, com $i \neq j$;
- para todo $n \in \mathbb{Z}$ existe um r_i tal que $n \equiv r_i \pmod{m}$.

Exemplo 14.4. *Dado $m \in \mathbb{N}$, o conjunto $\{0,\ 1, \ldots,\ m-1\}$ é um sistema completo de resíduos módulo m.*

As provas das seguintes duas proposições serão omitidas.

Proposição 14.6. *Se um conjunto com k números inteiros $\{r_1,\ r_2, \ldots,\ r_k\}$ é um sistema completo de resíduos módulo m, então $k = m$.*

Proposição 14.7. *Se o conjunto $\{r_1,\ r_2, \ldots,\ r_m\}$ é um sistema completo de resíduos módulo m e $a,\ b \in \mathbb{Z}$, com $(a, m) = 1$, então o conjunto*

$$\{a\, r_1 + b,\ a\, r_2 + b, \ldots,\ a\, r_m + b\}$$

também é um sistema completo de resíduos módulo m.

Considere $a, b \in \mathbb{Z}$ e $m \in \mathbb{N}$. Chamamos de *congruência linear em uma variável* a uma congruência da forma

$$a\, x \equiv b \pmod{m}, \quad x \in \mathbb{Z}. \tag{39}$$

Suponha que $x_0 \in \mathbb{Z}$ é uma *solução* da congruência linear (39), isto é,

$$a\, x_0 \equiv b \pmod{m}.$$

Suponha que $x_1 \in \mathbb{Z}$ satisfaz $x_1 \equiv x_0 \pmod{m}$. Então, x_1 também é solução da congruência linear (39). De fato,

$$x_1 \equiv x_0 \pmod{m} \implies a\, x_1 \equiv a\, x_0 \pmod{m} \equiv b \pmod{m}.$$

Dada uma congruência linear, $a\, x \equiv b \pmod{m}$, quantas são as suas soluções incongruentes (não congruentes), caso exista alguma?

A próxima proposição responde a esta pergunta. A sua prova será omitida.

Proposição 14.8. *Considere $a, b \in \mathbb{Z}$ e $m \in \mathbb{N}$, com $(a, m) = d$. Valem as seguintes afirmações.*

- *Se $d \nmid b$, a congruência $a\, x \equiv b \pmod{m}$ não possui solução.*
- *Se $d \mid b$, a congruência $a\, x \equiv b \pmod{m}$ possui exatamente d soluções incongruentes módulo m.*

Dizemos que uma solução $x_0 \in \mathbb{Z}$ da congruência linear $a\, x \equiv b \pmod{m}$ é *única módulo m* quando qualquer outra solução $x_1 \in \mathbb{Z}$ for congruente a x_0 módulo m.

Uma solução $\overline{a} \in \mathbb{Z}$ de $a\, x \equiv 1 \pmod{m}$ é chamada de *inverso de $a \in \mathbb{Z}$ módulo m*. Se $(a, m) = 1$, então, da Proposição 14.8, segue que $a \in \mathbb{Z}$ possui um único inverso módulo m.

A próxima proposição dá informações quando $a \in \mathbb{Z}$ é o seu próprio inverso módulo um número primo p.

Proposição 14.9. *Considere p um primo. O número $a \in \mathbb{N}$ é o seu próprio inverso módulo p se, e somente se, $a \equiv 1 \pmod{p}$ ou $a \equiv -1 \pmod{p}$.*

Demonstração. Se a é o seu próprio inverso módulo p, então $a^2 \equiv 1 \pmod{p}$, o que significa que

$$p \mid (a^2 - 1) = (a+1)(a-1).$$

Assim, $p \mid (a-1)$ ou $p \mid (a+1)$, de onde $a \equiv 1 \pmod{p}$ ou $a \equiv -1 \pmod{p}$. Por outro lado, se $a \equiv 1 \pmod{p}$ ou $a \equiv -1 \pmod{p}$, então $p \mid (a-1)$ ou $p \mid (a+1)$. Portanto,

$$p \mid (a+1)(a-1) = a^2 - 1.$$

Assim, $a^2 \equiv 1 \pmod{p}$, ou seja, a é o seu próprio inverso módulo p, como queríamos demonstrar. □

Como aplicações da ideia de congruência, faremos, na próxima seção, as provas completas dos seguintes dois teoremas.

Teorema 14.1 (Teorema de Wilson)**.** *O número $p \in \mathbb{N}$ é primo se, e somente se, $p \mid (p-1)! + 1$, ou equivalentemente,*

$$(p-1)! \equiv -1 \pmod{p}.$$

Teorema 14.2 (Pequeno Teorema de Fermat)**.** *Considere $p \in \mathbb{N}$ um número primo. Se $p \nmid a$, então*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Faremos, agora, a prova de uma parte do Teorema 14.1 (Wilson).

Demonstração. **Parte 1.** Se $p \mid (p-1)! + 1$, então p é primo.

Faremos a prova por contradição. Suponha que p não é um número primo, ou seja, existem números inteiros $a > 1$ e $b > 1$, tais que

$$p = a\,b.$$

Em particular, $b < p$, o que implica que $b \mid (p-1)!$. Agora, por hipótese, $p \mid (p-1)! + 1$ e como $b \mid p$, segue, por transitividade, que $b \mid (p-1)! + 1$. Assim, do que vimos, $b \mid (p-1)!$ e $b \mid (p-1)!+1$, de onde b divide a diferença

$$(p-1)! + 1 - (p-1)! = 1,$$

um absurdo.

Parte 2. Se p é primo, então $p \mid (p-1)! + 1$, ou equivalentemente,

$$(p-1)! \equiv -1 \pmod{p}.$$

A prova da Parte 2 ficará para a próxima seção. □

Observação 14.1. *A afirmação da Parte 2 do Teorema 14.1 (Wilson) é: se p é primo, então $p \mid (p-1)! + 1$, ou equivalentemente,*

$$(p-1)! \equiv -1 \pmod{p}.$$

Afirmamos que p é o menor número primo com essa propriedade. De fato, suponha que exista um número primo $q < p$, tal que $q \mid (p-1)! + 1$. Como $q < p$, então q é um fator de $(p-1)!$. Portanto, $q \mid (p-1)!$ e, assim, divide a diferença

$$(p-1)! + 1 - (p-1)! = 1,$$

um absurdo.

Exercício 14.1. *Utilizando o Teorema 14.1 (Wilson), encontre o menor resíduo positivo de*

$$6 \cdot 7 \cdot 8 \cdot 9 \quad \textit{módulo} \quad 5.$$

Exercício 14.2. *Utilizando o Teorema 14.2 (Pequeno Teorema de Fermat), encontre o resto da divisão de*

$$2^{100.000} \quad \textit{por} \quad 17.$$

15 Congruências e aplicações II: Teoremas de Wilson e de Fermat

Nesta seção estudaremos as provas do Teorema de Wilson e do Pequeno Teorema de Fermat. Antes de exibirmos a prova do Teorema 14.1 (Wilson), discutiremos a ideia dessa prova no exemplo a seguir.

Exemplo 15.1. *Considere o número primo $p = 13$. Dentre os números*

$$1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11,\ 12,$$

somente os números 1 e 12 são os seus próprios inversos módulo 13. De fato, pela Proposição 14.9,

$$1 \equiv 1 \pmod{13} \quad e \quad 12 \equiv -1 \pmod{13},$$

e nenhum dos números restantes é congruente a 1 ou a -1 módulo 13. Como os números

$$2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11,$$

são relativamente primos com 13, pela Proposição 14.8, cada um deles possui um único inverso módulo 13. Eles podem ser agrupados em

$$5 = \frac{13-3}{2}$$

pares da forma

$$2 \cdot 7 \equiv 1 \pmod{13}, \quad 3 \cdot 9 \equiv 1 \pmod{13}, \quad 4 \cdot 10 \equiv 1 \pmod{13},$$
$$5 \cdot 8 \equiv 1 \pmod{13}, \quad 6 \cdot 11 \equiv 1 \pmod{13}.$$

Pelo item 3 da Proposição 14.4, podemos multiplicar essas congruências membro a membro, obtendo

$$2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \equiv 1 \pmod{13}.$$

Multiplicando ambos os membros por 12*, teremos*

$$2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \equiv 12 \pmod{13}.$$

O membro esquerdo é $12! = (13-1)!$*. Por outro lado, o membro direito pode ser escrito da forma* $12 \equiv -1 \pmod{13}$*. Assim,*

$$(13-1)! \equiv -1 \pmod{13},$$

como queríamos mostrar.

Prova do Teorema 14.1 (Wilson). **Parte 1.** Se $p \mid (p-1)! + 1$, então p é primo. Faremos a prova por contradição. Suponha que p não é primo, ou seja, existem números inteiros $a > 1$ e $b > 1$, tais que

$$p = a\,b.$$

Em particular, $b < p$, o que implica que $b \mid (p-1)!$. Agora, por hipótese, $p \mid (p-1)! + 1$ e como $b \mid p$, segue que $b \mid (p-1)! + 1$, por transitividade. Assim, $b \mid (p-1)!$ e $b \mid (p-1)! + 1$, de onde b divide a diferença

$$(p-1)! + 1 - (p-1)! = 1,$$

um absurdo.
Parte 2. Se p é primo, então

$$p \mid (p-1)! + 1 \iff (p-1)! \equiv -1 \pmod{p}.$$

Considere o número primo $p = 2$. Assim,

$$(p-1)! + 1 = (2-1)! + 1 = 1 + 1 = 2,$$

é divisível por $p = 2$. Considere, agora, um número primo $p \geq 3$, arbitrário, fixado e a congruência linear

$$a\,x \equiv 1 \pmod{p}. \tag{40}$$

Considere o conjunto

$$C = \{1,\ 2, \ldots,\ p-1\}.$$

Se $a \in C$, então $(a, p) = 1$. Segue, assim, da Proposição 14.8, que a congruência linear (40) tem uma única solução para todo $a \in C$. Segue ainda que, no conjunto C, apenas $a = 1$ e $a = p-1$ são seus próprios inversos módulo p. De fato, da Proposição 14.9, $a = 1$ é congruente a 1 módulo p e $a = p-1$ é congruente a -1 módulo p.

Afirmação. Pode-se agrupar os elementos restantes do conjunto C, quais sejam, $2,\ 3,\ \ldots,\ p-2$, em $(p-3)/2$ pares cujos produtos são congruentes a 1 módulo p.

Multiplicando essas congruências membro a membro (item 3 da Proposição 14.4), obtemos

$$2 \cdot 3 \cdot 4 \cdots (p-2) \equiv 1 \pmod{p}.$$

Multiplicando ambos os membros da congruência acima por $p-1$ (item 3 da Proposição 14.3), teremos

$$2 \cdot 3 \cdot 4 \cdots (p-2)\,(p-1) \equiv (p-1) \pmod{p}.$$

Como $p - 1 \equiv -1 \pmod{p}$, segue da congruência acima que

$$(p-1)! \equiv (p-1) \pmod{p} \equiv -1 \pmod{p},$$

terminando a prova da Parte 2. □

No exemplo a seguir, ilustraremos a ideia da prova do Teorema 14.2 (Pequeno Teorema de Fermat).

Exemplo 15.2. *Considere $p = 11$ e $a = 5$. Como $p = 11 \nmid 5 = a$, queremos mostrar que $a^{p-1} = 5^{10} \equiv 1 \pmod{p = 11}$. Considere a seguinte lista:*

$$\begin{aligned}
1 \cdot 5 &\equiv 5 \pmod{11}, & 2 \cdot 5 &\equiv 10 \pmod{11},\\
3 \cdot 5 &\equiv 4 \pmod{11}, & 4 \cdot 5 &\equiv 9 \pmod{11},\\
5 \cdot 5 &\equiv 3 \pmod{11}, & 6 \cdot 5 &\equiv 8 \pmod{11},\\
7 \cdot 5 &\equiv 2 \pmod{11}, & 8 \cdot 5 &\equiv 7 \pmod{11},\\
9 \cdot 5 &\equiv 1 \pmod{11}, & 10 \cdot 5 &\equiv 6 \pmod{11}.
\end{aligned}$$

Note que 11 não divide nenhum dos produtos

$$j \cdot 5, \quad j \in \{1,\ 2, \ldots,\ 9,\ 10\},$$

que estão nos membros esquerdos das congruências da lista acima. Note também que esses produtos são dois a dois incongruentes módulo 11. De fato,

$$5 \cdot j \equiv 5 \cdot k \pmod{11} \implies j \equiv k \pmod{11},$$

com $j,\ k \in \{1,\ 2, \ldots,\ 9,\ 10\}$*, de onde* $j = k$*. Das duas observações acima, resulta que cada produto da forma* $j \cdot 5$ *deve ser congruente a um número diferente do conjunto*

$$D = \{1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10\}.$$

Observe que os números do conjunto D *aparecem, sem repetições, nos membros direitos das congruências da lista inicial. Podemos multiplicar, membro a membro, as congruências dessa lista, obtendo*

$$(1 \cdot 5) \cdot (2 \cdot 5) \cdots (10 \cdot 5) \equiv 5 \cdot 10 \cdot 4 \cdot 9 \cdot 3 \cdot 8 \cdot 2 \cdot 7 \cdot 1 \cdot 6 \pmod{11}.$$

A expressão acima pode ser escrita da forma

$$5^{10} \cdot 10! \equiv 10! \pmod{11}.$$

Como $(10!, 11) = 1$*, pela Proposição 14.5,* $5^{10} \equiv 1 \pmod{11}$*, como queríamos mostrar.*

Prova do Teorema 14.2 (Pequeno Teorema de Fermat). O conjunto formado pelos p números

$$E = \{0,\ 1,\ 2, \ldots,\ p-1\}$$

é um sistema completo de resíduos módulo p. Isto implica, em particular, que qualquer conjunto contendo, no máximo, p elementos incongruentes módulo p pode ser colocado em correspondência bijetora com um subconjunto do conjunto E. Considere, agora, o conjunto

$$F = \{a,\ 2a,\ 3a, \ldots,\ (p-1)a\}.$$

Como, por hipótese, $(a, p) = 1$, nenhum elemento do conjunto F é divisível por p, ou seja, nenhum deles é congruente a zero módulo p. Por outro lado, quaisquer dois elementos (distintos) de F são incongruentes módulo p. De fato,

$$a\,j \equiv a\,k \pmod{p} \quad \Longrightarrow \quad j \equiv k \pmod{p}$$

o que só é possível se $j = k$, uma vez que ambos j e k são positivos e menores que p. Em resumo, o conjunto F contém $p-1$ números incongruentes módulo p e não divisíveis por p. Logo, cada um deles é congruente a exatamente um dentre os números

$$1,\ 2,\ 3, \ldots,\ p-1.$$

Se multiplicarmos essas congruências membro a membro, teremos

$$a \cdot (2a) \cdot (3a) \cdots ((p-1)a) \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p},$$

ou seja,

$$a^{p-1} \cdot (p-1)! \equiv (p-1)! \pmod{p}.$$

Como $((p-1)!, p) = 1$, podemos cancelar o fator $(p-1)!$ em ambos os membros, obtendo

$$a^{p-1} \equiv 1 \pmod{p},$$

como queríamos demonstrar. □

Agradecimentos

O autor foi parcialmente apoiado pela Fundação de Amparo à Pesquisa do Estado de Minas Gerais (projetos números APQ-02153-23, RED-00133-21 e APQ-05207-23). O autor agradece a calorosa hospitalidade da Universitat Autònoma de Barcelona durante a redação deste artigo.

Referências

[1] M. Aigner, G.M. Ziegler, Proofs from The Book, fourth edition. Springer-Verlag, Berlin, 2010.

[2] M. El Bachraoui, *Bertrand's postulate for high-school students*, International Journal of Mathematical Education, **9** (2019), 73-77.

[3] A.R. Booker, *On Mullin's second sequence of primes*, Integers, **12** (2012), 1167-1177.

[4] J.-R. Chen, *On the representation of a larger even integer as the sum of a prime and the product of at most two primes*, Sci. Sinica, **16** (1973), 157-176.

[5] H.-B. Chen, H.-L. Fu, J.-Y. Guo, *From a consequence of Bertrand's Postulate to Hamilton cycles*, arXiv:1804.07104 [math.CO], 2018.

[6] U. Dudley, *History of a formula for primes*, Amer. Math. Monthly, **76** (1969), 23-28.

[7] Euclides, Os Elementos/Euclides, tradução e introdução de Irineu Bicudo, Editora UNESP, São Paulo, 2009.

[8] J. Gimbert, *Fem matemàtiques treballant amb els nombres primers*, Materials Matemàtics, vol. 2009 (2009), no. 7, pp. 30.

[9] H.A. Helfgott, *The ternary Goldbach conjecture is true*, arXiv:1312.7748v2 [math.NT], 2013-2014.

[10] F. Martinez, C.G. Moreira, N. Saldanha, E. Tengan, Teoria dos Números - um passeio com primos e outros números familiares pelo mundo inteiro, 5ª edição, IMPA, 2018.

[11] J. Maynard, *Small gaps between primes*, Ann. of Math., **181** (2015), 383-413.

[12] J.P. de Oliveira Santos, Introdução à Teoria dos Números, 3ª edição, IMPA, 2020.

[13] D.H.J. Polymath, *Variants of the Selberg sieve, and bounded intervals containing many primes*, Res. Math. Sci., **1** (2014), Art. 12, 83 pp.

[14] P. Ribenboim, Números Primos: mistérios e recordes, IMPA, 2001.

[15] D. Shanks, *Euclid's primes*, Bull. Inst. Combin. Appl., **1** (1991), 33-36.

[16] R.G. Watanabe, *Uma fórmula para os números primos*, CD da Revista do Professor de Matemática, São Paulo, IME-USP, 2012.

[17] Y. Zhang, *Bounded gaps between primes*, Ann. of Math., **179** (2014), 1121-1174.

Instituto de Matemática e Computação
Universidade Federal de Itajubá
lfmelo@unifei.edu.br
ORCID: http://orcid.org/0000-0002-4989-3052

Publicat el 26 de gener de 2026