Primos de Fermat, Primos de Mersenne, Números Perfeitos e O Fatorial

Gabriel Lúcio de Araújo RA: 172233 Matheus Luís Bernardi RA: 184331
Daniel Aguilar Gomes RA: 166163
Lucas Henrique Silveira Gomes RA: 172797 Maico Gouveia RA: 156502

Novembro de 2017

1 Introdução

Apresentamos neste trabalho uma coleção de resultados sobre os primos de Fermat, os primos de Mersenne e sua relação com os números perfeitos, terminando com a decomposição do Fatorial em fatores primos segundo o teorema fundamental da aritmética.

2 Primos de Fermat

Nesta seção abordaremos sobre os números de Fermat através de uma breve introdução histórica e alguns resultados sobre estes tipos especiais de números.

2.1 Breve Introdução

Pierre de Fermat(1601-1665) foi um jurista e matemático amador francês que se interessava profundamente pela Teoria dos Números -sendo considerado o primeiro matemático a contribuir para este ramo do ponto de vista teórico- na qual obteve muitos resultados inestimáveis para a matemática; e conjecturou uma fórmula de números primos, os que hoje são chamados números de Fermat. Esta conjectura foi lançada em 1640 em uma carta a Marin Mersenne, outro matemático da época, na qual Fermat afirmava que todos os números da forma $2^{2^n}+1$, com $n \in \mathbb{N}$, eram primos.

Fermat morreu com a convicção de que tinha encontrado uma fórmula para números primos, mas em 1732 o matemático Leonhard Euler mostrou que para n=5, $2^{2^5}+1 = 4.294.967.297 = 641 \times 6.700.417$, portanto um número composto, desmentindo a conjectura de Fermat.

2.2 Os números de Fermat

Um número de Fermat, como visto acima, é um número da forma:

$$F_n = 2^{2^n}+1 \tag{1}$$

De n=0 até n=4 obtemos números primos, estes são chamados de primos de Fermat. Apesar de Euler ter comprovado que para n=5 obtemos um número composto e para alguns outros valores de n temos números compostos, não se sabe ainda hoje se existem outros primos de Fermat além destes 5 iniciais para valores de n grandes.

A título de curiosidade, a prova de que 641 é um fator de F_5 se dá através da aritmética dos restos. Veja que:

$$641 = 2^7 \times 5 + 1 \tag{2}$$
$$641 = 2^4 + 5^4 \tag{3}$$

De (2) temos que $2^7 \times 5 \equiv -1 \pmod{641}$ e,portanto, ao elevar à quarta potência $2^{28} \times 5^4 \equiv 1 \pmod{641}$. Por outro lado, de (3) temos que $5^4 \equiv -2^4 \pmod{641}$. Destas duas congruências obtemos que $-2^{32} \equiv 1 \pmod{641}$, o que implica que 641 é fator de $2^{32}+1 = 2^{2^5}+1$

2.3 Propriedades dos números de Fermat

Agora vamos enunciar algumas propriedades interessantes dos números de Fermat. Todo número de Fermat satisfaz as seguintes relações de recorrência:

1. $F_n = (F_{n-1} - 1)^2 + 1$ para $n \geq 1$
2. $F_n = F_{n-1} + 2^{n-1} F_0 \cdots F_{n-2}$
3. $F_n = F_{n-1}^2 - 2(F_{n-2} - 1)^2$
4. $F_{n+k} - 1 = (F_n - 1)^{2^k}$

Todas estas relações podem ser provadas por indução matemática finita. Em particular, temos mais uma relação de recorrência, a qual iremos demonstrar para que o leitor tenha alguma visualização concreta.

Afirmação 1. Todo número de Fermat é igual ao produto de seus anteriores somado a 2.

$$F_n = F_0 \cdots F_{n-1} + 2 \tag{4}$$

Demonstração. Para $n = 1$, temos:

$$F_1 = 5 \tag{5}$$

$$F_0 + 2 = 3 + 2 = 5 \tag{6}$$

Como 5=5, temos que vale para $n = 1$. Agora supomos válido para um $n = k - 1$ e vamos provar para $n = k$:

Temos que:

$$\begin{aligned} F_0 \cdots F_{n-1} + 2 &= (F_{n-1} - 2)F_{n-1} + 2 \\ &= (2^{2^{n-1}} + 1 - 2)(2^{2^{n-1}} + 1) + 2 \\ &= 2^{2^n} + 1 = F_n \end{aligned}$$

□

Agora enunciaremos um resultado interessante de Christian Goldbach:

Teorema 2.1. *Sejam F_n e F_m números de Fermat tais que $n \neq m$. Então, F_n e F_m são coprimos.*

Demonstração. Suponha por absurdo que F_n e F_m tenham um divisor p em comum tal que p é primo. Como F_n e F_m são ímpares, p tem que ser ímpar. Sem perda de generalidade, suponha que $m > n$. Então, $m = n + k$ para algum $k \in \mathbb{N}$. Temos que:

$$\begin{aligned} F_m - 1 &\equiv -1 (mod\ p) \\ F_n - 1 &\equiv -1 (mod\ p) \\ \implies (F_n - 1)^{2^k} &\equiv -1 (mod\ p) \\ \implies (-1)^{2^k} &\equiv -1 (mod\ p) \\ \implies 1 &\equiv -1 (mod\ p) \\ \implies 0 &\equiv \quad 2 (mod\ p) \end{aligned}$$

Então, $p = 2$. Mas p é ímpar por hipótese. Absurdo! Portanto, não existe tal p e o resultado segue. □

Este teorema nos dá como corolário mais uma prova de que os números primos são infinitos: para cada F_n escolha um fator primo p_n; então a sequência (p_n) é uma sequência infinita de primos distintos. Para encerrar esta seção, deixaremos algumas perguntas ainda em aberto para o leitor:

1. Para $n > 4$, todo F_n é composto?
2. Existem infinitos primos de Fermat?
3. Existem infinitos números de Fermat compostos?
4. Existe algum número de Fermat que não tem como fator um quadrado perfeito?

Enfim, até hoje intriga aos matemáticos estes números especiais de Fermat. Muitas questões ainda estão para ser descobertas e muitas outras perguntas surgirão para alimentar ainda mais o avanço da Teoria dos Números.

3 Primos de Mersenne

Durante muitos séculos, diversos matemáticos acreditavam que todos os números da forma $2^n - 1$ com n primo fossem primos. Entretanto, em 1536 Hudalricus Regius mostrou que $2^{11} - 1$ era composto. A classificação de tais números com relação a serem primos ou não continuou e na primeira metade do século 17 Marin Mersenne publicou sua lista de primos

$$2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$$

para os quais acreditava que o número $2^p - 1$ seria primo. Ele pouco revelou sobre como chegou a esta lista, mas alguns anos mais tarde outros matemáticos apontaram erros nela, como inclusão de números compostos e omissão de números primos. Somente três séculos mais tarde esta lista (até o expoente 257) foi completada e verificada rigorosamente. Apesar dos erros cometidos, Mersenne ainda ficou conhecido por tais números. Abaixo mostraremos alguns dos resultados referentes aos chamados primos de Mersenne.

Definição 3.1. É dito primo de Mersenne todo número primo da forma $M_n = 2^n - 1$, onde n é um número natural.

Com o seguinte resultado, o número de possíveis primos de Mersenne é muito reduzido.

Teorema 3.1. *Se $2^n - 1$ é primo então n é primo.*

Demonstração. Suponha $n = ab$ com $a, b > 1$. Como $2^a - 1 > 1$, segue que $2^n - 1 = 2^{ab} - 1 = (2^a)^b - 1 \equiv 1^b - 1 = 0 \mod (2^a - 1)$, provando que $2^n - 1$ é composto. □

Este teorema e o fato de que os primos de Mersenne se tornam rapidamente gigantescos são parte do sucesso deles, já que, em novembro de 2017, os seis maiores primos conhecidos são primos deste tipo. A título de exemplo, o maior primo conhecido nesta mesma data é $2^{74207281} - 1$ que possui 22.338.618 dígitos. A descoberta de tais números se baseia em algoritmos que testam a primalidade de candidatos a primos. Algoritmos que testam a primalidade de primos de Mersenne têm como base o teste de Lucas-Lehmer, apresentado a seguir.

Teorema 3.2 (Teste de Lucas-Lehmer)**.** *Para todo primo ímpar p, o número de Mersenne $M_p = 2^p$ é primo se, e somente se, M_p divide S_{p-2}, onde $S_{n+1} = S_n^2 - 2$ e $S_0 = 4$.*

Não provaremos este teorema pois sua prova foge do escopo deste trabalho. Entretanto, mostraremos o primeiro número de Mersenne não primo com expoente primo usando este teste.

Exemplo 1. Neste exemplo usaremos o teste de Lucas-Lehmer para mostrar que $M_{11} = 2047$ não é primo. Para isto, basta verificar que $S_9 \equiv 0 \mod (M_{11})$. As próximas congruências serão todas módulo 2047. Temos

$$S_0 = 4, S_1 = 14, S_2 = 194,$$
$$S_3 = 37634 \equiv 788,$$
$$S_4 = S_3^2 - 2 \equiv 788^2 - 2 = 620942 \equiv 701,$$
$$S_5 \equiv 701^2 - 2 = 491399 \equiv 119,$$
$$S_6 \equiv 14159 \equiv 1877,$$
$$S_7 \equiv 3525127 \equiv 240,$$
$$S_8 \equiv 57598 \equiv 282,$$
$$S_9 \equiv 79522 \equiv 1736 \neq 0.$$

Desta última congruência vemos que M_{11} não divide S_9 e, portanto, pelo teste de Lucas-Lehmer, M_{11} não é primo.

Apesar dos números da sequência S_n crescerem muito rapidamente, os cálculos são feitos módulo M_p, o que torna viável sua execução. Note que este teste não é viável para cálculos à mão, e como tal teste foi inventado por volta de 1870 e aperfeiçoado de modo a torná-lo simples em 1930, naturalmente ele não foi usado para provar a primalidade dos primeiros números de Mersenne compostos. Com o teorema abaixo, enunciado por Euler em 1750 e provado por Lagrange em 1775, é possível entender como tais testes eram feitos antes dos computadores.

Teorema 3.3. *Sendo p e $2p+1$ primos com $p \equiv 3 \mod 4$, tem-se que $2p+1|M_p$.*

Demonstração. Seja $q = 2p+1$. Então $M_p = 2^p - 1 = 2^{\frac{(q-1)}{2}} - 1 \equiv \left(\frac{2}{q}\right) - 1 \mod q$, pois sabe-se do estudo de resíduos quadráticos que para todo primo q, se $(2,q) = 1$ então $2^{\frac{q-1}{2}} = \left(\frac{2}{q}\right)$. Mas $p \equiv 3 \mod 4$ significa que $q = 2p+1 = 2(4n+3)+1 = 8n+7 \equiv 7 \mod 8$, para algum n natural. Como $\left(\frac{2}{q}\right) = (-1)^\kappa$, com $\kappa = [\frac{2}{q}] + [2 \cdot \frac{2}{q}] + \cdots + [\frac{q-1}{2} \cdot \frac{2}{q}] = 0$, ou seja, $\left(\frac{2}{q}\right) = 1$, segue que $M_p \equiv 0 \mod 2p+1$, e portanto $2p+1|M_p$. $\left(\frac{2}{q}\right)$ □

Observe que usando este teorema é possível não só mostrar que M_{11} não é primo, mas que 23 é um de seus fatores. De fato, nos termos do teorema temos que $p = 11$ e $2p+1 = 23$ são primos, além de que $11 \equiv 3 \mod 4$ e, portanto, $23|M_{11}$, provando que este número de Mersenne não é primo.

Como adendo, os números primos p tais que $2p+1$ também é primo são chamados de primos de Sophie Germain. Logo, todo primo deste tipo congruente a três módulo 4 será índice de um número de Mersenne composto. A lista com os primeiros vinte primos de Sophie Germain é

$$2, 3, 5, 11, 23, 29, 41, 53, 83, 89, 113, 131, 173, 179, 191, 233, 239, 251, 281, 293.$$

Atualmente existem projetos colaborativos que buscam primos de Mersenne, como o GIMPS (Great Internet Mersenne Prime Search). Os voluntários que participam de tal projeto utilizam um software em seus computadores pessoais que se baseia na computação em cluster (sistema de processamento distribuído) que divide o processo do cálculo entre os computadores que tenham o software instalado. Nesta busca por novos primos de Mersenne, diversos teoremas e algoritmos que se baseiam nos aqui apresentados são utilizados para conjecturar sobre a primalidade de um número de Mersenne e, posteriormente, checar novamente para comprovar se é primo ou não.

Finalizamos a seção com a apresentação de uma nova conjectura sobre os primos de Mersenne. A primeira conjectura, feita por Mersenne e apresentada no início da seção, se baseava na crença de Mersenne de que $2^p - 1$ seria primo se, e somente se, p fosse um primo da forma $2^{2n}+1, 2^{2n} \pm 3$ ou $2^{2n+1} - 1$. Provou-se mais tarde que as condições de tal conjectura não eram nem suficientes, nem necessárias. Mais recentemente Bateman, Selfridge, e Wagstaff defenderam a ideia da Nova Conjectura de Mersenne. Ela diz que se p é primo ímpar e se duas das três condições abaixo são satisfeitas, então a terceira também será satisfeita:

- $p = 2^k \pm 1$ ou $p = 4^k \pm 3$;
- $2^p - 1$ é primo;
- $(2^p + 1)/3$ é primo.

Até o momento, os únicos números conhecidos que satisfazem as três condições acima são $3, 5, 7, 13, 17, 19, 31, 61$ e 127. Este resultado foi verificado para todos os primos até pelo menos doze milhões.

4 Números perfeitos e primos de Mersenne

Para a numerologia, os números 6 e 28 são ambos vistos como símbolo de perfeição. Deus criara o universo em 6 dias e descansara no sétimo. A quantidade de dias que a Lua leva para completar uma volta em torno da Terra é de 28 dias. Não à toa, estes números foram ambos postos como números *perfeitos.* Em termos numerológicos, um divisor de um número distinto dele mesmo é chamado de uma parte do número. Os números 6 e 28 possuem uma interessante propriedade relacionada a este termo: ambos são iguais a soma de suas partes. De fato,

$$6 = 1 + 2 + 3$$

$$28 = 1 + 2 + 4 + 7 + 14.$$

Assim, um número perfeito seria aquele que é dado pela soma de suas partes. Além dessa notável propriedade, estes números também possuem uma curiosa relação com os primos de Mersenne que já apresentamos anteriormente. Mostraremos aqui como tal relação se dá. Mas para tanto, precisaremos de uma abordagem mais precisa e menos misticista, o que requer um trabalho maior do arsenal matemático à disposição.

Definição 4.1. Dados $n, d \in \mathbb{N}$, diremos que d é um divisor próprio de n se $d|a$ e $d < n$.

Definição 4.2. Dado $n \in \mathbb{N}$ natural, denotaremos por $\sigma(n)$ a soma de todos os divisores de n. Denotaremos também por $\sigma_0(n)$ a soma de todos os divisores próprios de n.

Veja que evidentemente se pode expressar $\sigma_0(n)$ em função de sigma por $\sigma_0(n) = \sigma(n) - n$. Além disso, é imediato que $\sigma(1) = 1$. Ainda, se p denota primo, também é imediato $\sigma(p) = p + 1$, pela própria definição de primo. Assim, buscaremos determinar valores menos óbvios para $\sigma(n)$, onde n é natural qualquer composto, $n \geq 2$.

Primeiro, consideremos um caso mais simples. Suponhamos que seja $n = ab$ com a, b naturais tais que $(a, b) = 1$. Temos o seguinte lema:

Lema 4.1. *Seja $n \in \mathbb{N}$ composto tal que $n = ab$, com $(a, b) = 1$. Então, $\sigma(n) = \sigma(a)\sigma(b)$.*

Demonstração. Como $(a, b) = 1$, vemos que os fatores primos de a e b são todos distintos. Portanto, qualquer divisor d de n tem de ser da forma $d = a_i b_i$, onde a_i é divisor de a e b_i é divisor de b. Denotando os divisores de a por: $1, a_1, \cdots, a$ e os divisores de b por: $1, b_1, \cdots, b$, então se tem $\sigma(a) = 1 + a_1 \cdots + a$ e $\sigma(b) = 1 + b_1 + \cdots + b$. Em seguida, fixado divisor a_k, consideremos todos os divisores de n da forma: $d_k = a_k b_i$. Veja que a soma deles será:

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

Agora, variando sobre todos os possíveis divisores a_k, então:

$$\sigma(n) = \sum_k \sum_i d_k = \sum_k a_k \sigma(b) = 1\sigma(b) + a_1\sigma(b) + \cdots + a\sigma(b) = \sigma(a)\sigma(b),$$

provando o resultado. □

O lema anterior mostra que σ é função multiplicativa quando a e b são primos entre si. E de fato ele dá uma pista de como generalizar este resultado para considerar qualquer n, já que pelo teorema fundamental da aritmética os fatores presentes na fatoração são sempre primos entre si. Veremos isto no teorema que segue.

Teorema 4.1. *Seja $n \in \mathbb{N}, n \geq 2$, cuja fatoração prima é dada por $n = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$. Então,*

$$\sigma(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdots \frac{p_r^{\alpha_r+1} - 1}{p_r - 1}.$$

Demonstração. Procedemos por indução em m para mostrar que $\sigma(n) = \sigma(p_1^{\alpha_1}) \cdots \sigma(p_m^{\alpha_m})$. De fato, a indução se inicia com $m = 2$, pois sendo $(p_1^{\alpha_1}, p_2^{\alpha_2}) = 1$, segue $\sigma(n) = \sigma(p_1^{\alpha_1})\sigma(p_2^{\alpha_2})$ pelo lema anterior.

Assim, admitindo a hipótese de indução para algum m, observamos que $(p_{m+1}^{\alpha_{m+1}}, p_j^{\alpha_j}) = 1$ para todo $j = 1, \cdots, m$. Consequentemente, vale que $(p_1^{\alpha_1} \cdots p_m^{\alpha_m}, p_{m+1}^{\alpha_{m+1}}) = 1$ e aplicando o lema anterior novamente, temos $\sigma(n) = \sigma(p_1^{\alpha_1} \cdots p_m^{\alpha_m})\sigma(p_{m+1}^{\alpha_{m+1}})$. Mas por hipótese de indução vale que $\sigma(p_1^{\alpha_1} \cdots p_m^{\alpha_m}) = \sigma(p_1^{\alpha_1}) \cdots \sigma(p_m^{\alpha_m})$ e, portanto, será $\sigma(n) = \sigma(p_1^{\alpha_1}) \cdots \sigma(p_{m+1}^{\alpha_{m+1}})$. A indução agora está completa.

Para completar a prova, basta sabermos calcular quanto vale $\sigma(p_j^{\alpha_j})$ para $j = 1, \cdots, m$. Assim, dado j, vemos que para uma potência prima da forma $p_j^{\alpha_j}$ seus divisores são todos potências do mesmo primo p_j: $1, p_j, p_j^2, \cdots, p_j^{\alpha_j}$. Logo, somando tais divisores vemos que

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

pela soma de progressões geométricas. Como isso vale para todo $1 \leq j \leq m$, o resultado segue. □

Temos o seguinte corolário:

Corolário 4.1. *Seja $n \in \mathbb{N}$. Então, n é primo se, e somente se, $\sigma(n) = n + 1$.*

Demonstração. A ida já foi provada durante o texto, observando a própria definição de primo. Porém, ela poderia ser provada também como aplicação direta do teorema anterior, pois será

$$\sigma(n) = \frac{n^2 - 1}{n - 1} = n + 1.$$

Para a volta, se valer $\sigma(n) = n + 1$, seguirá $n > 1$ e que n e 1 são os únicos divisores de n. Portanto, n será primo. □

Agora já estamos prontos para estabelecer em termos mais precisos o que seria um número perfeito.

Definição 4.3. Denotaremos por número perfeito a todo $n \in \mathbb{N}$ satisfazendo $\sigma(n) = 2n$.

Veja que esta definição se relaciona com aquela numerológica. De fato, aquela dizia que um número perfeito é a soma de suas partes, isto é, a soma de seus divisores próprios. Nesta linguagem, a definição se traduz para n é perfeito se $\sigma_0(n) = n$. Como vale $\sigma_0(n) = \sigma(n) - n$, então será $\sigma(n) = 2n$, como já definimos. O último teorema será de grande uso para decidir se um número é perfeito ou não. Vejamos alguns exemplos:

Exemplo 2.

$$\sigma(6) = \sigma(2.3) = \frac{2^2 - 1}{2 - 1} \cdot \frac{3^2 - 1}{3 - 1} = 12 = 2.6$$

$$\sigma(28) = \sigma(2^2.7) = \frac{2^3 - 1}{2 - 1} \cdot \frac{7^2 - 1}{7 - 1} = 56 = 2.28$$

$$\sigma(45) = \sigma(3^2.5) = \frac{3^2 - 1}{3 - 1} \cdot \frac{5^2 - 1}{5 - 1} = 78 \neq 90 = 2.45$$

E assim reconfirmamos pela nova definição que 6 e 28 são perfeitos e que 45 não é perfeito. Demais números perfeitos são: $496, 8128$ e 33550336, por exemplo. Esta nova definição também será muito útil para esclarecer a relação existente entre números perfeitos e primos de Mersenne. Tal relação será vista nos próximos teoremas.

Teorema 4.2. *Um natural da forma $n = 2^{p-1}(2^p - 1)$ é perfeito quando $2^p - 1$ é um primo de Mersenne. Além disso, n é par.*

Demonstração. Aplicamos o teorema anterior e verificamos se a definição é satisfeita. De fato, calculando $\sigma(n)$, vemos

$$\sigma(n) = \sigma(2^{p-1})\sigma(2^p - 1) = \frac{2^{p-1+1} - 1}{2 - 1} \cdot (2^p - 1 + 1) = 2^p(2^p - 1) = 2.2^{p-1}(2^p - 1) = 2n.$$

Portanto, n é um número perfeito. O fato de n ser par segue diretamente da hipótese de $2^p - 1$ ser primo de Mersenne. De fato, será p primo e então $p - 1 > 0$ garante que n seja par ao observamos a potência 2^{p-1} fator de n. □

Como uma curiosidade, o teorema que acabamos de demonstrar aparece nos Elementos do matemático grego Euclides. Mostramos agora a recíproca.

Teorema 4.3. *Todo número perfeito par é da forma $n = 2^{p-1}(2^p - 1)$ discutida anteriormente.*

Demonstração. Sendo n par, considere 2^{p-1} a maior potência de 2 que o divide e o escreva na forma $n = 2^{p-1}q$, com q ímpar. Observando que $(2^{p-1}, q) = 1$, seguirá $\sigma(n) = \sigma(2^{p-1})\sigma(q) = (2^p - 1)\sigma(q)$ pela propriedade multiplicativa de σ. Como n é perfeito, então será $\sigma(n) = 2n$ por definição. Logo, igualando isto ao que acabamos de ver, obteremos $\sigma(n) = (2^p - 1)\sigma(q) = 2^p q$. Mas lembrando que $\sigma_0(q) = \sigma(q) - q$, então $(2^p - 1)(\sigma_0(q) + q) = 2^p q$. Resolvendo para q, vemos que

$$q = (2^p - 1)\sigma_0(q).$$

Desta relação, concluímos que $d = \sigma_0(q)$ é um divisor próprio de q. Contudo, veja que $\sigma_0(q)$ é, por definição, a soma de todos os divisores próprios de q, incluindo o próprio d, e portanto não deve existir outros divisores próprios além de d. Assim, seguirá do corolário anterior que q é primo e consequentemente que $d = 1$. Portanto, vemos que $q = 2^p - 1$, de onde seguirá n da forma discutida. □

Assim, os dois teoremas que acabamos de apresentar discute a relação existente entre números perfeitos e primos de Mersenne. Com os primos de Mersenne é possível obter alguns dos números perfeitos, bastando para isso substituí-lo na fórmula $n = 2^{p-1}(2^p - 1)$. Por outro lado, vimos também que qualquer perfeito par é dessa mesma forma. No entanto, estes dois teoremas nada dizem a respeito da existência ou não de números perfeitos ímpares. Na verdade, esse é um problema que se mantém irresoluto até hoje em Teoria de Números. Nunca fora encontrado algum exemplo, mas diversos critérios a que este número deveria satisfazer já foram estabelecidos, mas nenhum deles suficiente para provar a não existência de tais números.

5 Decomposição do Fatorial em Fatores Primos

Seja $n \in \mathbb{N} \cup \{0\}$. Definimos o fatorial $n!$ de n por:

$$n! = \prod_{i=0}^{n-1} (n - i)$$

$$0! = 1$$

Pelo teorema fundamental da aritmética, temos que, dado um número natural n, este n é unicamente escrito como produto de potências de primos:

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

Nesta seção mostraremos como obter a fatoração do Fatorial em fatores primos.

Definamos $E_p(n)$ como a maior potência de p que aparece na fatoração de n em fatores primos. Também denotaremos por $\left[\frac{b}{a}\right]$ o quociente da divisão de b por a. Se $a > b$ definiremos $\left[\frac{b}{a}\right] = 0$.

Proposição 5.1. *Sejam $a \in \mathbb{N} \cup \{0\}$ e $b, c \in \mathbb{N}$. Então, temos que:*

$$\left[\frac{\left[\frac{a}{b}\right]}{c}\right] = \left[\frac{a}{bc}\right]$$

Demonstração. Sejam, $q_1 = \left[\frac{a}{b}\right]$ e $q_2 = \left[\frac{\left[\frac{a}{b}\right]}{c}\right]$. Dividindo a por b, obtemos: $a = bq_1 + r_1$, com $0 \leq r_1 \leq b - 1$. Dividindo q_1 por c, obtemos: $q_1 = cq_2 + r_2$, com $0 \leq r_2 \leq c - 1$ Logo: $a = bq_1 + r_1 = b(cq_2 + r_2) + r_1 = bcq_2 + br_2 + r_1$ Como $br_2 + r_1 \leq b(c-1) + b - 1 = bc - 1$ Assim, q_2 é o quociente da divisão de a por bc, ou seja:

$$q_2 = \left[\frac{a}{bc}\right]$$

□

Com o seguinte teorema poderemos encontrar cada potência máxima de cada primo p menor ou igual que n, do fatorial $n!$.

Teorema 5.1 (Legendre)**.** *Seja $n \in \mathbb{N} \cup \{0\}$ e seja p primo. Seja $k \in \mathbb{N}$ tal que $\forall r > k$, $p^r > n$ (tal k existe pelo princípio arquimediano dos naturais). Então:*

$$E_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots + \left[\frac{n}{p^k}\right] \text{ se } p \leq n$$

$$E_p(n!) = 0 \text{ se } p > n$$

Demonstração. Vamos demonstrar utilizando indução sobre n. Para $n = 0$ e $n = 1$ temos que $E_p(n!) = 0$, pois todo primo p é maior que 0 ou 1. Assim, é válido para $n = 0$ ou $n = 1$. Suponha que o resultado valha para todo natural $m < n$. Para $p > n$, temos que p não aparece no fatorial de n. Logo $E_p(n!) = 0$. Assim, seja p primo menor ou igual a n. Sabemos que os múltiplos de p entre 1 e n são:

$$p, 2p, 3p, \cdots, \left[\frac{n}{p}\right] p$$

De fato, para algum $0 \leq r < p$, temos $n = \left[\frac{n}{p}\right] p + r \geq p \left[\frac{n}{p}\right]$, mas para $\left(\left[\frac{n}{p}\right] + 1\right) p$:

$$\left(\left[\frac{n}{p}\right] + 1\right) p = \left[\frac{n}{p}\right] p + p > \left[\frac{n}{p}\right] p + r = n$$

Como todos os múltiplos de p entre 1 e n aparecem em $n!$, obtemos que p aparece pelo menos $\left[\frac{n}{p}\right]$ vezes em $n!$. Assim:

$$n! = n(n-1)\cdots\left[\frac{n}{p}\right] p \left(\left[\frac{n}{p}\right] p - 1\right)\cdots\left(\left[\frac{n}{p}\right] - 1\right) p \cdots \left(\left[\frac{n}{p}\right] - 2\right) p \cdots p(p-1)!$$

$$\implies n! = p^{\left[\frac{n}{p}\right]} \left(\left[\frac{n}{p}\right]\right)!(p-1)! \prod_{i=0}^{\left[\frac{n}{p}\right]-2} \prod_{j=1}^{p-1} \left(\left(\left[\frac{n}{p}\right] - i\right) p - j\right)$$

Agora, o termo $\prod_{i=0}^{\left[\frac{n}{p}\right]-2} \prod_{j=1}^{p-1} \left(\left(\left[\frac{n}{p}\right] - i\right) p - j\right)$ não possui potências de p, já que $j \neq p$. Logo, o termo $\left(\left[\frac{n}{p}\right]\right)!$ é o único que pode contribuir para potências de p em $n!$. Portanto:

$$E_p(n!) = \left[\frac{n}{p}\right] + E_p\left(\left[\frac{n}{p}\right]!\right)$$

Pela hipótese de indução, temos que:

$$E_p\left(\left[\frac{n}{p}\right]!\right) = \left[\frac{\left[\frac{n}{p}\right]}{p}\right] + \left[\frac{\left[\frac{n}{p}\right]}{p^2}\right] + \cdots + \left[\frac{\left[\frac{n}{p}\right]}{p^k}\right]$$

Usando a proposição anterior, obtemos, por fim, que:

$$E_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots + \left[\frac{n}{p^k}\right]$$

□

Para ilustrar a aplicação do teorema, mostramos o seguinte exemplo:

Exemplo 3. $E_2(10!) = 5 + 2 + 1 = 8$, $E_3(10!) = 3 + 1 = 4$, $E_5(10!) = 2$, $E_7(10!) = 1$. Como 2, 3, 5, 7 são os primos menores que 10, segue que $10! = 2^8 3^4 5^2 7$. Em particular, 10! termina com 2 zeros.

Vamos usar o seguinte lema para demonstrar um corolário do Teorema de Legendre:

Lema 5.1. *Sejam $a_1, \cdots, a_m, b \in \mathbb{N}$, sendo $b \neq 0$. Temos então que*

$$\left[\frac{a_1 + \cdots + a_n}{b}\right] \geq \left[\frac{a_1}{b}\right] + \cdots + \left[\frac{a_m}{b}\right]$$

Demonstração. Sejam a_i o quociente e q_i o resto da divisão de a_i por b. Somando todos os a_i's temos que

$$a_1 + ... + a_m = (q_1 + \cdots + q_m)b + r_1 + \cdots + r_m$$

Dividindo $a_1 + \cdots + a_m$ por b, o quociente é maior ou igual a $(q_1 + ... + q_m)$, pois $r_1 + \cdots + r_m \geq 0$ e poderia aparecer mais fatores de b na soma. □

Corolário. Sejam $a_1, ..., a_m \in \mathbb{N}$. Então

$$\frac{(a_1 + \cdots + a_m)!}{a_1! \cdots a_m!} \in \mathbb{N}$$

Demonstração. Sabemos do lema anterior que, $\forall p$ primo e $i \in \mathbb{N}$:

$$\left[\frac{a_1 + \cdots + a_n}{p^i}\right] \geq \left[\frac{a_1}{p^i}\right] + \cdots + \left[\frac{a_m}{p^i}\right]$$

Ou seja, temos que $E_p((a_1 + \cdots + a_m)!) \geq E_p(a_1!) + \cdots + E_p(a_m!)$. Isso nos diz que $(a_1 + \cdots + a_m)!$ possui mais fatores de cada primo que $a_1! \cdots a_m!$. Daí, segue o resultado. □

Outro teorema que obtemos é o seguinte:

Teorema 5.2. *Sejam $p, n \in \mathbb{N}^*$, onde p é primo. Se escrevermos n na base p da seguinte maneira:*

$$n = n_r p^r + \cdots + n_1 p + n_0$$

Então

$$E_p(n!) = \frac{n - (n_0) + \cdots + n_r}{p-1}$$

Demonstração. Como $0 \leq n_i < p$, temos

$$\begin{aligned}
\left[\frac{n}{p}\right] &= n_r p^r + \cdots + n_2 p + n_1 \\
\left[\frac{n}{p^2}\right] &= n_r p^{r-1} + \cdots + n_3 p + n_2 \\
&\vdots \\
\left[\frac{n}{p^r}\right] &= n_r
\end{aligned}$$

Assim, temos que

$$\begin{aligned}
E_p(n!) = \left[\frac{n}{p}\right] + \cdots + \left[\frac{n}{p^r}\right] &= n_r \frac{p^r - 1}{p-1} + n_{r-1}\frac{p^r - 2}{p-1} + \cdots + n_1 \\
&= \frac{n_r p^r + \cdots + n_1 p + n_0 - (n_r + n_{r-1} + \cdots + n_0)}{p-1}
\end{aligned}$$

□

Referências

[1] Carlos Gustavo Tamm de Araujo Moreira et al. *Teoria dos Números: Um Passeio com Primos e Outros Números Familiares Pelo Mundo Inteiro*. Projeto Euclides. Sociedade Brasileira de Matemática, 2015.

[2] Chris K. Caldwell. *Mersenne Primes: History, Theorems and Lists*. URL: `https://primes.utm.edu/mersenne/`.

[3] *Fermat number*. URL: `https://en.wikipedia.org/wiki/Fermat_number`.

[4] Abramo Hefez. *Elementos de Aritmética*. Textos Universitários. Sociedade Brasileira de Matemática, 2006.

[5] *Mersenne prime*. URL: `https://en.wikipedia.org/wiki/Mersenne_prime`.

[6] Oystein Ore. *Number Theory and Its History*. Dover Publications, 1988.