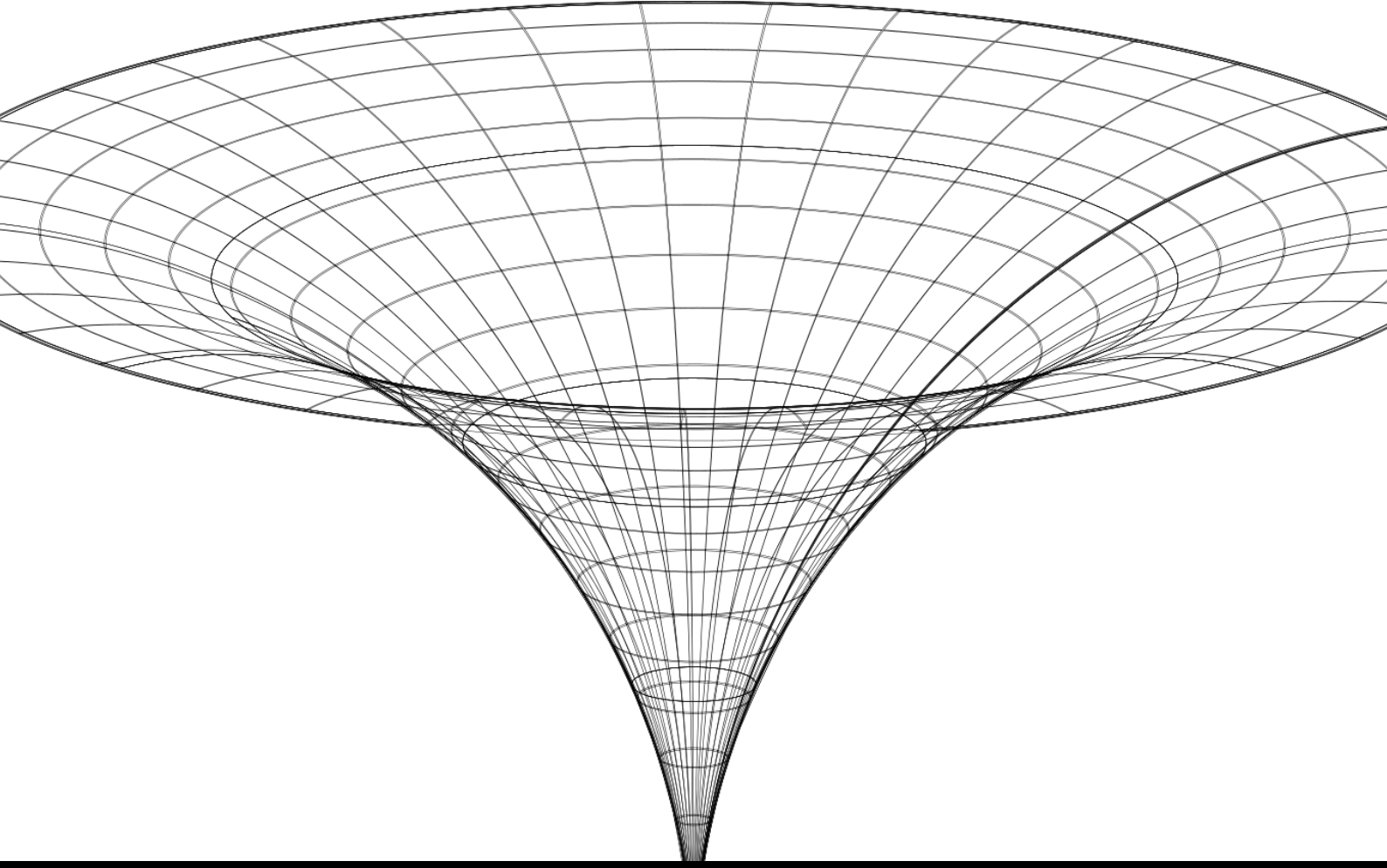
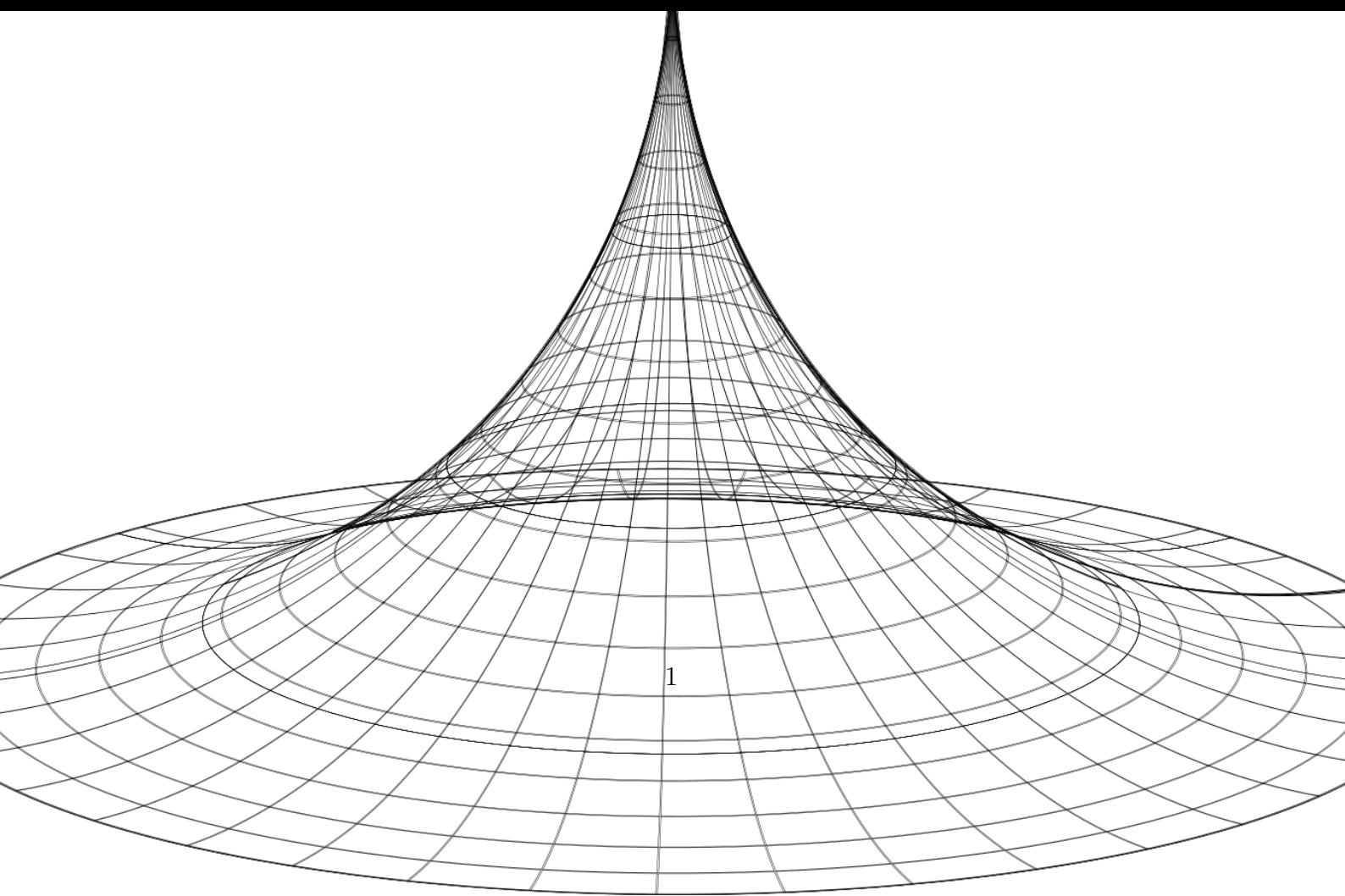


Uma introdução aos números primos e aos irracionais



Sumário

Agradecimentos

Eu gostaria de agradecer a Deus, ao Prof. Dr. Raimundo Bastos pela orientação e enorme ajuda durante a elaboração deste texto, ao PETMAT e ao FNDE/MEC pelo auxílio financeiro.

Introdução

Temos como objetivo introduzir um aluno do segundo ano de graduação no estudo dos números reais numa perspectiva complementar aos cursos visto até então. Tal estudo leva em conta os conhecimentos adquiridos em Teoria dos Números, Cálculo 1 e 2. O estudo levará em conta duas classes extremas dos números reais, a saber: os números Primos e os números Irracionais.

Os números primos foram estudados inicialmente por *Euclides*. Ao mesmo é atribuído a primeira demonstração da infinitude desses números. Cabe ressaltar que, até hoje, tal classe fornece um tema relevante de pesquisa matemática. A distribuição dos números primos é algo muito interessante e despertou o interesse de muitos matemáticos, inclusive do famoso matemático K. F. Gauss.

Os números irracionais também formam um subconjunto infinito dos números reais. Tal classe tem um comportamento bastante peculiar. Nos ocuparemos de apresentar um estudo baseado em Sequências/Séries de números reais, polinômios e Cálculo para determinar a irracionalidade de números famosos, por exemplo: número π e o número e, tal estudo foi possível pelo trabalho ímpar de *Ivan Niven*.

1 Preliminares

Neste primeiro capítulo nos ocuparemos de quatro assuntos não diretamente relacionados, mas que serão usados ao longo do texto. Caso o leitor seja familiarizado com os assuntos pode seguir para o capítulo [2]

1.1 Identidades trigonométricas importantes

As identidades trigonométricas apresentadas a seguir, serão muito importantes no desenvolvimento dos argumentos utilizados no capítulo [4.1] para mostrar a irracionalidade do seno e cosseno de determinados arcos.

$$cos(A+B) = cos(A)cos(B) - sen(A)sen(B) \tag{1}$$

$$sen(A+B) = sen(A)sen(B) - cos(A)cos(B) \tag{2}$$

Caso consideremos $A = B = \theta$, ganharemos o seguinte

$$cos(2\theta) = cos^2(\theta) - sen^2(\theta) \tag{3}$$

$$sen(2\theta) = 2sen(\theta)cos(\theta) \tag{4}$$

agora, sendo $A = 2\theta$ e $B = \theta$ e substituindo na identidade (1) obtemos

$$cos(3\theta) = cos(2\theta)cos(\theta) - sen(2\theta)sen(\theta) \tag{5}$$

Agora usando (3) e (4) e a identidade trigonométrica fundamental obtemos

$$\begin{aligned} cos(3\theta) &= (cos^2(\theta) - sen^2(\theta))cos(\theta) - (2cos(\theta)cos(\theta))sen(\theta) \\ &= cos^3(\theta) - 3sen^2(\theta)cos(\theta) \\ &= cos^3 - 3(1 - cos^2(\theta))cos(\theta) \end{aligned}$$

,ou seja,

$$cos(3\theta) = 4cos^3(\theta) - 3cos(\theta) \tag{6}$$

1.2 Critério das raízes racionais

Teorema 1. *Considere o polinômio* $p(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_0$ *com coeficientes inteiros e que esse polinômio admite como raíz um número racional da forma* $\frac{p}{q}$ *sendo mdc(p,q)* $= 1$ *e* p *e* $q \in \mathbb{Z}$*. Então* $p|a_0$ *e* $q|a_n$

Critério das raízes racionais. Seja $p(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_0$ e seus coeficientes inteiros. Suponha que $p(\frac{p}{q}) = 0$ tal que mdc$(p,q) = 1$ e inteiros. Sendo assim:

$$p(\tfrac{p}{q}) = a_n \tfrac{p^n}{q^n} + a_{n-1}\tfrac{p^{n-1}}{q^{n-1}} + ... + a_0 = 0 \text{ (I)}$$
$$p(\tfrac{p}{q}) = a_n \tfrac{p^n}{q^n} + a_{n-1}\tfrac{p^{n-1}}{q^{n-1}} + ... + a_1\tfrac{p}{q} = -a_0$$

Multiplicando ambos os lados por q^n e colocando p em evidência temos:

$$p(a_n p^{n-1} + a_{n-1}q \cdot p^{n-2} + ... + a_1 q^{n-1}) = -a_0 q^n$$

É evidente que $p| - a_0 q^n$ e como mdc$(p,q) = 1$, então $p|a_0$. Isolando o a_n da equação (I) e multiplicando ambos o lados por q^n e colocando-o em evidência obteremos o seguinte:

$$q(a_{n-1} \cdot p^{n-1} + \ldots + q^{n-1} \cdot a_0) = -a_n \cdot p^n$$

De maneira análoga, podemos concluir que $q|a_n$, assim como queríamos. □

1.3 Teorema fundamental da Aritmética

Teorema 2. *Todo inteiro maior do que 1 pode ser representado de maneira única (a menos da ordem) como um produto de fatores primos.*

Demonstração. Se n é primo não há nada a ser demonstrado. Suponhamos, pois, n composto. Seja $p_1 (p_1 > 1)$ o menor dos divisores positivos de n. Afirmamos que p_1 é primo. Isto é verdade, pois, caso contrário existitiria p, $1 < p < p_1$ com $p|n$, contradizendo a escolha de p_1. Logo, $n = p_1 n_1$.

Se n_1 for primo a prova está completa. Caso contrário, tomamos p_2 como o menor fator de n_1. Pelo argumento anterior, p_2 é primo e temos que $n = p_1 p_2 n_2$.

Repetindo este procedimento, obtemos uma sequência decrescente de inteiros positivos $n_1, n_2, n_3, ..., n_r$. Como todos eles são inteiros maiores do que 1, este procedimento deve terminar. Como os primos na sequência $p_1, p_2, p_3, ..., p_k$ não são, necessariamente, distintos, n terá, em geral, a forma:

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

Para mostrarmos a unicidade usamos indução em n. Para $n = 2$ a afirmação é verdadeira. Assumimos, então, que ela se verifica para os inteiros maiores do que 1 e menores do que n. Vamos provar que ela também é verdadeira para n. Se n é primo, não há nada a provar. Vamos supor,então, que n seja composto e que tenha duas fatorações, isto é,

$$n = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_r$$

Vamos provar que $s = r$ e que cada p_i é igual a algum q_j. Sem perda de generalidade podemos supor que $p_1 = q_1$. Logo $n/p_1 = p_2 \cdots p_s = q_2 \cdots q_r$. Como $1 < n/p_1 < n$, a hipótese de indução nos diz que as duas fatorações são idênticas, isto é, $s = r$ e, a menos da ordem, as fatorações $p_1 p_2 \cdots p_s$ e $q_1 q_2 \cdots q_r$ são iguais. □

1.4 A função ϕ é multiplicativa

Teorema 3. *Para $p \in \mathbb{P}$ e a um inteiro positivo temos*

$$\phi(p^a) = p^a - p^{a-1}$$

Demonstração. Pela definição de $\phi(n)$ sabemos que $\phi(p^a)$ é um número de inteiro positivos não superiores a p^a e relativamente primos com p^a.Mas os únicos números não primos com p^a com menores do que ou iguais a p^a são aqueles divisíveis por p. Como os múltiplos de p não superiores a p^a são, em números,p^{a-1}, o resultado segue. □

Observação 1. *Se $a = 1$, então $\phi(p) = p^1 - p^{1-1} = p - 1$.*

Teorema 4. *A função ϕ de Euler é multiplicativa, isto é, $\phi(mn) = \phi(m) \cdot \phi(n)$ para $(m, n) = 1$.*

Demonstração. Vamos dispor os números de 1 até mn da seguinte forma:

$$\begin{array}{cccc}
1 & m+1 & 2m+1 \ldots & (n-1)m+1 \\
2 & m+2 & 2m+2 \ldots & (n-1)m+2 \\
3 & m+3 & 2+3 \ldots & (n-1)m+3 \\
\vdots & & \vdots & \\
m & 2m & 3m \ldots & nm
\end{array}$$

Se na linha r, onde estão os termos $r, m+r, 2m+r, \ldots, (n-1)m+r$, tivermos $(m,r) = d > 1$, então nenhum termo nesta linha será primo com mn, uma vez que estes termos, sendo da forma $km + r, 0 \leq k \leq n-1$, eão todos divisíveis por d que é o máximo divisor comum de m e r. Logo, para encontrarmos os inteiros desta tabela qe são primos com mn, devemos olhar na lina r somente se $(m,r) = 1$. Portanto temos $\phi(m)$ linhas onde todos os elementos são primos com m.

Devemos, pois, procurar em cada uma dessas $\phi(m)$ linhas, quantos elementos são primos com n, uma vez que todos são primos com m. Como $(m,n) = 1$ os elementos $r, m+r, 2m+r, \ldots, (n-1)m+r$ formam um sistema completo de resíduos módulo n. Logo, cada uma destas linhas possuir $\phi(n)$ elementos primos com n e, portanto, como eles são primos com m, eles são primos com mn. Isto nos garante que $\phi(mn) = \phi(m) \cdot \phi(n)$. □

2 Números Primos

2.1 Infinitude dos primos

A infinitude dos primos foi mostrada por Euclides em seu livro *Elementos* [Livro IX,proposição 20, página 342](5). Nesta seção mostraremos três demonstrações. A primeira delas é a mais clássica, as duas últimas envolvem conceitos de Teoria dos Números. Mais precisamente, utilizando duas funções bem conhecidas nesse campo, a saber a função ϕ de Euler; e a função que gera os números de Fermat.

2.2 Demonstração de Euclides

Essa é a primeira demonstração que é creditada a Euclides (cf. (5, Livro IX,proposição 20, página 342)).

Teorema 5. *O conjunto dos números primos é infinito.*

Demonstração. (Demonstração por absurdo) Suponha que todos os primos estejam contidos no seguinte conjunto $\mathbb{P} = \{p_1, p_2, p_3, ..., p_k\}$. Como sabemos pelo *Teorema Fundamental da Aritmética* todo número natural, maior que 1, pode ser decomposto em um produto de fatores primos, ou seja, todo natural tem que ser divisível por ao menos um dos primos do conjunto acima, assumindo a hipótese de que são finitos.

Suponha que os primos são finitos e considere o seguinte número N.

$$N = (p_1 \cdot p_2 \cdot \ldots \cdot p_k) + 1$$

Esse número não pode ser divido por p_1, pois, de acordo com o algoritmo de Euclides, $N = p_1 \cdot q + r$, sendo que

$$q = p_2 \cdot p_3 \cdot \ldots \cdot p_k \text{ e } r = 1.$$

De modo análoga, nenhum dos p_i's divide N.

Dessa forma temos um número $N > 1$ que não pode ser dividido por nenhum dos primos. Absurdo. Dada a hipótese inicial de que os primos são finitos, ou seja, pode-se concluir que existem infinitos primos. □

2.3 Demonstrações envolvendo Teoria dos Números

2.3.1 Função ϕ de Euler

A função $\phi(n)$ conta a quantidade de números que são primos entre si com n de 1 até n. Mais precisamente,

$$\begin{array}{rccl} \phi & : & \mathbb{N} & \longrightarrow & \mathbb{N} \\ & & n & \longmapsto & |\{m \mid 1 \leqslant m \leqslant n \text{ e } mdc(m,n) = 1\}| \end{array}$$

Observação 2. *Em particular,*

$\phi(1) = 1.$ $\phi(3) = 2.$ $\phi(5) = 4.$

$\phi(2) = 1.$ $\phi(4) = 2.$ $\phi(6) = 2.$

Para a demonstração que apresentaremos faremos uso das seguintes propriedades:

Proposição 1.

(I) Sejam $a, b \in \mathbb{N}$. Se $mdc(a,b) = 1$, então $\phi(a) \cdot \phi(b) = \phi(a \cdot b)$.

(II) Se p é um número primo, então $\phi(p) = p - 1$.

Observação 3. *A demonstração dessas propriedades se encontra em 1.4 e (4).*

Agora podemos apresentar a segunda demonstração da infinitude dos números primos:

Demonstração. Suponha por absurdo que $\mathbb{P} = \{p_1, p_2, \ldots, p_n\}$ é o conjunto com todos os primos e que $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n$. Como N possui todos os fatores primos em sua composição, então $\phi(N) = 1$. Assim:

$$\phi(N) = \phi(p_1 \cdot p_2 \cdot \ldots \cdot p_n)$$

Pela propriedade (I) temos:

$$\phi(p_1 \cdot p_2 \cdot \ldots \cdot p_n) = \phi(p_1) \cdot \phi(p_2) \cdot \ldots \cdot \phi(p_n)$$

pela propriedade (II) temos:

$$\phi(p_1) \cdot \phi(p_2) \cdots \phi(p_n) = (p_1 - 1) \cdot (p_2 - 1) \cdot \ldots \cdot (p_n - 1)$$

assim:

$$(p_1 - 1) \cdot (p_2 - 1) \cdot \ldots \cdot (p_n - 1) = 1$$

Porém, é evidente que

$(p_1 - 1) \cdot (p_2 - 1) \cdots (p_n - 1) > 1$, ou seja, $(p_1 - 1) \cdot (p_2 - 1) \cdots (p_n - 1) = 1$

O que é um absurdo. Portanto podemos concluir que os primos são infinitos. □

2.3.2 Chirstian Goldbach

O matemático prussiano *Christian Goldbach* mostrou que os números de Fermat [9.1], que são da forma $F_n = 2^{2^n} + 1$ podem nos apresentar uma terceira demonstração da infinitude dos primos.

Lema 1. *Quaisquer dois números de Fermat distintos F_n e F_m são relativamente primos.*

Demonstração. Para provar este resultado vamos mostrar, primeiramente, que a seguinte relação se verifica

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

A demonstração de que essa propriedade é válida é feita por indução. O caso n = 1 se verifica, ou seja, $F_0 = F_1 - 2$, vamos supor a validade para n e mostrar que a mesma relação também vale para n + 1.

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

Supondo $n < m$ temos, pela relação acima, que

$$F_0 F_1 F_2 \cdots F_n \cdots F_{m-1} = F_m - 2.$$

o que implica que $F_m - F_0F_1F_2 \cdots F_n \cdots F_{m-1} = 2$. Logo, se um número d divide F_n e F_m então d divide 2. Como F_n é ímpar d não pode ser 2, portanto $(F_n, F_m) = 1$. □

Agora podemos apresentar a prova da infinitude dos números primos a partir do lema anterior:

Corolário 1. *O conjunto dos números primos é infinito.*

Como pudemos ver anteriormente os números de *Fermat* são primos entre si dois a dois, ou seja, pelo Teorema Fundamental da Aritmética é possível observar que na fataroção desses números há pelo menos um fator primo que não há no outro. Em outras palavras:

F_1 possui um fator primo que F_0 não possui, F_2 possui um fator primo que F_1 e F_0 não possuem e assim por diante. A partir disso podemos dizer que há infinitos números primos.

Exercícios - Lista 1

Exercício 1. *Demonstre que um número ímpar e a metade do seu sucessor são sempre primos entre si.*

Exercício 2. *Para cada $n \in \mathbb{N}$ considere p_n como sendo o n-ésimo primo. E seja:*

$$X = \left(\prod_{i=1}^{n} p_n\right) + 1 \tag{7}$$

Encontre um p_n tal que X não seja primo.

Exercício 3. *Suponha que a e b são números naturais primos entre si. Mostre que, para qualquer natural m, $a \cdot b | m$ se a e b dividem m.*

Exercício 4. *Demonstre que existem infinitos números primos da forma $4m + 3$ e da forma $6m + 5$, onde $m \in \mathbb{Z}$.*

Exercício 5. *Apresente uma formalização da construção de infinitos primos utilizando a ideia do Lema 1, ou seja, tome uma sequência do tipo:*

$$N_i = p_i + k \tag{8}$$

onde $i \in \{1, 2, 3, \ldots, n\}$ e $p_1, p_2, \ldots, p_n$ são primos e k é uma constante positiva. Agora, prove que dado o fato que o MDC entre dois números quaisquer dessa sequência é 1, então existem infinitos números primos.

3 Comentários do Capítulo

O estudo dos primos permanece uma fonte de questões interessantes na matemática. No apêndice [] falarei algumas curiosidades, além de incluir as definições de primos de *Mersenne* e *Fermat.*

Caso tenha interesse em continuar seus estudos veja:

1. *Números primos, amigos que causam problemas* - Paulo Ribenboim, Editora SBM;

2. Em (4) no capítulo [XX] *Plínio* demonstra o famoso postulado de *Bertrand*;

3. No seguinte site ⟨https://mathworld.wolfram.com/PrimeNumberTheorem.html⟩ você pode encontrar informações muito interessantes sobre *O Teorema dos Nùmeros Primos*, onde se é estudado a famosa função $\pi(n)$ que conta a quantidade de primos até n.

4 Números Irracionais - parte 1

O estudo dos números reais desempenha um papel central na matemática moderna. Aqui nos ocuparemos no estudo dos números irracionais que surgem naturalmente no contexto das identidades trigonométricas e logarítmicas (e o Teorema Fundamental da Aritmética). Essa seção foi baseada no livro do Ivan Niven (1), mais precisamente, o capítulo 5.

4.1 Valores irracionais das funções trigonométricas

As funções trigonométricas $sen(\theta)$ e $cos(\theta)$ associam para cada ângulo θ um valor de x real, que nos seguintes casos serão irracionais. Iremos apresentar alguns métodos e certas identidades trigonométricas que serão utilizados para mostrar que "muitos"valores associados aos ângulos θ são irracionais.

Exemplo 1. *O número* $cos(20°)$ *é irracional.*

Demonstração. Considerando $\theta = 20°$ na equação (6) obtemos

$$cos(60°) = 4cos^3(20°) - 3cos(20°)$$

Substituindo o $cos(20°) = x$ e o fato de que $cos(60°) = \frac{1}{2}$ obtemos

$$4x^3 - 3x = \frac{1}{2}$$

ou seja

$$8x^3 - 6x - 1 = 0 \tag{9}$$

Ou seja, a partir de uma expressão trigonométrica, criamos um polinômio $p(x) = 8x^3 - 6x - 1$ que tem como raiz o número $cos(20)$. Agora, utilizaremos o critério das raízes racionais [1.2] para mostrar que $cos(20)$ é irracional. De fato, por ele temos que: se α é uma raiz racional de $p(x)$, então $\alpha \in \{\pm 1, \pm\frac{1}{2}, \pm\frac{1}{4}$ e $\pm\frac{1}{8}\}$. Porém, nenhum desses 8 candidatos é raiz do polinômio obtido. Logo $cos(20°)$ é um número irracional. □

Proposição 2. *O número* $cos(40°)$ *é irracional.*

Demonstração. Utilizando a equação (6) e assumindo $\theta = 40°$ temos:

$$cos(3 \cdot 40°) = 4cos^3(40°) - 3cos(\theta)$$

Sabemos que $cos(120°) = -\frac{1}{2}$ e substituindo $cos(40°) = x$ temos:

$$\begin{gathered} -\tfrac{1}{2} = 4x^3 - 3x \ (\cdot 2) \\ -1 = 8x^3 - 6x \\ 8x^3 - 6x + 1 = 0 \end{gathered}$$

Pelo critério das raízes racionais, temos que os candidatos a raízes racionais são os divisores p, q inteiros tal que $q|8$ e $p|1$, ou seja, $\pm 1, \pm 2, \pm 4, \pm 8$. Como nenhum desses valores é raiz, podemos concluir que não existem raízes racionais para esse polinômio, portanto $cos(40°)$ é irracional. □

Observação 4. *Se θ for um ângulo tal que $cos(2\theta)$ é irracional, então $cos(\theta)$, $sen(\theta)$ e $tan(\theta)$ também serão irracionais.*

Para demonstrar esse princípio, usaremos, inicialmente a seguinte equação : $cos(2\theta) = 2cos^2(\theta) - 1$, $cos(2\theta) = 1 - 2sen^2(\theta)$.Suponha que $cos(\theta)$ é racional. Então, $cos^2(\theta)$ e $2cos^2(\theta) - 1$ também seriam racionais. Mas, $2cos^2(\theta) - 1 = cos(2\theta)$, que é irracional.

Analogamente suponhamos $sen(\theta)$ racional. Então, $sen^2(\theta)$ seria racional, bem como $1 - 2sen^2(\theta)$. Mas, $1 - 2sen^2(\theta) = cos(2\theta)$. Por fim, suponha que $tan(\theta)$ é racional. Então , $tan^2(\theta)$ seria racional e poderíamos usar a seguinte identidade trigonométrica:

$$1 + tan^2(\theta) = sec^2(\theta) = \frac{1}{cos^2(\theta)}$$

para ver que $cos^2(\theta)$ seria racional. Mas, novamente, das equações iniciais concluiríamos que $cos(2\theta)$ é racional, obtendo, assim, uma contradição. Portanto, $tan(\theta)$ tem que ser irracional. Portanto, aplicando o princípio que acabou de ser demonstrado, podemos proofr que uma infinidade de números trigonométricos são irracionais.

Exercícios - Lista 2

Para fixação suguem os seguintes exercícios:

Exercício 6. *Prove que os seguintes números são irracionais:*

(a) $cos(20°)$

(b) $sen(20°)$

(c) $cos(10°)$

(d) $sen(50°)$.

Exercício 7.

(a) Demonstre a identidade $cos(5\theta) = 16cos^5(\theta) - 20cos^3(\theta) + 5cos(\theta)$

(b) Prove que $cos(12°)$ *é irracional.*

Exercício 8. *Seja um produto de primos distintos $p_1 \cdots p_n$ e $r > 1 \in \mathbb{Z}$ tal que $x = \sqrt[r]{p_1 \cdots p_n}$. Prove que x é irracional.*

4.2 Valores irracionais dos logaritmos decimais

Todos os logaritmos utilizados nesse texto serão na base 10. Relembrando a definição de logaritmo. Dado um número $x \in \mathbb{R}_+^*$, seu logaritmo na base 10 é um número k, tal que $10^k = x$. Assim, para qualquer $x > 0$:

$$log(x) = k$$

e

$$10^k = x$$

são afirmações equivalentes. Todas as demonstrações das irracionalidades serão baseadas o Teorema Fundamental da Aritmética [1.3] e induzir a uma contradição.

Teorema 6. *Todo inteiro maior do que 1 pode ser representado de maneira única (a menos da ordem) como um produto de fatores primos.*

Observação 5. *A demonstração do teorema 6 se encontra em 1.3.*

Exemplo 2. *O número $log(2)$ é irracional.*

Demonstração. Suponha que $log(2)$ é racional, ou seja, $log(2) = \frac{a}{b}$, com a e b inteiros positivos. Utilizando a definição de logaritmo temos que:

$$2 = 10^{\frac{a}{b}}$$

elevando ambos os membros à potência b, temos

$$2^b = 10^a = 2^a 5^a$$

Observando a igualdade e aplicando o Teorema Fundamental da Aritmética. Podemos ver que de fato pelo Teorema Fundamental da Aritmética essa igualdade não pode ser verdadeira, pois para qualquer valor de b, 2^b é um inteiro não divisível por 5, enquanto $2^a 5^a$ é divisível por 5. Portanto, $log(2)$ é irracional. □

Exemplo 3. *Sejam c e d inteiros não negativos distintos. O número $log(2^c 5^d)$ é irracional.*

Demonstração. Pelas condições iniciais, sabemos que $2^c 5^d > 1$, de modo que $log(2^c 5^d) > 0$. Suponha que $log(2^c 5^d)$ é racional.

$$log(2^c 5^d) = \frac{a}{b}$$

com a e b inteiros positivos, temos

$$2^c 5^d = 10^{\frac{a}{b}}$$

elevando ambos os membros à potência b, temos

$$2^{bc} 5^{bd} = 10^a = 2^a 5^a$$

Assim, pelo Teorema Fundamental da Aritmética, essa igualdade se verifica somente se $bc = a$ e $bd = a$, ou seja, $bc = bd$, mas como pelas condições iniciais $d \neq c$, então bc e bd são distintos. Portanto, $log(2^c 5^d)$ é irracional. □

Exercícios - Lista 3

Exercício 9. *Demonstre que* $log(\frac{3}{2})$ *é irracional.*

Exercício 10. *Demonstre que* $log(15)$ *é irracional.*

Exercício 11. *Faça um exercício que contemple* $log_7(10) \notin \mathbb{Q}$.

Exercício 12. *Sejam* p, q *primos distintos. Mostre que* $log_p(q) \notin \mathbb{Q}$.

4.3 Critério das Raízes Racionais

Existe um argumento bastante útil no estudo de raízes racionais de um dado polinômio com coeficientes inteiros. O conceito de polinômio é bastante versátil no estudo da matemática. Aqui nos ocuparemos na tentantiva de investigar as possibilidade de raízes racionais de um polinômio com coeficientes inteiros, olhando apenas dois de seus coeficientes mais precisamente.

Teorema 7. *Considere o polinômio* $p(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_0$ *com coeficientes inteiros e que esse polinômio admite como raíz um número racional da forma* $\frac{p}{q}$ *sendo mdc(p,q)* $= 1$ *e* p *e* $q \in \mathbb{Z}$. *Então* $p|a_0$ *e* $q|a_n$

Observação 6. *A demonstração do teorema 7 se encontra em 1.2.*

Corolário 2. *Seja* $p(x) = a_0 + a_1 x + \ldots + a_n x^n$. *Se* $\alpha = \frac{m}{n} \in \mathbb{Q}$, *tal que* $(m, n) = 1$, *é raiz de p, então* $\alpha \in \mathbb{Z}$

Observação 7. *Tal resultado não pode ser aplicado para o estudo de raízes irracionais. Por exemplo:*

$$p(x) = x^2 - 2 \in \mathbb{Q}[x]$$

e $\sqrt{2}$ *é raiz.*

Exemplo 4. *O polinômio* $p(x) = 8x^3 - 6x - 1$ *não possui raízes racionais.*

Exemplo 5. $p(x) = x^2 - 2$ *não possui raízes racionais.*

Exemplo 6. *Se* $\alpha \in \mathbb{R}$ *é raiz de um polinômio* $p(x) = a_0 + a_1 x + \ldots + a_n x^n$, *tal que,* $p(x) \in \mathbb{Z}[x]$ *e* $r, s \in \mathbb{Z}$ *onde*

$$\alpha \notin \{\tfrac{r}{s} : r|a_0 \text{ e } s|a_n\}$$

então $\alpha \notin \mathbb{Q}$

Observação 8. *Os exemplos citados acima ficam como exercício ao leitor.*

De modo mais geral, o critério das raízes racionais nos dá um critério de irracionalidade, pois após testar os candidatos, obtidos através do critério das raízes racionais, e nenhum deles ser raiz, então o polinômio não possui raízes racionais, ou seja, suas raízes são pelo menos irracionais.

5 Considerações do capítulo

Os números irracionais são comumente divididos em duas subfamílias: *Algébricos* e *Transcendentes*.

Definição 1. *Dizemos que $\alpha \in \mathbb{R}$ é Algébrico se existe $p(x) \in \mathbb{Z}[x]$, tal que α é raiz de $p(x)$, ou seja, $p(\alpha) = 0$.*

Portanto vale à pena ser mencionado que os números π e e não são *Algébricos*((14); Capítulo 7; proposição 7.1). As demonstrações desses fatos fogem dos nossos objetivos imediatos. Para mais detalhes veja os capítulos 6 e 7 de (3).

6 Números Irracionais - parte 2

6.1 A irracionalidade de e

O estudo dos números reais desempenha um papel central na matemática moderna. Aqui nos ocuperemos nas demonstrações da irracionalidade dos números: e, e^r tal que $r \in \mathbb{Q}^*$ e π^2. A seguinte demonstração foi feita por *Fourier* em 1815. Nela iremos mostrar de uma maneira bastante intuitiva, utilizando o teorema fundamental da aritmética, a irracionalidade de e.

Teorema 8. *e é irracional.*

Demonstração. Sendo $e = \sum_{k\geq 0} \frac{1}{k!}$, suponha que e é racional tal que $e = \frac{a}{b}$ para inteiros a e $b > 0$.Dessa forma:

$$n!be = n!a \ \forall n \geq 0$$

Contudo observe que essa igualdade não é válida, conforme iremos demonstrar a seguir.Do lado direito temos um inteiro, porém do lado esquerdo com

$$e = \left(1 + \tfrac{1}{2!} + \tfrac{1}{3!} + ... + \tfrac{1}{n!}\right) + \left(\tfrac{1}{(n+1)!} + \tfrac{1}{(n+2)!} + \tfrac{1}{(n+3)!} + ...\right)$$

Se decompõe em uma parte inteira

$$bn!\left(1 + \tfrac{1}{2!} + \tfrac{1}{3!} + ... + \tfrac{1}{n!}\right)$$

E uma segunda parte

$$b\left(\tfrac{1}{(n+1)} + \tfrac{1}{(n+1)(n+2)} + \tfrac{1}{(n+1)(n+2)(n+3)} + ...\right)$$

que é aproximadamente $\frac{b}{n}$, de modo que para n suficientemente grande ela não pode ser inteira: ela é maior quando $\frac{b}{n+1}$ é menor do que $\frac{b}{n}$, como podemos ver a partir de uma comparação com a série geométrica:

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

Observação 9. *É fácil ver que essa desigualdade vale, pois:*

$(q+1)(q+2) > (q+1)^2 \implies (q+1)((q+1)+1) > (q+1)(q+1)$*, então:*

$$\frac{1}{(q+1)(q+2)} < \frac{1}{(q+1)^2}$$

Ou seja de um lado da igualdade temos um número inteiro e do outro temos um número que não é inteiro. O que é um absurdo! Logo podemos concluir que e não é racional. □

6.2 A irracionalidade de e^r

A seguinte demonstração que usaremos foi proposta pelo matemático americano *Ivan Niven*, em artigo publicado no *Bulletin of the American Mathematical Society*, 53 (1947), página 509, o qual usou um método desenvolvido por *Hermite* para proofr a transcendência do número e.

Lema. Para algum $n \geq 1$ fixado, seja:

$$f(x) = \frac{x^n(1-x)^n}{n!}$$

- (i) Para $0 < x < 1$, temos $0 < f(x) < \frac{1}{n!}$;
- (ii) As derivadas $f^{(k)}(0)$ e $f^{(k)}(1)$ são números inteiros para todo $k \geq 0$.

Teorema 9. *e^r é irracional para todo $r \in \mathbb{Q} \setminus 0$.*

Demonstração. Basta mostrar que e^r não pode ser racional para um inteiro positivo r (se $e^{\frac{r}{t}}$ fosse racional, então $e^{\frac{r}{t}t}$ seria racional também). Suponha que $e^r = \frac{a}{b}$ para inteiros $a, b > 0$. Faça:

$$F(x) = s^{2n}f(x) - s^{2n-1}f'(x) + ... + f^{(2n)}(x),$$

em que $f(x)$ é a função do lema.

$F(x)$ pode ser também escrita como uma soma infinita

$$F(x) = s^{2n}f(x) - s^{2n-1}f'(x) + s^{2n-2}f''(x) \mp ...,$$

uma vez que as derivadas de ordem $f^{(k)}(x)$, para $k > 2n$, se anulam. A partir disso, vemos que o polinömio $F(x)$ satisfaz a identidade

$$F'(x) = -sF(x) + s^{2n+1}f(x).$$

Assim, derivando, vem

$$\frac{d}{dx}[e^{srx}F(x)] = re^{rx}F(x) + e^{rx}F'(x) = r^{2n+1}e^{rx}f(x)$$

a partir disso

$$N = b\int_0^1 r^{2n+1}e^{rx}f(x)dx = aF(1) - bF(0)$$

Esse número é um inteiro, pois a partir do lema (ii) $F(0)$ e $F(1)$ são inteiros. Contudo a partir da parte (i) do lema podemos fazer uma estimativa superior e inferior quanto ao tamanho de N,

$$0 < N = b\int_0^1 r^{2n+1}e^{rx}f(x)dx < br^{2n+1}e^r\frac{1}{n!} = \frac{ar^{2n+1}}{n!} < 1$$

O que mostra que N não pode ser inteiro: uma contradição. □

6.3 A irracionalidade de π

A seguinte demonstração foi realizada também por *Ivan Niven* e nela utilizaremos uma técnica muito semelhante a utilizada na demonstração 5.

Teorema 10. *π é irracional.*

Lema 2. *Para algum $n \geq 1$ fixado, seja:*

$$f(x) = \frac{x^n(1-x)^n}{n!} \tag{10}$$

- *(i) Para $0 < x < 1$, temos $0 < f(x) < \frac{1}{n!}$;*
- *(ii) As derivadas $f^{(k)}(0)$ e $f^{(k)}(1)$ são números inteiros para todo $k \geq 0$.*

Propriedade 1. *Se $x \in (0;\pi)$, então $0 < f(x)sen(x) < \dfrac{\pi^n a^n}{n!}$*

Demonstração. Pela hipótese $0 < x < \pi$ e portanto $x^n < \pi^n$. E como $b > 0$, então $0 < bx \implies a < a + bx \implies a - bx < a \implies (a - bx)^n < a^n$.
Daí, sabemos que $a - bx > 0$. Agora, levando em conta o intervalo $0 < x < \pi$, podemos dizer que $0 < sen(x) < 1$ $6\forall x \in (0;\pi)$, assim concluímos o que queríamos:

$$f(x)sen(x) = \frac{x^n(a-bx)^n sen(x)}{n!} < \frac{\pi^n a^n}{n!} \tag{11}$$

□

Corolário 3. *Como $x \in (0;\pi)$, então $0 < f(x)sen(x) < \dfrac{\pi^n a^n}{n!}$*

Demonstração. Suponha que $\pi = \frac{a}{b}$, onde $(a;b) = 1$. Sejam definidos os seguintes polinômios.

$$f(x) = \frac{x^n(a-bx)^n}{n!} \tag{12}$$

$$F(x) = f(x) - f^{(2)}(x) + f^{(4)} - \ldots + (-1)^n f^{(2n)}(x) \tag{13}$$

E as i-ésimas derivadas de $f(x)$ possuem valores inteiros para $x = 0$ e para $x = \pi = \dfrac{a}{b}$, pois $f(x) = f(\dfrac{a}{b} - x)$.

Observação 10. *Vamos mostrar a igualdade anterior.*

$$f(\frac{a}{b}-x)=\frac{(\frac{a}{b}-x)^n\cdot(a-b(\frac{a}{b}-x))^n}{n!}$$
$$f(\frac{a}{b}-x)=\frac{(\frac{a}{b}-x)^n\cdot(bx)^n}{n!}$$
$$f(\frac{a}{b}-x)=\frac{((\frac{a}{b}-x)\cdot bx)^n}{n!}$$
$$f(\frac{a}{b}-x)=\frac{(ax-bx^2)^n}{n!}$$
$$f(\frac{a}{b}-x)=\frac{(x(a-bx))^n}{n!}$$
$$f(\frac{a}{b}-x)=\frac{x^n(a-bx)^n}{n!}=f(x)$$

assim como queríamos mostrar.

Agora utilizando cálculo elementar temos:

$$\frac{d}{dx}(F'(x)sin(x)-F(x)\cos(x))=F''(x)\sin(x)+F(x)\sin(x)=f(x)s\sin(x)$$

$$\int_0^\pi f(x)\sin(x)dx=(F'(x)\sin(x)-F(x)\cos(x))|_0^\pi=F(\pi)+F(0) \quad (14)$$

Agora $F(\pi)+F(0)$ é um inteiro, pois $f^{(i)}(\pi)$ e $f^{(i)}(0)$ são inteiros para $0<x<\pi$. Do corolário 3:

$$0<f(x)<\frac{\pi^n a^n}{n!}$$

Agora integrando de 0 a π

$$0<\int_0^\pi f(x)\sin(x)<\int_0^\pi\frac{\pi^n a^n}{n!}$$
$$0<F(\pi)+F(0)<\frac{\pi^{n+1}a^n}{n!}$$

contudo para n suficientemente grande $\frac{\pi^{n+1}a^n}{n!}<1$, portanto:

$$0<F(\pi)+F(0)<1\ absurdo! \quad (15)$$

Pois $F(\pi)+F(0)\in\mathbb{Z}$, portanto $\pi\notin\mathbb{Q}$ □

Exercícios - Lista 4

Exercício 13. *Mostre que $2 \cdot e$ é irracional.*

Exercício 14. *Mostre que $k \cdot e$ é irracional para $k \in \mathbb{Z}$*

Exercício 15. *Prove que $\sqrt[3]{4+\sqrt{11}} \in \mathbb{I}$*

Exercício 16. *Sejam a e b naturais ímpares e $a^2 + b^2 = c^2$. Prove que c não é racional.*

Exercício 17. *Prove que tais números não são racionais:*

- $\sqrt{3} + \sqrt{5}$
- $\sqrt[3]{5} + \sqrt{2}$
- $\sqrt{3} - \frac{\sqrt{5}}{17}$

7 Curiosidades

7.1 Números Irracionais

7.1.1 Dia do π

O dia do π é comemorado na data 3/14, data no padrão americano, às 1:59 da tarde porque $\pi \approx 3,14159$. Na seguinte referência (13) você pode encontrar um pouco da história desse dia.

7.1.2 Ludolph Van Ceulen e o π

Ludolph Van Ceulen foi um matemático alemão que viveu no século XVI. Ele foi um dos matemáticos mais importantes quando se trata do assunto π. *Ludolph* recebia vários desafios matemáticos de *Simon van der Eycke*, outro matemático da época, que em 1584, propôs a demonstração de um problema muito famoso "A quadratura do círculo"(12). Cerca de um anos após a publicação de *Simon*, *Van Ceulen* mostrou que a demonstração estava incorreta e provavelmente foi a partir dai que *Van Ceulen* se aproximou dos trabalhos de *Arquimedes*, onde muito provavelmente ele conheceu o método da exaustão que foi muito usado em seus estudos sobre o π. A partir daí *Van Ceulen* dedicou boa parte sua vida na matemática a calcular π com a maior precisão de casas decimais. Em 1596, *Van Ceulen* publicou seu trabalho mais importante, onde apresentou π como 20 casas decimais usando um polígono com $15 \cdot 2^{31}$ lados e depois um com 2^{62} lados ele chegou a 35 casas decimais.

Em 1621 *Willebrord Snell*, aluno de *Van Ceulen*, publicou uma variação do método da exaustão de *Arquimedes*, levando à seguinte fórmula, chamada *fórmula de Van Ceulen*.

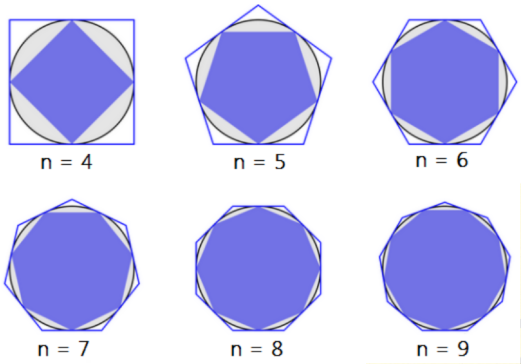
Observação 11. *Em homenagem ao matemático Ludolph Van Ceulen na Alemanha o número π também é conhecido como número de Ludolphine (11).*

$$\pi = n \cdot \sin \frac{180^\circ}{n}, \text{ onde } n \text{ é o número de lados do polígono}$$

Exemplo 7. *Pegue um polígono com 2^{62} lados, utlizando a fórmula anterior temos:*

$$2^{62} \cdot \sin \frac{180^\circ}{2^{62}} \approx 3.14159264\ldots$$
$$\textit{enquanto } \pi = 3.14159265\ldots$$

(a) Ludolf Van Ceulen



(b) Pi pelo método da exaustão

Observação 12. *A ideia por trás desta demonstração pode ser encontrada em (11).*

7.2 Números Primos

7.2.1 Primos de Mersenne

O matemático francês *Marin Mersenne* é o criador dos primos de *Mersenne*, sendo eles da forma:

- Primos de *Mersenne*: $M_p = 2^p - 1$ tal que $p \in \mathbb{P}$.

Muitos matemáticos acreditavam que para qualquer primo p seria verdadeiro, contudo, em 1536, *Hudalrichus Regius* apresentou uma fatoração de $2^{11} - 1 = 2047 = 23 \cdot 89$, proofndo que a conjectura estava errada.

Existe um grupo chamado *Great Internet Mersenne Prime Search ou Gimps* que busca os primos de *Mersenne*. No site deles, é disponilizado um software onde você empresta um pouco do desempenho da sua máquina para efetuar os cálculos para encontrar o próximo primo. Atualmente o maior número primo conhecido é um primo de *Mersenne*, ele é da forma: $2^{82.589.933} - 1$ e possui mais de 24 milhões de dígitos em sua representação decimal e foi descoberto pelo *GIMPS*(8). A procura de novos primos de *Mersenne* é estimulada pela *EEF (Eletronic Frontier Foundantion)*(9) que oferece 100 mil dólares(7) para o indivíduo ou grupo de indivíduos que primeiro descobrirem um número primo de *Mersenne* com mais de 100 milhões de dígitos.

A busca por novos números primos é muito importante para a criptografia, pois quanto maior for esse número maior será o tempo necessário para uma máquina realizar os testes para descobrir se esse número é primo ou composto. Ou seja, tudo gira em torno disso, caso o leitor tenha interesse em entender a relação do tempo de execução de um algoritmo e os testes para saber se um número é primo, recomendo que pesquise sobre um dos problemas do milênio chamado de: *P vs NP*. O leitor pode encontrar exemplos em (6).

7.2.2 Um erro de Fermat?

O matemático *Pierre de Fermat* conjecturou que todos os números Primos poderiam ser escritos da seguinte forma:

$$F_n = 2^{2^n} + 1$$
$$\text{exemplos: } F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$$

Fermat apostava que todos os números da forma citada acima seriam primos. Para $n > 5$ são enormes e na época era muito difiícil, ou impossível, testar se eles seriam ou não primos, então Fermat conjecturou que todos os seus números seriam primos. Contudo o matemático suíço *Leonhard Euler* mostrou que a conjectura de *Fermat* não era verdadeira utilizando o seguinte teorema, proofdo por ele mesmo.

Teorema 11. *Se um primo p divide o número de Fermat F_n, então, p é um número da forma $k \cdot 2^{n+2} + 1$*

Assim quando Euler tomou o primo $641 = 5 \cdot 2^7 + 1$, ele descobriu que:

$$F_5 = 641 \cdot 6700417$$

Logo F_5 não é primo. O fato é que é mais difícil procurar por fatores de F_n do que submetê-lo a um teste para verificar se um número é primo ou composto. Por fim, até hoje não se sabe se existem ou não infinitos números primos ou compostos de Fermat.

8 Bibliografia

Referências

1 Ivan Niven: *Números: Racionais e Irracionais*, 1^a edição, Rio de Janeiro, Editora SBM, 2012.

2 Martin Aigner & Gunter M. Ziegler: *Paul Erdós: as mais belas demonstrações matemáticas*, 5^a edição, São Paulo, Editora Blucher, 2014.

3 Djairo Guedes de Figueiredo: *Números Irracionais e Transcendentes*, 3^a edição, Rio de Janeiro, Editora SBM, 2011.

4 Jose Plínio de Oliveira Santos: *Introdução à Teoria dos Números*, 3^a edição, Rio de Janeiro, IMPA, 2020.

5 Euclides: *Os elementos*, 1^a edição, São Paulo, Editora Unesp, 2009.

6 Primos: *Números primos, amigos que causam problemas- Um Triálogo com o Papa Paulo*, Rio de Janeiro, Editora SBM, 2015.

7 Site:⟨*https://g1.globo.com/Noticias/Ciencia/0,,MUL777282-5603, 00-CIENTISTAS+DEFINEM+NUMERO+PRIMO+COM+MILHOES+ DE+DIGITOS.html*⟩, 2024.

8 Gimps:⟨*https://www.mersenne.org/*⟩,2024.

9 EEF:⟨*https://www.eff.org/awards/coop/primeclaim-43112609*⟩ , 2024.

10 Livro I:*A Readable Introduction to Real Mathematics*, Editora Springer, 2^a edição, Suiça, 2018.

11 LVC: ⟨*http://docmadhattan.fieldofscience.com/2016/03/ ludolph-van-ceulen-in-searching-of-pi.html*⟩, 2024. ⟨*https://mathshistory.st-andrews.ac.uk/Biographies/Van_Ceulen/*⟩, 2024.

12 Quadratura: ⟨*https://mathshistory.st-andrews.ac.uk/HistTopics/ Squaring_the_circle/*⟩, 2024.

13 Dia do pi: ⟨*https://web.archive.org/web/20081226041642/http: //www.exploratorium.edu/pi/pi-2008-announce.html*⟩

14 Diego: *Teoria dos Números Transcendentes* Rio de Janeiro, Editora SBM, 1^a edição, 2013.

9 Apêndice

9.1 Números de Fermat

Um número de *Fermat* é um número da forma:

$$F_n = 2^{2^n} + 1 \quad tal\ que\ n \in \mathbb{N} \tag{16}$$

Eles foram estudados pelo matemática Francês *Pierre de Fermat* no século XVII e receberam este nome em sua homenagem. *Fermat* conjecturou que todos os números primos seriam dessa forma, contudo em [7.2.2] o matemático suíço *Leonhard Euler* mostrou que a conjectura estava incorreta. Até o momento em que esse material está sendo escrito não foi demonstrado se há ,ou não, infinitos os primos de *Fermat*.

9.2 Números de Mersenne e Primos de Mersenne

Os números de Mersenne são números que foram estudados pelo monge francês *Marin Mersenne* no século XVII e são números da forma:

$$M_n = 2^n + 1\ \forall n \in \mathbb{N} \tag{17}$$

E um caso especial desses números seriam os primos de *Mersenne* que são:

$$M_p = 2^p + 1\ p \in \mathbb{P} \tag{18}$$

Que são o objeto de procura do grupo GIMPS(8). Contudo cada vez fica mais complicado, caro e trabalhoso encontrar novos primos de *Mersenne* e até o momento em que esse material está sendo escrito não foi demonstrado se há, ou não, infinitos primos de *Mersenne*.