Universidade Federal de Mato Grosso
Instituto de Ciências Exatas e da Terra
Departamento de Matemática

Aplicações da Função Parte Inteira

Ricardo Sávio Aguiar de Souza
Mestrado Profissional em Matemática: PROFMAT/SBM

Orientador: **Prof. Dr. Martinho da Costa Araújo**

Trabalho financiado pela Capes

Cuiabá - MT

Setembro de 2014

Aplicações da
Função Parte Inteira

Este exemplar corresponde à redação final da dissertação, devidamente corrigida e defendida por Ricardo Sávio Aguiar de Souza e aprovada pela comissão julgadora.

Cuiabá, 26 de setembro 2014.

Prof. Dr. Martinho da Costa Araújo
Orientador

Banca examinadora:

Prof. Dr. Martinho da Costa Araújo
Prof. Dr. Reinaldo de Marchi
Prof. Dr. José de Arimatéia Fernandes

Dissertação apresentada ao curso de Mestrado Profissional em Matemática – PROFMAT, desenvolvido pela Sociedade Brasileira de Matemática na Universidade Federal de Mato Grosso, como requisito parcial para obtenção do título **de Mestre em Matemática**.

Dados Internacionais de Catalogação na Fonte.

S729a Souza, Ricardo Sávio Aguiar de.
Aplicações da Função Parte Inteira / Ricardo Sávio Aguiar de Souza. -- 2014
xi, 47 f. : il. ; 30 cm.

Orientador: Martinho da Costa Araújo.
Dissertação (mestrado profissional) - Universidade Federal de Mato Grosso, Instituto de Ciências Exatas e da Terra, Programa de Pós-Graduação em Matemática, Cuiabá, 2014.
Inclui bibliografia.

1. Função parte inteira. 2. Fórmula de Legendre. 3. Teorema de Chebyshev. 4. Jogo de Wythoff. I. Título.

Ficha catalográfica elaborada automaticamente de acordo com os dados fornecidos pelo(a) autor(a).

Dissertação de Mestrado defendida em 26 de setembro de 2014 e aprovada pela banca examinadora composta pelos Professores Doutores

Prof. Dr. Martinho da Costa Araujo

Prof. Dr. Reinaldo de Marchi

Prof. Dr. José de Arimatéia Fernandes

A DEUS e a meus pais.

Agradecimentos

A Deus por me amparar nos momentos de dificuldade e me suprir em todas as minhas necessidades.

Ao meu orientador, Professor Dr. Martinho da Costa Araújo, que compartilhou do saber e das valiosas contribuições para o trabalho. Acima de tudo, obrigado por me acompanhar nesta jornada.

A meus pais, Afonso e Jacira, as quais amo muito, pelo carinho e incentivo.

À minha irmã e seu esposo, Laura e Paulo, meus sobrinhos Gustavo e Rafaeli e minha prima, Fabielle , que me dedicaram sorrisos e atenção sem reservas.

À minha noiva, Raquel, pelo companheirismo.

Aos meus amigos do mestrado, em especial, Nivaldo, Luiz Fernando, Gilliard, Marco, Jesse e Gledson pelos momentos divididos juntos, pelas angústias, alegrias, provas, demonstrações, soluções, teoremas, lemas, exame de qualificação,...

A CAPES pelo auxílio financeiro.

"Em verdade, o que proporciona o máximo de prazer não é o conhecimento e sim a aprendizagem, não é a posse, mas a aquisição, não é a presença, mas o ato de atingir a meta".

(Carl Friedrich Gauss).

Resumo

Neste trabalho trataremos da função parte inteira e suas propriedades. Além disso, mostraremos como calcular o expoente de um número primo na decomposição canônica de n!, determinaremos a ordem de grandeza da função contagem dos números primos e uma formulação matemática para o jogo de Wythoff.

Palavras chave: Função parte inteira, Fórmula de Legendre, Teorema de Chebyshev e o jogo de Wythoff.

Abstract

In this paper work we will discuss about the entere function part and its properties. Besides, we will show how to calculate the exponent of a prime number in the canonical decomposition of n!, We will determine in order of gheatness counting function of prime numbers and a mathematical formulation for the Wythoff game.

Keywords: Integer part function, Legendre formula, Theorem Chebyshev and the Wythoff game.

Sumário

Lista de Figuras

Introdução

"Deus faz aritmética."

(Carl Friedrich Gauss)

A presença da Aritmética na educação formal ou informal, hoje, pode ser entendida como um conjunto de conhecimento que faz parte da necessidade de apropriação de todo cidadão, justificando a busca de compreensão de como esse ramo da matemática lida com os números e com as operações possíveis entre eles.

Tendo em vista a relevância da Aritmética no conjunto de conhecimentos indispensáveis, este trabalho contemplará tópicos que estão presentes no ensino fundamental, médio e algumas aplicações da função parte inteira.

Organizaremos o trabalho da seguinte forma:

No Capítulo 1, trabalharemos ferramentas básicas, como divisibilidade que possibilita discutir como a divisão de um certo número natural por outro nem sempre é possível. Quando não existir uma relação de divisibilidade entre dois números, será possível efetuar tal divisão, conhecida como Divisão Euclidiana. Em seguida apresentaremos os números primos, que desempenham papel fundamental na Aritmética e a eles estão associados problemas famosos, cujas soluções têm resistido aos esforços de várias gerações de matemáticos, segundo HEFEZ[2011]. Na sequência o Teorema Fundamental da Arimética que estabelece a fatoração de números naturais em fatores primos, revelando toda uma estrutura multiplicativa.

Noções básicas de congruência, ou seja a aritmética com os restos da divisão Euclidiana por um número fixado, conforme HEFEZ[2011]. Esse tópico será trabalhado em virtude da divisibilidade por potências de números primos e números binomiais.

No Capítulo 2 apresentaremos uma importante função em teoria dos números, a função parte inteira e suas propriedades. Em seguida apresentaremos um resultado,

devido ao Matemático Francês Adrien-Marie Legendre (Matemático Francês dos séculos XVIII e XIX) que nos ensina a decomposição canônica em fatores primos do fatorial de um número, mesmo que não conheçamos tal decomposição explícita, conforme consta em MUNIZ NETO[2002]. Existe uma belíssima expressão de um certo número natural n, em função dos termos do desenvolvimento p-ádico que determina a potência exata de um primo que divide o fatorial $n!$. Em 1852, Kummer utilizou o resultado de Legendre para determinar a potência exata p^n que divide um coeficiente binomial $\begin{pmatrix} a \\ b \end{pmatrix}$. Os resultados de Legendre e Kummer tiveram aplicação em análise p-ádica, de acordo com RIBENBOIM[2012].

Sabemos que não há qualquer indicação sobre a determinação de uma fórmula dando o enésimo número primo, todavia, é possível estimar, com boa aproximação, o número de primos inferiores a N (principalmente se N é grande). Designaremos por $\pi(x)$ a função contagem dos números primos. Certamente isto não é fácil como se pode esperar, existe sempre algum erro, então estimaremos a sua ordem de grandeza. Um importante progresso para a determinação da ordem de grandeza da função $\pi(x)$ é devido ao Matemático Russo do século XIX Pafnuty Chebyshev que em 1850 apresentou uma estimativa acerca dos números primos , usando método elementares, de acordo com MUNIZ NETO[2002]. Chebyshev também demonstrou o postulado de Bertrand (1845), que afirma que, para todo número natural $n \geq 2$, existe um número primo entre n e o seu dobro $2n$. Na sequência calcularemos precisamente $\pi(x)$, utilizando uma fórmula de Minác. Discutiremos detalhes sobre o Teorema de Chebyshev, o postulado de Bertrand e a fórmula de Minác usando apenas a função parte inteira e a maior potência de p primo que divide o binomial.

No Capítulo 3 apresentaremos uma outra aplicação da função parte inteira, o jogo de Wythoff (um jogo de estratégia), é um exemplo de um jogo combinatório, ou seja, jogo sequencial nos quais ambos os jogadores têm informação completa. Em particular, resolver um jogo combinatório significa determinar quem vence e qual é a estratégia vencedora a cada lance. Todo jogo combinatório pode ser resolvido por um algoritmo que analisa completamente a árvore de opções, portanto não há o elemento sorte. Em seguida estabeleceremos relações entre o jogo de Wythoff, número áureo e a sequência de Fibonacci. Lembrando que a sequêcia de Fibonacci é concebida por $1, 1, 2, 3, 5, 8, 13, ...$ em outras palavras é a soma dos dois números antecessores e a razão áurea é uma constante

real algébrica irracional. É um número que há muito tempo é empregado na arte e aparece em diversas formas da natureza. Contudo existe um fato interessante acerca da sequência de Fibonaci: tomando as razões de cada termo pelo seu antecessor, obtemos uma outra sequência numérica que vai se aproximando de um valor, o número áureo $\varphi = \frac{1+\sqrt{5}}{2}$. Para realizar a formulação matemática do jogo de Wythoff, esses fatos descritos acima serão relevantes.

Com o jogo de Wythoff tentaremos despertar a curiosidade naqueles que dele se aproximarem, quer pela simplicidade de suas regras, quer pelo desafio intelectual de descobrir a maneira de vencer o jogo. O público alvo são todas as séries do ensino fundamental e médio. Na sequência trataremos da divisibilidade da parte inteira de um número irracional e da resolução de exercícios.

Capítulo 1

Noções de Aritmética

Neste capítulo apresentaremos uma breve revisão dos conceitos de Aritmética dos inteiros, tais como divisibilidade, números primos e congruências que serão necessários para o desenvolvimento do segundo e terceiro capítulo deste trabalho. Informamos ao leitor que, as bibliografias utilizadas foram: HEFEZ[2011], SANTOS[1998] e MUNIZ NETO[2002].

1.1 Divisibilidade

Como em tudo há sempre um ponto de partida, o nosso será admitir que o leitor esteja familiarizado com o conjunto dos números naturais e o conjunto dos números inteiros

$$\mathbb{N} = \{0, 1, 2, 3, ...\},$$
$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, ...\}.$$

Definição 1.1.1 *Dados dois números inteiros a e b com $a \neq 0$, diremos que a divide b , escrevendo $a|b$, quando existir $c \in \mathbb{Z}$ tal que $b = ac$. Neste caso, diremos também que a é um divisor ou um fator de b ou, ainda que b é um múltiplo de a.*

Observe que a notação $a|b$ não representa nenhuma operação em $\mathbb{Z}$, nem representa uma fração. Trata-se de uma sentença que diz ser verdade que existe c tal que $b = ac$. A negação dessa sentença é representado por $a \nmid b$, significando que não existe inteiro c tal que $b = ac$.

Proposição 1.1.1 *Sejam* $a, b \in \mathbb{Z}^* = \mathbb{Z} - \{0\}$ *e* $c \in \mathbb{Z}$ *. Então:*

i) $1|a$ *,* $a|a$ *e* $a|0$*.*

ii) *se* $a|b$ *e* $b|c$ *, então* $a|c$ *.*

Demonstração: *i)* Isto decorre das igualdades $a = 1.a$, $a = a.1$ e $a.0 = 0$.

ii) Se $a|b$ e $b|c$ implica que existem $f, g \in \mathbb{Z}$, tais que $b = a.f$ e $c = b.g$. Substituindo o valor de b da primeira equação na outra , obtemos $c = b.g = (a.f).g = a.(f.g)$ o que mostra que $a|c$. ■

O item i) da proposição acima nos diz que todo número inteiro é divisível por 1 e, se não nulo, por si mesmo .

Proposição 1.1.2 *Se* $a, b, c, d \in \mathbb{Z}$ *, com* $a \neq 0$ *e* $c \neq 0$*, então* $a|b$ *e* $c|d \Rightarrow a.c|b.d$*.*

Demonstração: Se $a|b$ e $c|d$, então $\exists\ f, g \in \mathbb{Z},\ b = a.f$ e $d = c.g$. Portanto, $b.d = (a.c)(f.g)$, logo, $a.c|b.d$.

Em particular, se $a|b$, então $a \cdot c|b \cdot c$, para todo $c \in \mathbb{Z}^*$. ■

Proposição 1.1.3 *Sejam* $a,\ b,\ c \in \mathbb{Z}$*,com* $a \neq 0$*, tais que* $a|(b + c)$*. Então* $a|b \Leftrightarrow a|c$*.*

Demonstração: Como $a|(b+c)$, existe $f \in \mathbb{Z}$ tal que $b+c = f.a$. Agora, se $a|b$, temos que exite $g \in \mathbb{Z}$ tal que $b = a.g$. Segue $a.g + c = f.a = a.f$. Portanto, da igualdade acima, obtemos $c = a.f - a.g = a.(f - g)$, o que implica que $a|c$. A prova da outra implicação é totalmente análoga. ■

Proposição 1.1.4 *Se* $a, b, c \in \mathbb{Z}$*, com* $a \neq 0$*, e* $x, y \in \mathbb{Z}$ *são tais que* $a|b$ *e* $a|c$*, então* $a|(xb \pm yc)$*.*

Demonstração: $a|b$ e $a|c$ implicam que existem $f, g \in \mathbb{Z}$ tais que $b = af$ e $c = ag$. logo, $xb \pm yc = x(af) \pm y(ag) = a(xf \pm yg)$. ■

Axioma 1.1.1 *(Princípio da Indução) Seja* A *um subconjunto não vazio de* $\mathbb{N}$*. Se*

i) $1 \in A$*;*

ii) $n + 1 \in A$ *sempre que* $n \in A$*.*

Então $A = \mathbb{N}$*.*

Usaremos este axioma para demonstrar a seguinte afirmação

Proposição 1.1.5 *(Princípio da Boa Ordenação) Todo subconjunto não vazio dos naturais possui um menor elemento.*

Demonstração: Sejam $\mathcal{A}$ um subconjunto não vazio dos naturais, $I_n = \{p \in \mathbb{N};\ 1 \leq p \leq n\}$ e $\mathcal{X} \subset \mathbb{N}$, um conjunto formado pelos elementos $n \in \mathbb{N}$ tais que $I_n \subset \mathbb{N} - \mathcal{A}$.

Se $1 \in \mathcal{A}$, então claramente 1 é o menor elemento de $\mathcal{A}$.

Agora, se $1 \notin \mathcal{A}$, então $1 \in \mathcal{X}$, tendo em vista que $I_1 = \{1\} \subset \mathbb{N} - \mathcal{A}$. Porém $\mathcal{X} \neq \mathbb{N}$, pois $\mathcal{A} \neq \{\ \}$ e $\mathcal{X} \subset \mathbb{N}$.

Logo, o princípio da indução não pode ser aplicado a $\mathcal{X}$, o que implica que o item ii) do axioma, não vale em $\mathcal{X}$, isto é: existe um $n_0 \in \mathcal{X}$ tal que $n_0 + 1 \notin \mathcal{X}$.

Como $I_n \subset \mathbb{N} - \mathcal{A}$, temos que todos os números inteiros de 1 a n_0 pertencem a $\mathcal{X}$ e como $n_0 + 1 \notin \mathcal{X}$, temos que $n_0 + 1 \in \mathcal{A}$ e $I_n = \mathcal{X}$.

Portanto, $a = n_0 + 1$ é o menor elemente de $\mathcal{A}$. ■

Teorema 1.1.1 *Sejam a e b dois números naturais com $0 < a < b$. Existem dois únicos números naturais q e r tais que $b = a.q + r$, com $r < a$.*

Demonstração: Suponha que $b > a$ e considere, os números

$b, b-a, b-2a, b-3a, ..., b-n.a, ...$

Pelo Princípio da Boa Ordenação, o conjunto S formado pelos elementos acima tem um menor elemento $r = b - q.a$. Vamos provar que r tem propriedade requerida , ou seja , que $r < a$.

Se $a|b$, então $r = 0$ e nada mais temos a provar . Se, por outro lado, $a \nmid b$, então $r \neq a$, e, portanto, basta mostrar que não pode ocorrer $r > a$. De fato , se isto ocorresse , existiria um número natural $c < r$ tal que $r = c + a$. Consequentemente, sendo $r = c + a = b - qa$, teríamos $c = b - (q+1).a \in S$, com $c < r$, contradição com o fato de r ser o menor elemento de S.

Portanto , temos que $b = a.q + r$ com $r < a$, o que prova a existência de q e r.

Agora vamos mostrar a unicidade. Note que, dados dois elementos distintos de S , a diferença entre o maior e o menor desses elementos, sendo um múltiplo de a, é pelo menos a Logo, se $r = b - a.q$ e $r' = b - a.q'$, com $r < r' < a$, teríamos $r' - r \geq a$, o que acarretaria $r' \geq r + a \geq a$, absurdo. Portanto, $r = r'$, daí segue-se que $b - a.q = b - a.q'$, o que implica que $a.q = a.q'$ e, portanto, $q = q'$. ■

Nas condições do teorema acima, os números q e r são chamados, respectivamente, de *quociente* e de *resto* da divisão de b por a. A demonstração do teorema fornece um algoritmo para calcular o quociente e o resto da divisão de um número natural por outro, através de subtrações sucessivas.

Exemplo 1.1.1 *Vamos achar o quocinte e o resto da divisão de 19 por 5 .*

Considere as diferenças sucessivas: $19 - 5 = 14,\ 19 - 2.5 = 9,\ 19 - 3.5 = 4 < 5.$ *Isto nos dá* $q = 3$ *e* $r = 4$ *.*

Trataremos a seguir de algumas propriedades acerca do máximo divisor comum.

1.2 Máximo Divisor Comum

Definição 1.2.1 *Dados dois inteiros a e b, chama-se máximo divisor comum de a e b o inteiro positivo ou não-negativo d, que satisfaz as condições:*

(1) Se $a = b = 0$ *então* $d = 0$*;*

(2) Se $a \neq 0$ *ou* $b \neq 0$ *então d é caracterizado pelas propriedades:*

i) $d|a$ *e* $d|b$*;*

ii) Para cada inteiro x, se $x|a$ *e* $x|b$ *então* $x|d$*. Neste caso, temos* $x \leq d$*.*

Se d é o máximo divisor comum de a e b, denotamos por $d = mdc(a, b) = (a, b)$. De maneira mais geral podemos definir $mdc(a_1, a_2, ...a_n)$ para inteiros $a_1, a_2, ...a_n$.

Exemplo 1.2.1 *Os divisores comuns de 24 e 32 são* $\pm 1, \pm 2, \pm 4$ *e* ± 8*. Portanto,* $(24, 32) = 8$*. Analogamente, olhando os conjuntos de divisores comuns, concluímos que* $(35, 55) = 5, (0, 5) = 5, (3, 2) = 1, (-9, -15) = 3$*.*

Definição 1.2.2 *Dois inteiros são ditos* **primos entre si** *quando* $(a, b) = 1$*.*

A proposição seguinte garante a existência do (a, b) em $\mathbb{Z}$, para a e b não simultaneamente nulos. Além disso, fornece uma caracterização extremamente útil para esse (a, b).

Proposição 1.2.1 *Sejam a e b números inteiros não simultaneamente nulos. Então existe* $d = (a, b)$ *em* $\mathbb{Z}$*. Além disso,* $d = (a, b) = min\{ma + nb > 0; m, n \in Z\}$*.*

Demonstração: Consideremos o conjunto $\mathcal{L} = \{ma + nb > 0; m, n \in Z\} \subset Z$. Inicialmente, note que $\mathcal{L} \neq \{\ \}$. De fato, como $a \neq 0$ ou $b \neq 0$, concluímos o inteiro $|a| + |b| > 0$ pertence a $\mathcal{L}$. Além disso, é fácil ver que $\mathcal{L}$ é limitado inferiormente. Logo, pelo Princípio da Boa Ordem, existe $d = min\ \mathcal{L}$.
Resta mostrar que $d = (a, b)$.

Com efeito, por um lado, como $d \in \mathcal{L}$, podemos escrever $d = m_0a + n_0b > 0$, com $m_0, n_0 \in \mathbb{Z}$. Por outro lado, efetuando a divisão euclidiana de a por d, obtemos $t, r \in \mathbb{Z}$ tais que $a = dt + r$, com $0 \leq r < d$. Daí:

$$r = a - dt = a - (m_0a + n_0b)t = a - m_0at - n_0bt = (1 - m_0t)a + (n_0t)b$$

Isto nos permite concluir que $r = 0$. De fato, se fosse $r > 0$, teríamos $r \in \mathcal{L}$, o que não pode ocorrer, uma vez que implicaria em $r < d = min\ \mathcal{L}$. Em vista da equação acima e do fato que $r = 0$, podemos conluir que $a = dt$, e, portanto, $d|a$.

Um raciocínio análogo (efetuando a divisão euclidiana de b por d) nos permite conluir que $d|b$. Logo, $d|a$ e $d|b$, e a condição (i) da definição de mdc está demonstrada.
Para mostrarmos que a condição (ii) também ocorre, seja $x \in \mathbb{Z}$ tal que $x|a$ e $x|b$. Então, existem $u, v \in \mathbb{Z}$ tais que $a = ux$ e $b = vx$. Devemos provar que $x|d$.
Com efeito, uma vez que $d \in \mathcal{L}$, podemos escrever $d = m_0a + n_0b$, $m_0, n_0 \in \mathbb{Z}$. Daí:

$$d = m_0a + n_0b = m_0(ux) + n_0(vx) = (m_0u + n_0v)x$$

O que significa que $x|d$. ■

Corolário 1.2.1 *Sejam $a, b \in \mathbb{Z}$ e $d = (a, b)$. Então existem $r, s \in \mathbb{Z}$ tais que $d = ra + sb$. Em particular, se $a, b \in \mathbb{Z}$ são primos entre si, então existem $r, s \in \mathbb{Z}$ tais que $ra + sb = 1$.*

Demonstração: Segue imediatamente do Proposição anterior. ■

Teorema 1.2.1 *Se $a|bc$ e $(a, b) = 1$, então $a|c$.*

Demonstração: Como $(a, b) = 1$ pelo resultado acima existem inteiros n e m tais que $na + mb = 1$. Multiplicando-se os dois lados desta igualdade por c, temos $cna + cmb = c$. Como $a|ac$ e, por hipótese, $a|bc$ então $a|(n(ac) + m(bc))$ e, portanto $a|c$. ■

1.3 Números Primos

Definição 1.3.1 *Um inteiro $p > 1$ é primo se seus únicos divisores positivos forem ele mesmo e 1. Um inteiro $a > 1$ que não é primo é dito composto .*

Dados dois números primos p e q e um número inteiro a qualquer, decorrem da definição acima as seguintes propriedades:

i) *Se $p|q$ então $p = q$.*

De fato, como $p|q$ e sendo q primo,temos que $p = 1$ ou $p = q$. Sendo p primo, tem-se que $p > 1$, o que acarreta $p = q$.

ii) *Se $p \not| a$, então $(p, a) = 1$.*

De fato, se $(p, a) = d$, temos que $d|p$ e $d|a$. Portanto, $d = p$ ou $d = 1$.Mas $d \neq p$, pois $p \not| a$ e consequentemente , $d = 1$.

Proposição 1.3.1 *Sejam $a, b, p \in \mathbb{Z}^*$,com p primo. Se $p|ab$, então $p|a$ ou $p|b$.*

Demonstração: Basta provar que, se $p|ab$ e $p \not| a$, então $p|b$. Mas, se $p \not| a$, temos que $mdc(p, a) = 1$, e o resultado segue Teorema 1.2.1. ■

Corolário 1.3.1 *Se $p, p_1, ..., p_n$ são números primos e, se $p|p_1...p_n$, então $p = p_i$ para algum $i = 1, ..., n$.*

Demonstração: Use a Proposição 1.3.1 e indução sobre n. Use o fato de que se $p|p_i$, então $p = p_i$. ■

Teorema 1.3.1 *Todo número natural maior do que 1 ou é primo ou se escreve de modo único, a menos da ordem de seus fatores, como um produto de números primos.*

Demonstração: Usaremos o Princípio de Indução. Se n = 2 , o resultado é obviamente verificado.

Suponhamos o resultado válido para todo número natural menor do que n e vamos provar que vale para n. Se o número n é primo, nada temos a demonstrar. Suponhamos, então, que n seja composto. Logo, existem números n_1 e n_2 tais que $n = n_1 n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$. Pela hipótese de indução, temos que existem números primos $p_1, ..., p_r$ e $q_1, ..., q_s$ tais que $n_1 = p_1...p_r$ e $n_2 = q_1...q_s$.*Portanto*, $n = p_1...p_r.q_1...q_s$.

Vamos, agora, provar a unicidade da escrita. Suponha, agora, que $n = p_1...p_r = q_1...q_s$, onde os p_i e os q_j são números primos. Como $p_1|q_1...q_s$, pelo Corolário1.3.1, temos $p_1 = q_j$ para algum j, que, após reordenamento de $q_1, ..., q_s$, podemos supor que seja q_1. Portanto,

$$p_2...p_r = q_2...q_s.$$

Como $p_2...p_r < n$, a hipótese de indução acarreta que $r = s$ e os p_i e q_j são iguais aos pares. ■

Agrupando, os fatores primos repetidos, se necessário, e ordenando os primos em ordem crescente, temos o seguinte enunciado:

Teorema 1.3.2 *Dado um número natural $n > 1$, existem primos $p_1 < ... < p_r$ e $\alpha_1, ..., \alpha_r \in \mathbb{N}^*$, univocamente determinados, tais que*

$$n = p_1^{\alpha_1}... \ p_r^{\alpha_r}.$$

Quando estivermos lidando com a decomposição em fatores primos de dois, ou mais números naturais, usaremos o recurso de acrescentar fatores da forma $p^0 = 1$, onde p é um número primo qualquer. Assim, dados, $m, n \in \mathbb{N}$ com $n > 1$ *e* $m > 1$ quaisquer, podemos escrever

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2}...p_r^{\alpha_r} \text{ e } m = p_1^{\beta_1} \cdot p_2^{\beta_2} ...p_r^{\beta_r}$$

Usando o mesmo conjunto de primos p_1 , p_2 , ... , p_r, desde que permitamos que os expoentes α_1, $\alpha_2, ..., \alpha_r$, β_1, $\beta_2, ...,$ β_r variem em $\mathbb{N}$ e não apenas em $\mathbb{N}^*$.

Exemplo 1.3.1 *Por exemplo, os números* $2^3.3^2.7.11$ *e* $2.5^2.13$ *podem ser escritos,respectivamente,* $2^3.3^2.5^0.7.11.13^0$ *e* $2.3^0.5^2.7^0.11^0.13$.

Apresentaremos aqui uma das noções mais fecundas da Aritmética, a de Congruência, introduzida por Gauss no seu livro *Disquisitiones Arithmeticae*, de 1801. Trata-se da realização de uma aritmética com os restos da divisão euclidiana por um número fixado.

1.4 Congruências

Definição 1.4.1 *Seja m um número natural diferente de zero. Diremos que dois números naturais a e b são congruentes módulo m se os restos de sua divisão euclidiana por m são iguais. Quando os inteiros a e b são congruentes módulo m, escreve-se*

$$a \equiv b \ mod \ m.$$

Exemplo 1.4.1 $21 \equiv 13 \ mod \ 2$*, já que os restos da divisão de 21 e de 13 por 2 são iguais a 1.*

Quando a relação $a \equiv b \ mod \ m$ for falsa, diremos que a e b não são congruentes, ou que são incongruentes, módulo m. Escreveremos, neste caso, $a \not\equiv b \ mod \ m$.

Como o resto da divisão de um número natural qualquer por 1 é sempre nulo, temos que $a \equiv b \ mod \ 1$, quaisquer que sejam $a, \ b \in \mathbb{N}$. Isto torna desinteressante a aritmética dos restos módulo 1. Portanto, doravante, consideraremos sempre $m > 1$. Decorre, imediatamente, da definição que a congruência, módulo um inteiro fixado m, é uma relação de equivalência. Vamos enunciar isto explicitamente abaixo.

Proposição 1.4.1 *Seja $m \in \mathbb{N}$, com $m > 1$. Para todos $a, b, c \in \mathbb{N}$, tem-se que*

(i) $a \equiv a \ mod \ m.$

(ii) *Se* $a \equiv b \ mod \ m$*, então* $b \equiv a \ mod \ m.$

(iii) *Se* $a \equiv b \ mod \ m$ *e* $b \equiv c \ mod \ m$*, então* $a \equiv c \ mod \ m.$

Para verificar se dois números são congruentes módulo m, não é necessário efetuar a divisão euclidiana de ambos por m para depois comparar os seus restos. É suficiente aplicar o seguinte resultado:

Proposição 1.4.2 *Suponha que $a, \ b \in \mathbb{N}$ são tais que $b \geq a$. Então $a \equiv b \ mod \ m$ se, e somente se, $m | b - a$.*

Demonstração: Sejam $a = mq + r$, com $r < m$ e $b = mq' + r'$, com $r' < m$, as divisões euclidianas de a e b por m, respectivamente. Logo,

$$b - a = \begin{cases} m(q' - q) + (r' - r), & se \ r' \geq r \\ m(q' - q) - (r' - r), & se \ r \geq r' \end{cases}$$

onde $r' - r < m$, *ou* $r - r' < m$. Portanto, $a \equiv b \; mod \; m$ se, e somente se, $r = r'$, o que é equivalente a dizer que $m|b - a$. ■

Note que todo número natural é congruente módulo m ao seu resto pela divisão euclidiana por m e, portanto, é congruente módulo m a um dos números $0, 1, ..., m-1$. Além disso, dois desses números distintos não são congruentes módulo m.

Portanto, para achar o resto da divisão de um número a por m, basta achar o número natural r dentre os números $0, 1, ..., m-1$ que seja congruente a a módulo m.

Chamaremos de *sistema completo de resíduos* módulo m a todo conjunto de números naturais cujos resto pela divisão por m são os números $0, 1, ..., m-1$, sem repetições e numa ordem qualquer.

Portanto, um sistema completo de resíduos módulo m possui m elementos.

É claro que, se $a_1, ..., a_m$ são m números naturais, dois a dois não congruentes módulo m, então eles formam um sistema completo de resíduos módulo m. De fato, os restos da divisão dos a_i por m são dois a dois distintos, o que implica que são os números $0, 1, ..., m-1$ em alguma ordem.

O que torna útil e poderosa a noção de congruência é o fato de ser uma relação de equivalência compatível com as operações de adição e multiplicação nos inteiros, conforme veremos na proposição a seguir.

Proposição 1.4.3 *Seja* $a, b, c, d, m \in \mathbb{N}$, *com* $m > 1$.

(i) *Se* $a \equiv b \; mod \; m \;\; e \;\; c \equiv d \; mod \; m$, *então* $a + c \equiv b + d \; mod \; m$.

(ii) *Se* $a \equiv b \; mod \; m \;\; e \;\; c \equiv d \; mod \; m$, *então* $ac \equiv bd \; mod \; m$.

Demonstração: Suponhamos que $a \equiv b \; mod \; m \;\; e \;\; c \equiv d \; mod \; m$. Podemos, sem perca de generalidade, supor que $b \geq a \;\; e \;\; d \geq c$. Logo, temos que $m|b - a \;\; e \;\; m|d - c$.

(i) Basta observar que $m|(b - a) + (d - c)$ e, portanto, $m|(b + d) - (a + c)$, o que prova essa parte do resultado.

(ii) Basta notar que $bd - ac = d(b - a) + a(d - c)$ e concluir que $m|bd - ac$.

■

Corolário 1.4.1 *Para todos* $n \in \mathbb{N}^*$, $a, b \in \mathbb{N}$, *se* $a \equiv b \, mod \, m$, *então* $a^n \equiv b^n \, mod \, m$.

Demonstração: Note inicialmente que se $a \equiv b \, mod \, m$, então $m|a-b$. Repare também que

$$a^n - b^n = (a-b)a^{n-1} + a^{n-2}b + a^{n-3}b^2 + ... + ab^{n-2} + b^{n-1}.$$

Da igualdade acima, obtemos que $m|(a^n - b^n)$ e, portanto $a^n \equiv b^n \, mod \, m$. ■

Teorema 1.4.1 *Se a,b,c e m são inteiros e* $ac \equiv bc \, (mod \, m)$*, então* $a \equiv b \, (mod \, m/d)$*, onde* $d = (c, m)$*.*

Demonstração: Se $ac \equiv bc \, (mod \, m)$, então $m|(ac - bc) = c(a-b)$. Logo existe um inteiro k, tal que

$$c(a-b) = km.$$

Se dividirmos os dois membros da equação acima por d, obtemos $(c/d)(a-b) = k(m/d)$. Logo $(m/d)|(c/d)(a-b)$ e, como $(m/d, c/d) = 1$, pelo Teorema 1.2.1, $(m/d)|(a-b)$, o que implica que $a \equiv b \, (mod \, m/d)$. ■

Teorema 1.4.2 *Sejam* a, b *e* m *inteiros tais que* $m > 0$ *e* $d = (a, m)$*. No caso em que* $d \not| b$ *a congruência* $ax \equiv b \, (mod \, m)$ *não possui nenhuma solução e quando* $d|b$*, possui exatamente d soluções incongruentes módulo m.*

Demonstração: Sabemos que um inteiro x é solução de $ax \equiv b \, (mod \, m)$ se, e somente se, existe outro inteiro y tal que $ax = b + my$, ou, o que é equivalente, $ax + my = b$. Do teorema anterior sabemos que esta equação não possui nenhuma solução caso $d \not| b$, e que se $d|b$ ela possui infinitas soluções dadas $x = x_0 + (b/d)k$ e $y = y_0 - (a/d)k$ onde (x_0, y_0) é uma solução particular de $ax - my = b$. Logo a congruência $ax \equiv b \, (mod \, m)$ possui infinitas soluções dadas por $x = x_0 - \dfrac{m}{d}k$. Como estamos interessados em saber o número de soluções incongruentes, vamos tentar descobrir sob que condições $x_1 = x_0 - (m/d)k_1$ e $x_2 = x_0 - (m/d)k_2$ são congruentes módulo m. Se x_1 e x_2 são congruentes então $x_0 - (m/d)k_1 \equiv x_0 - (m/d)k_2 \, (mod \, m)$. Isto implica $(m/d)k_1 \equiv (m/d)k_2 \, (mod \, m)$, e como $(m/d)|m$, temos $(m/d, m) = m/d$, o que nos permite o cancelamento de m/d resultando, pelo Teorema 1.4.1, que $k_1 \equiv k_2 \, (mod \, m)$. Observe que m foi subtituído por $d = m/(m/d)$. Isto nos mostra que soluções incongruentes serão obtidas ao tomarmos $x = x_0 - (m/d)k$, onde k percorre um sistema completo de resíduos módulo d, o que conclui a demonstração. ■

Teorema 1.4.3 *(Teorema de Wilson) Se p é primo, então* $(p-1)! \equiv -1 \ (mod\ p)$.

Demonstração: Como $(2-1)! \equiv 1 \equiv -1 \ (mod\ 2)$ o resultado é valido para $p = 2$. Pelo Teorema 1.4.2, a congruência $ax \equiv \ 1 \ (mod\ m)$ tem uma única solução para todo a no conjunto $\{1, 2, 3, ..., p-1\}$ e como, destes elementos, somente 1 e $p-1$ são seus próprios inversos módulo p, podemos agrupar os números $2, 3, 4, ..., p-2$ em $(p-3)/2$ pares cujo produto seja congruente a 1 módulo p. Se multiplicarmos estas congruências, membro a membro, teremos, pelo Teorema $...2 \times 3 \times 4 \times ... \times (p-2) \equiv 1 \ (mod\ p)$. Multiplicando-se ambos os lados desta congruência por $p-1$ teremos

$$2 \times 3 \times 4 \times ... \times (p-2)(p-1) \equiv (p-1) \equiv -1 \ (mod\ p).$$

■

Capítulo 2

A Função Parte Inteira

Neste capítulo apresentaremos a função parte inteira e suas propriedades, a Fórmula de Legendre, o Teorema de Kummer, o Teorema de Chebyshev, a Fórmula de Minác, além Congruências e números binomiais. As bibliografias utilizadas foram: HEFEZ[2011], SANTOS[1998], MUNIZ NETO[2002], RIBENBOIM[2012] e FEITOSA[2012]

2.1 Definição e Algumas Propriedades

Definição 2.1.1 *A parte inteira de um número real x é o maior inteiro $\lfloor x \rfloor$ menor do que ou igual x. Definimos a parte fracionária $\{x\}$ de x por $\{x\} = x - \lfloor x \rfloor$.*

Exemplo 2.1.1 $\lfloor 3 \rfloor = 3$, $\lfloor 3,5 \rfloor = 3$ *e* $\lfloor -4,7 \rfloor = -5$.

Teorema 2.1.1 *Sejam x e y números reais. Então:*

i) $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$ *e* $0 \leq \{x\} < 1$.

ii) $\lfloor x + m \rfloor = \lfloor x \rfloor + m$ *se m é inteiro.*

iii) $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1$.

iv) $\left\lfloor \dfrac{\lfloor x \rfloor}{m} \right\rfloor = \left\lfloor \dfrac{x}{m} \right\rfloor$ *se m é um número inteiro positivo.*

v) *Se n e a são inteiros positivos então* $\left\lfloor \dfrac{n}{a} \right\rfloor$ *é o número de inteiros $1, 2, 3, ..., n$ que são divisíveis por a.*

Demonstração:

i) Temos por definição $\lfloor x \rfloor \leq x = \lfloor x \rfloor + \{x\}$ como $\{x\} < 1$, segue $x < \lfloor x \rfloor + 1$.

ii) Seja $x = k + \alpha$, sendo k parte inteira e α parte fracionária. Logo $\lfloor x + m \rfloor = \lfloor k + \alpha + m \rfloor$. Segue $\lfloor k + m + \alpha \rfloor = k + m$ (por hipótese m é inteiro) mas $k = \lfloor x \rfloor$ e portanto $\lfloor x + m \rfloor = \lfloor x \rfloor +$ m.

iii) Veja que:

$$\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + \lfloor \{x\} + \{y\} \rfloor = \lfloor \lfloor x \rfloor + \lfloor y \rfloor + \{x\} + \{y\} \rfloor = \lfloor x + y \rfloor.$$

Como $\{x\} + \{y\} < 2$, $\lfloor \{x\} + \{y\} \rfloor \leq 1$ e daí:

$$\lfloor x + y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor + \lfloor \{x\} + \{y\} \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1$$

.

iv) Seja $\lfloor x \rfloor = qm + r$ com $0 \leq r < m - 1$, então :

$$\left\lfloor \frac{\lfloor x \rfloor}{m} \right\rfloor = \left\lfloor q + \frac{r}{m} \right\rfloor = q.$$

Como $0 \leq \{x\} < 1$, $q = q + \left\lfloor \dfrac{r + \{x\}}{m} \right\rfloor = \left\lfloor \dfrac{qm + r + \{x\}}{m} \right\rfloor = \left\lfloor \dfrac{x}{m} \right\rfloor$.

v) Sejam $a, 2a, 3a, ..., ja$ todos os inteiros positivos $\leq n$ que são divisíveis por a, então,

$$ja \leq n < (j+1)a \Rightarrow j \leq \frac{n}{a} < j + 1 \Rightarrow j = \left\lfloor \frac{n}{a} \right\rfloor.$$

■

Suponha que sabemos que um certo natural n admite um divisor primo p. O teorema a seguir, devido ao matemático francês Adrien - Marie Legendre, ensina como calcular o expoente de p na decomposição canônica de n em fatores primos, mesmo que não conheçamos tal decomposição explícita. A fórmula é conhecida como a *Fórmula de Legendre* ou *Fórmula de Polignac*.

Definiremos por $\mathbf{E_p(n!)}$ o expoente da maior potência de p que divide $n!$, ou seja, é o expoente da potência de p que aparece na fatoração de $n!$ em fatores primos.

2.2 Teorema de Legendre

Teorema 2.2.1 *Sejam n um número natural e p um número primo. Então,*

$$E_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \left\lfloor \frac{n}{p^4} \right\rfloor + ...$$

Demonstração: Note inicialmente que a soma acima é finita, uma vez que, para $p^k > n$, temos $\left\lfloor \frac{n}{p^k} \right\rfloor = 0$. No produto $n! = 1.2.3.4...n$, apenas os múltiplos p contribuem com um fator p. Segue pelo Teorema2.1.1 (item v) que há $\left\lfloor \frac{n}{p} \right\rfloor$ múltiplos de p entre 1 e n. Destes, os que são múltiplos de p^2 contribuem com um fator p entra e há $\left\lfloor \frac{n}{p^2} \right\rfloor$ tais fatores. Dentre estes últimos, os que são múltiplos de p^3 contribuem com mais um fator p extra e assim por diante, resultando na fórmula acima. ■

Exemplo 2.2.1 *Determinar a decomposição de* $10!$ *em fatores primos.*

Pela Fórmula de Legendre temos :

$$E_2(10!) = \left\lfloor \frac{10}{2} \right\rfloor + \left\lfloor \frac{10}{2^2} \right\rfloor + \left\lfloor \frac{10}{2^3} \right\rfloor = 5 + 2 + 1 = 8.$$

$$E_3(10!) = \left\lfloor \frac{10}{3} \right\rfloor + \left\lfloor \frac{10}{3^2} \right\rfloor = 3 + 1 = 4.$$

$$E_5(10!) = \left\lfloor \frac{10}{5} \right\rfloor = 2.$$

$$E_7(10!) = \left\lfloor \frac{10}{7} \right\rfloor = 1.$$

Segue $10! = 2^8.3^4.5^2.7^1$.

Exemplo 2.2.2 *(União Soviética) Ache o número de zeros consecutivos no final de* $1000!$.

Pela fórmula de Legendre temos :

$$E_2(1000!) = \left\lfloor \frac{1000}{2} \right\rfloor + \left\lfloor \frac{1000}{2^2} \right\rfloor + \left\lfloor \frac{1000}{2^3} \right\rfloor + \left\lfloor \frac{1000}{2^4} \right\rfloor + ... + \left\lfloor \frac{1000}{2^8} \right\rfloor + \left\lfloor \frac{1000}{2^9} \right\rfloor.$$

$$E_2(1000!) = 500 + 250 + 125 + 62 + 31 + 15 + 7 + 3 + 1 = 994.$$

$E_5(1000!) = \left\lfloor \frac{1000}{5} \right\rfloor + \left\lfloor \frac{1000}{5^2} \right\rfloor + \left\lfloor \frac{1000}{5^3} \right\rfloor + \left\lfloor \frac{1000}{5^4} \right\rfloor$. $E_5(1000!) = 200 + 40 + 8 + 1 = 249.$

Segue $1000! = 2^{994}.5^{249}.\alpha = 2^{249}.5^{249}.(2^{745}.\alpha)$, *Com* $\alpha \in \mathbb{Z}$. $1000! = 10^{249}.\beta$, *com* $\beta \in \mathbb{Z}$ *ou seja termina em 249 zeros.*

Exemplo 2.2.3 *É possível repartir exatamente* $\begin{pmatrix} 2357 \\ 528 \end{pmatrix}$ *objetos entre 49 pessoas ?*

Temos $\begin{pmatrix} 2357 \\ 528 \end{pmatrix} = \dfrac{2357!}{528!(2357-528)!} = \dfrac{2357!}{528!1829!}$.

$$E_7(2367!) = \left\lfloor \frac{2357}{7} \right\rfloor + \left\lfloor \frac{2357}{7^2} \right\rfloor + \left\lfloor \frac{2357}{7^3} \right\rfloor = 336 + 48 + 6 = 390.$$

$$E_7(1829!) = \left\lfloor \frac{1829}{7} \right\rfloor + \left\lfloor \frac{1829}{7^2} \right\rfloor + \left\lfloor \frac{1829}{7^3} \right\rfloor = 261 + 37 + 5 = 303.$$

$$E_7(528!) = \left\lfloor \frac{528}{7} \right\rfloor + \left\lfloor \frac{528}{7^2} \right\rfloor + \left\lfloor \frac{528}{7^3} \right\rfloor = 75 + 10 + 1 = 86.$$

Segue que $2357! = 7^{390}.\alpha$, $1829! = 7^{303}.\beta$, $528! = 7^{86}.\theta$. Sendo $\alpha, \beta, \theta \in \mathbb{Z}$.

$\dfrac{2357!}{1829!.528!} = \dfrac{7^{390}}{7^{303}.7^{86}} = 7\omega$, com $\omega \in \mathbb{Z}$. Logo não é possível repartir exatamente para 49 pessoas.

Exemplo 2.2.4 *Mostre que* $2^{1000} \mid 1001.1002.1003...2000$ *mas que* $2^{1001} \nmid 1001.1002.1003...2000$.

Note que $1001.1002.1003...2000 = \dfrac{2000!}{1000!}$.

$$E_2(2000!) = \left\lfloor \frac{2000}{2} \right\rfloor + \left\lfloor \frac{2000}{2^2} \right\rfloor + \left\lfloor \frac{2000}{2^3} \right\rfloor + ... + \left\lfloor \frac{2000}{2^{10}} \right\rfloor$$

$$E_2(2000!) = 1000 + 500 + 250 + 125 + 62 + 31 + 15 + 7 + 3 + 1 = 1994.$$

Realizando o mesmo procedimento teremos, $E_2(1000!) = 994$.

Logo $\dfrac{2000!}{1000!} = \dfrac{2^{1994}.\alpha}{2^{994}.\beta} = 2^{1000}.\theta$, com $\alpha,\ \beta,\ \theta \in \mathbb{Z}$.

O próximo Teorema relacionará $E_p(n!)$ e a representação p-ádica de n isto é, a representação relativa à base p.

Teorema 2.2.2 *Sejam* $p, n \in \mathbb{N}^*$ *com* p *primo. Suponha que*

$$n = n_r p^r + n_{r-1} p^{r-1} + n_{r-3} p^{r-3} + ... + n_1 p + n_0$$

seja a representação p-ádica de n. Então

$$E_p(n!) = \frac{n - (n_0 + n_1 + n_2 + ... + n_r)}{p-1}.$$

Demonstração: Sendo $0 \leq n_i \leq p$, temos

$$\left\lfloor \frac{n}{p} \right\rfloor = n_r p^{r-1} + n_{r-1} p^{r-2} + ... + n_2 p + n_1$$

$$\left\lfloor \frac{n}{p^2} \right\rfloor = n_r p^{r-2} + n_{r-1} p^{r-3} + ... + n_2$$

$$\left\lfloor \frac{n}{p^3} \right\rfloor = n_r p^{r-3} + n_{r-1} p^{r-4} + ... + n_3$$

$$\vdots$$

$$\left\lfloor \frac{n}{p^r} \right\rfloor = n_r$$

Somando membro a membro e aplicando a fórmula da soma dos termos de uma *progressão geométrica de razão q* teremos,

$$E_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + ... + \left\lfloor \frac{n}{p^r} \right\rfloor = n_r \frac{p^r - 1}{p-1} + n_{r-1} \frac{p^{r-1} - 1}{p-1} + n_{r-2} \frac{p^{r-2} - 1}{p-1} + ... + n_1 =$$

$$\frac{n_r p^r + n_{r-1} p^{r-1} + ... + n_1 p + n_0 - (n_r + n_{r-1} + ... + n_1 + n_0)}{p-1} = \frac{n - (n_0 + n_1 + ... + n_r)}{p-1}.$$

■

Exemplo 2.2.5 *Determinar a maior potência de 3 que divide 150!.*

$150 = (12120)_3$ pelo teorema anterior segue que

$$E_3(150)! = \frac{150 - (1 + 2 + 1 + 2 + 0)}{3-1} = 72.$$

Exemplo 2.2.6 *Ache o menor valor de n, de modo que a maior potência de 5 que divide n! seja 5^{84}. Quais são os outros números que gozam dessa propriedade?*

Pelo Teorema anterior temos $E_5(n!) = \frac{n - (n_0 + n_1 + n_3 + ... + n_r)}{5-1}$

$$84 = \frac{n - (n_0 + n_1 + ... + n_r)}{4} \text{ segue,}$$

$$n - (n_0 + n_1 + n_2 + ... + n_r) = 336 \Rightarrow n = 336 + (n_0 + n_1 + n_2 + ... + n_r).$$

Tomando $n = 336$ e calculando $E_5(336!) = 82$. Observe que se acrescentarmos mais uma unidade nas potências de 5 precisamos de mais um múltiplo de 5. Logo $E_5(345!) = 84$. O menor valor de n é 345. Outros números que gozam dessa propriedade é $346!,\ 347!,\ 348!,\ 349!$.

Em 1852, *Kummer* utilizou o resultado de *Legendre* para determinar a potência exata p^n que divide um coeficiente binomial $\begin{pmatrix} n \\ m \end{pmatrix}$.

2.3 Teorema de Kummer

Teorema 2.3.1 *(Teorema de Kummer) Dados $n \geq 1$, $0 \leq m \leq n$ e p primo, o expoente da maior potência de p que divide $\begin{pmatrix} n \\ m \end{pmatrix}$ é igual ao número de "vai-uns"na soma $n = m + (n - m)$ calculada na base p.*

Observação: o termo "vai-uns"se baseia no valor posicional ou seja é na realidade "vai uma dezena"ou "vai uma centena"e assim sucessivamente de números escritos na base 10. De maneira geral "vai-uns"é o número de retenções na adição de $m + (n - m)$ escritos na base p.

Exemplo 2.3.1 *Note que $265 + 167 = 432$, ocorreram dois "vai-uns".*

Denotaremos por $s_p(n)$ a soma dos algarismos p-ádicos de n e ψ sendo o número de "vai-uns".

Demonstração: *Temos $\begin{pmatrix} n \\ m \end{pmatrix} = \frac{n!}{m!(n-m)!}$, pelo Teorema 2.2.2 o expoente da maior potência de p que divide o binomial é*

$$\frac{n - s_p(n)}{p-1} - \left(\frac{m - s_p(m)}{p-1} + \frac{n - m - s_p(n-m)}{p-1} \right) \text{ segue}$$

$$\frac{n - s_p(n) - m + s_p(m) - n + m + s_p(n-m)}{p-1} = \frac{s_p(m) + s_p(n-m) - s_p(n)}{p-1} \ (*)$$

Por outro lado $m = b_k b_{k-1} ... b_1 b_0$ e $n - m = c_k c_{k-1} ... c_1 c_0$ escritos na base p logo na operação $m + (n - m) = (b_k + c_k)(b_{k-1} + c_{k-1})...(b_1 + c_1)(b_0 + c_0)$

Quando há "vai-um"temos $b_i + c_i \geq p \Rightarrow b_i + c_i = p + d_i$, *com*
$0 \leq d_i \leq p-1 < p \Rightarrow b_i + c_i = (1d_i)_p = p + d_i$. *Note que para cada operação de "vai-um", a soma dos algarismos do resultado diminui de* $p-1$. *No fim,*
$s_p(n) = s_p(m) + s_p(n-m) - (p-1).\psi \Rightarrow \psi = \dfrac{s_p(m) + s_p(n-m) - s_p(n)}{p-1}$ *que comparando com* $(*)$ *completa a demonstração.* ■

Exemplo 2.3.2 *É possível repartir exatamente* $\begin{pmatrix} 2357 \\ 528 \end{pmatrix}$ *objetos entre* 49 *pessoas ?*

Notemos que $\begin{pmatrix} 2357 \\ 528 \end{pmatrix} = \begin{pmatrix} 1829 + 528 \\ 528 \end{pmatrix}$. *O próximo passo é escrever* 1829 *e* 528 *na base* 7. *Segue*

$$(1829)_{10} = (5222)_7 \text{ e } (528)_{10} = (1353)_7 \Rightarrow (5222)_7 + (1353)_7 = (6605)_7$$

.

Na operação anterior ocorreu 1 *"vai-um", logo pelo teorema anterior a maior potência de* 7 *que divide o binomial é* 1.

O Teorema a seguir é uma estimativa da distribuição de números primos ao longo dos naturais. Esse resultado é devido ao Matemático Russo do século XIX Pafnuty Chebyshev. Antes de enunciá-lo apresentaremos alguns resultados auxiliares e para cada número real positivo x, *denotaremos por* $\pi(x)$ *o número de primos menores ou iguais a* x.

2.4 O Teorema de Chebyshev

Lema 2.4.1 $\forall \in \mathbb{N}^*$ *temos* $2^{2n} > \begin{pmatrix} 2n \\ n \end{pmatrix}$.

Demonstração: *Note que* $2^{2n} = (1+1)^{2n} = \sum_{k=0}^{2n} \begin{pmatrix} 2n \\ k \end{pmatrix}$, *Assim*

$$\sum_{k=0}^{2n} \begin{pmatrix} 2n \\ k \end{pmatrix} > \begin{pmatrix} 2n \\ n \end{pmatrix}.$$

■

Lema 2.4.2 *Se* $m > 4$ *então* $\frac{m.log2}{log\frac{m}{2}} < \frac{2m.log2}{log\ m}$.

Demonstração: *Como* $m > 4$, *temos que* $log\ m > log2^2 \Rightarrow 2log\ m - log\ m > 2log\ 2 \Rightarrow 2log\ m - 2log\ 2 > log\ m \Rightarrow \frac{1}{2log\ m - 2log\ 2} < \frac{1}{log\ m} \Rightarrow \frac{1}{log\ m - log2} < \frac{2}{log\ m} \Rightarrow \frac{m.log\ 2}{log\ \frac{m}{2}} < \frac{2m.log2}{log\ m}$. ■

Lema 2.4.3 *Seja* $E_p = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$ *então* $E_p = \sum_{k=1}^{\left\lfloor \frac{log\ n}{log\ p} \right\rfloor} \left\lfloor \frac{n}{p^k} \right\rfloor$.

Demonstração: *Se* $p^k > n$ *então* $\left\lfloor \frac{n}{p^k} \right\rfloor = 0$. *Segue* $p^k > n \Rightarrow log\ p^k > log\ n \Rightarrow k.log\ p > log\ n \Rightarrow k > \frac{log\ n}{log\ p}$. *Portanto* $E_p = \sum_{k=1}^{\left\lfloor \frac{log\ n}{log\ p} \right\rfloor} \left\lfloor \frac{n}{p^k} \right\rfloor$. ■

Lema 2.4.4 $\lfloor 2x \rfloor - 2 \lfloor x \rfloor \in \{0, 1\}\ \forall x \in \mathbb{R}$.

Demonstração: *Pelo Teorema 2.1.1 temos* $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1 \Rightarrow 2 \lfloor x \rfloor \leq 2x < 2 \lfloor x \rfloor + 2$. *Por outro lado* $\lfloor 2x \rfloor \leq 2x$ *e* $2 \lfloor x \rfloor \leq 2x \Rightarrow 2 \lfloor x \rfloor - \lfloor 2x \rfloor \leq 0 \Rightarrow \lfloor 2x \rfloor - 2 \lfloor x \rfloor \geq 0.(*)$
Segue $\lfloor 2x \rfloor \leq 2x < 2 \lfloor x \rfloor + 2 \Rightarrow 2 \lfloor x \rfloor \leq \lfloor 2x \rfloor < 2 \lfloor x \rfloor + 2 \Rightarrow \lfloor 2x \rfloor \leq 2 \lfloor x \rfloor + 1 \Rightarrow \lfloor 2x \rfloor - 2 \lfloor x \rfloor \leq 1$ *e por* $(*) \Rightarrow 0 \leq \lfloor 2x \rfloor - 2 \lfloor x \rfloor \leq 1$. ■

Lema 2.4.5 *Seja* $n \in \mathbb{N}$ *então* $log \begin{pmatrix} 2n \\ n \end{pmatrix} > 2n.log2 - log(2n + 1)$.

Demonstração: *A razão de dois termos consecutivos é* $\frac{\begin{pmatrix} 2n \\ k+1 \end{pmatrix}}{\begin{pmatrix} 2n \\ k \end{pmatrix}} = \frac{2n-k}{k+1}$. *Note que se* $k < n$ *então* $\frac{2n-k}{k+1} > 1$, *agora se* $k \geq n$ *então* $\frac{2n-k}{k+1} < 1$. *Em particular*

$$\begin{pmatrix} 2n \\ n \end{pmatrix} > 2^{2n}.\frac{1}{2n+1} = \frac{2^{2n}}{2n+1} \Rightarrow log \begin{pmatrix} 2n \\ n \end{pmatrix} > log\frac{2^{2n}}{2n+1} \Rightarrow$$

$$log \begin{pmatrix} 2n \\ n \end{pmatrix} > 2n.log2 - log2n + 1.$$ ■

Lema 2.4.6 *Se* $n > 3$ *então* $\dfrac{2nlog\ 2 - log\ (2n+1)}{log\ 2n} > \dfrac{2nlog\ 2}{2log\ 2n}$.

Demonstração: *Como* $n > 3$, *temos que* $2^n > 2n+1$ *(para verificar basta aplicar indução sobre* n*) segue* $log\ 2^n > log\ (2n+1) \Rightarrow nlog\ 2 - log\ (2n+1) > 0 \Rightarrow$

$2nlog\ 2 - log\ (2n+1) > nlog\ 2 \Rightarrow \dfrac{2nlog\ 2 - log(2n+1)}{log\ 2n} > \dfrac{nlog\ 2}{log\ 2n}$. ■

Teorema 2.4.1 *(Teorema de Chebyshev) Existem constantes* $o < c < C$ *tais que* $\dfrac{m}{log\ m} \cdot c < \pi\,(m) < C \cdot \dfrac{m}{log\ m}\ \forall\ m\ >\ 4$.

Demonstração: *Se* p *é primo e* $n < p \leq 2n$ *então* $p| \begin{pmatrix} 2n \\ n \end{pmatrix}$, *de fato* $\begin{pmatrix} 2n \\ n \end{pmatrix} = \dfrac{(2n)!}{n!n!} = \dfrac{2n.(2n-1).(2n-2)...p...n!}{n!n!}$. *Logo* $\begin{pmatrix} 2n \\ n \end{pmatrix}$ *é múltiplo de todos os primos entre* n *e* $2n$ *então* $\prod p \leq \begin{pmatrix} 2n \\ n \end{pmatrix}$. *Pelo Lema 2.4.1 temos* $\prod P \leq \begin{pmatrix} 2n \\ n \end{pmatrix} < 2^{2n}$, *como* $p > n \Rightarrow$

$$\begin{aligned} p_1 &> n \\ p_2 &> n \\ p_3 &> n \\ &\vdots \end{aligned}$$

$n^{\pi(2n)-\pi(n)} < \prod p < 2^{2n} \Rightarrow log\ n^{\pi(2n)-\pi(n)} < log 2^{2n} \Rightarrow$
$(\pi(2n) - \pi(n)).log\ n < 2n.log\ 2 \Rightarrow \pi(2n) - \pi(n) < \dfrac{2n.log\ 2}{log\ n}$. *Fazendo* $m = 2n$

$$\begin{aligned} \pi(m) - \pi(\frac{m}{2}) &< \frac{m.log\ 2}{log\frac{m}{2}}, \text{ pelo Lema 2.4.2} \\ \pi(m) - \pi(\frac{m}{2}) &< \frac{m.log\ 2}{log\frac{m}{2}} < \frac{2m.log\ 2}{log\ m} \\ \pi(\frac{m}{2}) - \pi(\frac{m}{4}) &< \frac{\frac{m}{2}.log\ 2}{log\frac{m}{4}} < \frac{m.log\ 2}{log\ m} \\ \pi(\frac{m}{4}) - \pi(\frac{m}{8}) &< \frac{\frac{m}{4}.log\ 2}{log\frac{m}{8}} < \frac{\frac{m}{2}.log\ 2}{log\ m} \\ &\vdots \end{aligned}$$

$$\pi(m) < 2m\frac{log\ 2}{log\ m} + m\frac{log\ 2}{log\ m} + \frac{m}{2}\frac{2}{log\ m} + ... + \frac{m}{2^r}\frac{2}{log\ m}$$
$$\pi(m) < \frac{log\ 2}{log\ m}(2m + m + \frac{m}{2} + ... + \frac{m}{2^r})$$
$$\pi(m) < \frac{log\ 2}{log\ m}4m.(1 - \frac{1}{2^r}) < \frac{m}{log\ m}5log2$$

Tome $C = 5log\ 2$ *segue* $\pi(m) < \frac{m}{log\ m}.C$. *O próximo passo é realizarmos a estimativa por baixo, segue*

$$\binom{2n}{n} = \frac{(2n)!}{n!n!} = \prod p^{E_p}\ e\ E_p = \sum_{k=1}^{\infty}(\left\lfloor\frac{2n}{p^k}\right\rfloor - \left\lfloor\frac{n}{p^k}\right\rfloor - \left\lfloor\frac{n}{p^k}\right\rfloor) = \sum_{k=1}^{\infty}(\left\lfloor\frac{2n}{p^k}\right\rfloor - 2\left\lfloor\frac{n}{p^k}\right\rfloor).$$

Pelo Lema 2.4.3 :

$$\sum_{k=1}^{\infty}(\left\lfloor\frac{2n}{p^k}\right\rfloor - 2\left\lfloor\frac{n}{p^k}\right\rfloor) = \sum_{k=1}^{\lfloor\frac{log\ 2n}{log\ p}\rfloor}(\left\lfloor\frac{2n}{p^k}\right\rfloor - 2\left\lfloor\frac{n}{p^k}\right\rfloor).$$

Pelo Lema 2.4.4 $\left\lfloor\frac{2n}{p^k}\right\rfloor - 2\left\lfloor\frac{n}{p^k}\right\rfloor$ *só pode ser 0 ou 1, então:*

$$E_p = \sum_{k=1}^{\lfloor\frac{log\ 2n}{log\ p}\rfloor}(\left\lfloor\frac{2n}{p^k}\right\rfloor - 2\left\lfloor\frac{n}{p^k}\right\rfloor) \leq \left\lfloor\frac{log\ 2n}{log\ p}\right\rfloor \leq \frac{log\ 2n}{log\ p} \Rightarrow E_p\ log\ p \leq log\ 2n.(*)$$

$$\binom{2n}{n} = \prod p^{E_p} \Rightarrow log\ \binom{2n}{n} = log\ \prod p^{E_p} = \sum_{p\ primo} E_p\ log\ p \leq \sum_{p\ primo} log\ 2n =$$

$\pi(2n).log(2n)$ *(observe em* $(*)$ *para verificar a desigualdade)*

$$log\binom{2n}{n} \leq \pi(2n).log\ 2n \Rightarrow \frac{log\binom{2n}{n}}{log\ 2n} \leq \pi(2n).$$ *Pelo Lema 2.4.5 e Lema 2.4.6 segue*

$$\pi(2n) \geq \frac{log\binom{2n}{n}}{log\ 2n} \geq \frac{2nlog\ 2 - log(2n+1)}{log\ 2n} > \frac{nlog\ 2}{log\ 2n}.$$ *Tome* $m = 2n\ e\ c = \frac{log\ 2}{2}$ *logo*

$$\pi(m) > \frac{m}{log\ m}c \Rightarrow \frac{m}{log\ m}c < \pi(m) < \frac{m}{log\ m}C.$$ ■

Nosso próximo resultado é também devido a Chebyshev, que afirma que os primos não são tão "esparsos"assim. Ele é chamado de postulado de Bertrand por razões históricas.

2.5 O Postulado de Bertrand

Lema 2.5.1 *Sejam n um número natural e p um número primo. Seja θ_p o inteiro tal que $p^{\theta_p} \leq 2n < p^{\theta_p+1}$. Então o expoente da maior potência de p que divide $\begin{pmatrix} 2n \\ n \end{pmatrix}$ é menor ou igual a θ_p. Em particular, se $p > \sqrt{2n}$ então o expoente desta máxima potência de p é menor do que ou igual a 1. Além disso, se $\frac{2}{3}n < p < n$ então p não divide $\begin{pmatrix} 2n \\ n \end{pmatrix}$.*

Demonstração: *Sejam α e β os expoentes das maiores potência de p que dividem $(2n)!$ e $n!$ respectivamente. Sabemos que*

$$\alpha = \left\lfloor \frac{2n}{p} \right\rfloor + \left\lfloor \frac{2n}{p^2} \right\rfloor + \left\lfloor \frac{2n}{p^3} \right\rfloor + ... \quad e \quad \beta = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + ...$$

Portanto o expoente da máxima potência de p que divide $\begin{pmatrix} 2n \\ n \end{pmatrix} = \frac{(2n!)}{n!n!}$ é

$$\alpha - \beta = \sum_{i=1}^{\theta_p} \left\lfloor \frac{2n}{p^i} \right\rfloor - 2 \left\lfloor \frac{n}{p^i} \right\rfloor.$$

Pelo Lema 2.4.4 que $\alpha - \beta$ só pode ser 0 ou 1. Concluímos que

$$\alpha - 2\beta \leq \sum_{i=1}^{\theta_p} 1 = \theta_p.$$

Além disso, se $\frac{2n}{3} < p < n \Rightarrow \frac{1}{n} < \frac{1}{p} < \frac{3}{2n} \Rightarrow 1 < \frac{n}{p} < \frac{3}{2} \Rightarrow \left\lfloor \frac{n}{p} \right\rfloor = 1$, da mesma forma $\frac{1}{n} < \frac{n}{p^2} < \frac{9}{4n} \Rightarrow \left\lfloor \frac{n}{p^2} \right\rfloor = 0$, portanto

$$\beta = 1 + 0 + 0 + 0 + 0 + ... = 1$$

Como $\frac{1}{n} < \frac{1}{p} < \frac{3}{2n} \Rightarrow 2 < \frac{2n}{p} < 3 \Rightarrow \left\lfloor \frac{2n}{p} \right\rfloor = 2$, de maneira análoga $\left\lfloor \frac{n}{p^2} \right\rfloor = 0$, portanto

$$\alpha = 2 + 0 + 0 + 0... = 2$$

Então $\alpha - \beta = 2 - 2.1 = 0$ ■

Lema 2.5.2 *Para todo $n \geq 2$, temos*

$$\prod_{p \leq n} p < 4^n.$$

Demonstração: *A prova é por indução em n. Para isso, vemos que para n pequeno tal desigualdade é válida. Além disso, se o resultado vale para $n = 2m+1$ então também vale para $n = 2m+2$ pois não agregamos novos primos ao produto quando passamos de $2m+1$ para $2m+2$. Logo basta provar a desigualdade para um valor ímpar $n = 2m+1$.*

Dado que para todo primo p tal que $m+1 < p \leq 2m+1$ tem-se que p divide $(2m+1)!$ mas não divide $(m+1)!$ nem $m!$ então

$$\prod_{m+1<p\leq 2m+1} p < \left(\begin{array}{c} 2m+1 \\ m+1 \end{array} \right) = \left(\begin{array}{c} 2m \\ m+1 \end{array} \right) + \left(\begin{array}{c} 2m \\ m \end{array} \right) \text{ (Relação de Stifel)}$$

$$\prod_{m+1<p\leq 2m+1} p < \left(\begin{array}{c} 2m+1 \\ m+1 \end{array} \right) = \left(\begin{array}{c} 2m \\ m+1 \end{array} \right) + \left(\begin{array}{c} 2m \\ m \end{array} \right) < 2^{m+1} < 2^{2m} = 4^m.$$

A última desigualdade foi utilizado o Lema 2.4.1.

Portanto da hipótese de indução temos que

$$\prod_{p\leq\ 2m+1} p = \prod_{p\leq\ m+1} p \prod_{m+1<p\leq\ 2m+1} p < 4^{m+1}4^m = 4^{2m+1}. \qquad \blacksquare$$

Teorema 2.5.1 *(O Postulado de Bertrand). Seja n um número inteiro e positivo. Então sempre existe um primo p tal que $n \leq p \leq 2n$.*

Demonstração: *Suponhamos que esta afirmação é falsa para algum valor de n e mostraremos que n não pode ser muito grande.*

Seja p_i o i-ésimo primo e α_i máximo tal que $p_i^{\alpha_i} | \left(\begin{array}{c} 2n \\ n \end{array} \right)$. Como estamos supondo que não há primos entre n e $2n$ e como nenhum primo entre $\frac{2}{3}n$ e n divide $\left(\begin{array}{c} 2n \\ n \end{array} \right)$ pelo Lema 2.5.1, temos $\left(\begin{array}{c} 2n \\ n \end{array} \right) = \prod_{p_i<\frac{2}{3}n} p_i^{\alpha_i}$. Ainda pelo Lema 2.5.1, $p_i^{\alpha_i} \leq 2n$ e $\alpha_j \leq 1$ para $p_j > \sqrt{2n}$, logo

$$\left(\begin{array}{c} 2n \\ n \end{array} \right) \leq \prod_{p_i \leq \sqrt{2n}} p_i^{\alpha_i} \prod_{\sqrt{2n} < p_j \leq \frac{2n}{3}} p_j \leq \prod_{p_i \leq \sqrt{2n}} 2n \prod_{p_j \leq \frac{2n}{3}} p_j.$$

Utilizando o lema anterior, e supondo que n *é suficientemente grande de modo que o número de primos entre* 1 *e* $\sqrt{2n}$ *é menor que* $\sqrt{\frac{n}{2}} - 1$ *(* $n = 100$ *é suficiente e a partir deste valor esta hipótese se cumpre já que metade dos números deste intervalo são pares), temos*

$$\left(\begin{array}{c} 2n \\ n \end{array} \right) < (2n)^{\sqrt{\frac{n}{2}}-1} 4^{\frac{2n}{3}}.$$

Por outra parte,

$$n \left(\begin{array}{c} 2n \\ n \end{array} \right) = n \left(\begin{array}{c} 2n-1 \\ n \end{array} \right) + n \left(\begin{array}{c} 2n-1 \\ n-1 \end{array} \right) > (1+1)^{2n-1} = 2^{2n-1}$$

e assim a desigualdade anterior implica

$$\frac{2^{2n-1}}{n} < (2n)^{\sqrt{\frac{n}{2}}-1} 4^{\frac{2n}{3}} \Rightarrow 2^{\frac{2n}{3}} < (2n)^{\sqrt{\frac{n}{2}}}.$$

Tomando logaritmo na base 2*, obtemos*

$$\frac{2\sqrt{2}}{3}\sqrt{n} < log_2 n + 1,$$

A desigualdade anterior é falso para todo $n \geq 50$*. Portanto, se existe um contra exemplo do Postulado de Bertrand, ele deve ser menor do que* 100*. Para terminar a demonstração só falta mostrar um primo que cumpra as condições do teorema para todo inteiro menor que 100 : tome*

$$p = 2 \text{ para } 1 \leq n \leq 2$$
$$p = 3 \text{ para } 3 \leq n \leq 5$$
$$p = 11 \text{ para } 6 \leq n \leq 11$$
$$p = 23 \text{ para } 12 \leq n \leq 23$$
$$p = 47 \text{ para } 24 \leq n \leq 47$$
$$p = 79 \text{ para } 48 \leq n \leq 79$$
$$p = 101 \text{ para } 80 \leq n \leq 100$$

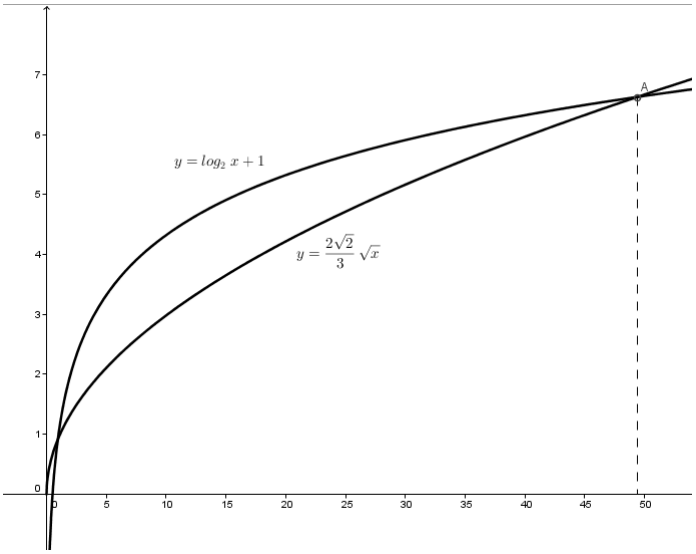

Figura 2.1: gráfico

■

Exemplo 2.5.1 *Seja $n > 2^k$. Demonstrar que os k primeiros números que são maiores que n e primos relativos com $n!$ são primos.*

Demonstração: *Como $n > 2^k$ então $n^2 > 2^k n$. Então entre dois termos consecutivos da sequência $n, 2n, 4n, ..., 2^k n$ existe ao menos um primo. Portanto, entre n e n^2 existem ao menos k primos. Em particular, os k primeiros números maiores que n que são primos relativos com $n!$ estarão entre n e n^2. Se um de tais números não for primo, digamos $l = ab$, supondo $a \leq b$. teremos que $a^2 \leq l \leq n^2$, logo $a \leq n$, o que contradiz o fato de que $n!$ e l são primos relativos.* ■

Exemplo 2.5.2 *Mostre que para o n-ésimo primo p_n vale a estimativa $p_n \leq 2^n$.*

Demonstração: *Mostraremos por indução. Se $n = 1$ verdadeiro, pois $2 = p_1 \leq 2^1$. Suponha verdadeiro para n e pelo Teorema 2.5.1 tem-se que*
$p_n \leq p_{n+1} \leq 2p_n \leq 2.2^n \Rightarrow p_{n+1} \leq 2^{n+1}$. ■

Apresentaremos a seguir uma fórmula que determina precisamente $\pi(n)$.

2.6 Fórmula de Minác

Teorema 2.6.1 *Se $n \in \mathbb{N}$ e $n \geq 2$, então*

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

Demonstração: *O somatório é para i de 2 até n. Cada vez que i for primo, a respectiva parcela será igual a 1, caso contrário será igual a zero. Então o valor do somatório será precisamente $\pi(n)$. Deve-se provar, portanto que*

$$\left\lfloor \frac{(i-1)!+1}{i} - \left\lfloor \frac{(i-1)!}{i} \right\rfloor \right\rfloor = 1 \text{ se } i \text{ é primo}$$

$$\left\lfloor \frac{(i-1)!+1}{i} - \left\lfloor \frac{(i-1)!}{i} \right\rfloor \right\rfloor = 0 \text{ se } i \text{ é composto}$$

Se i é primo então pelo Teorema de Wilson $(i-1)! \equiv -1 \ mod\ i$, isto é, $i|(i-1)!+1$, ou seja, existe q inteiro satisfazendo $(i-1)!+1 = qi$, logo,

$$\left\lfloor \frac{(i-1)!+1}{i} - \left\lfloor \frac{(i-1)!}{i} \right\rfloor \right\rfloor = \left\lfloor \frac{qi}{i} - \left\lfloor \frac{qi-1}{i} \right\rfloor \right\rfloor = \left\lfloor q - \left\lfloor q - \frac{1}{i} \right\rfloor \right\rfloor = \lfloor q - (q-1) \rfloor = 1.$$

Por outro lado, se $i > j$ e composto então

- *ou $i = ab$ com $1 < a < b < i$ e $i|1.2...a...b...(i-1)$.*
- *ou $i = p^2$ é o quadrado de um número primo ímpar e $i|1.2...p...2p...(i-1)$.*

Em qualquer caso $i|(i-1)!$, isto é, existe um q satisfazendo $(i-1)! = qi$ donde:

$$\left\lfloor \frac{(i-1)!+1}{i} - \left\lfloor \frac{(i-1)!}{i} \right\rfloor \right\rfloor = \left\lfloor \frac{qi+1}{i} - \left\lfloor \frac{qi}{i} \right\rfloor \right\rfloor = \left\lfloor q + \frac{1}{i} - q \right\rfloor = \left\lfloor \frac{1}{i} \right\rfloor = 0.$$

O caso de $i = 4$ é tratado separadamente e não oferece problema:

$$\left\lfloor \frac{3!+1}{4} - \left\lfloor \frac{3!}{4} \right\rfloor \right\rfloor = \left\lfloor \frac{3}{4} \right\rfloor = 0. \qquad \blacksquare$$

Exemplo 2.6.1 $\pi(6) = \left\lfloor \frac{1!+1}{2} - \left\lfloor \frac{1!}{2} \right\rfloor \right\rfloor + \left\lfloor \frac{2!+1}{3} - \left\lfloor \frac{2!}{3} \right\rfloor \right\rfloor + \left\lfloor \frac{3!+1}{4} - \left\lfloor \frac{3!}{4} \right\rfloor \right\rfloor +$
$+ \left\lfloor \frac{4!+1}{5} - \left\lfloor \frac{4!}{5} + \right\rfloor \right\rfloor + \left\lfloor \frac{5!+1}{6} - \left\lfloor \frac{5!}{6} \right\rfloor \right\rfloor = 1+1+0+1+0 = 3.$

Resultado que nos diz que existem três primos antes do número seis.

Na próxima seção, enunciaremos vários resultados envolvendo divisibilidade por potências de números primos e congruências de números binomiais.

2.7 Congruências e Números Binomiais

Teorema 2.7.1 *Sejam $p, m \in \mathbb{N}$ com p primo. Então:*

i) *Tem-se que $(pm)! = p^m M m!$, onde $M \in \mathbb{N}$ e $M \equiv [(p-1)!]^m \ mod\ p$.*

ii) *$E_p((mp)!) = m + E_p(m!)$.*

Demonstração: *(i): Notemos a igualdade*
$(pm)! = (pm).(pm-1).(pm-2)...(2p+1).(2p).(2p-1)...(p+1).p.(p-1)...\ 3.2.1.$
O próximo passo é organizar os múltiplos de p, logo

$$(pm)! = p.2p.3p...mp.1.2.3...(p-1).[(p+1)...(2p-1)]...[(m-1).p+1...(mp-1)].$$

$$(pm)! = p.2p.3p...mp.(p-1)!.[(p+1)...(2p-1)]...[(m-1).p+1...mp-1)].$$

$$(pm)! = p...mp.(p-1)!.[(p+1)...(p+p-1)]...[((m-1).p+1)...((m-1)p+p-1)].(*)$$

Fazendo $M = [(p+1)...(p+p-1)]...[((m-1).p+1)...((m-1)p+p-1)]$. Segue que

$$\begin{aligned} p+1 &\equiv 1 \ mod\ p \\ p+2 &\equiv 2 \ mod\ p \\ p+3 &\equiv 3 \ mod\ p \\ p+4 &\equiv 4 \ mod\ p \\ &\vdots \\ 2p-1 &\equiv p-1 \ mod\ p \\ &\vdots \\ (m-1)p+p-1 &\equiv p-1 \ mod\ p \end{aligned}$$

Portanto $M \equiv [(p-1)!]^m \ mod\ p$.

Note que em $(*)$ há m Múltiplos de p e M não há fatores de p. Restando apenas contar a maior potência de p que divide m. Portanto $E_p((mp)!) = m + E_p(m!)$. ■

Teorema 2.7.2 *Sejam $a,\ p,\ r \in \mathbb{N}$, com $a \neq 0$, p primo e $0 \leq r < p$. Então*

i) $E_p((pa+r)!) = E_p((pa)!)$;

ii) $E_p((pa-r)!) = E_p((pa)!) - 1$;

iii) $(pa+r)! \equiv r!\ mod\ p$.

Demonstração: *(i) e (iii) decorrem imediatamente da igualdade*

$$(pa+r)! = (pa)!(pa+1)...(pa+r).$$

Observando que $p \not| (pa+i)$, *para todo* $i = 1, ..., r$, *e que* $pa + i \equiv i\ mod\ p$.
(ii) Isto, por sua vez, decorre da igualdade:

$$(pa-r)!(pa-r+1)...(pa-r+r) = (pa)!.$$

Observe que a maior potência de p *que divide* $(pa-r+1)...(pa-r+r)$ *é* p. ■

Teorema 2.7.3 *Sejam* p *um número primo e* $\alpha,\ \beta,\ \in \mathbb{N}$, *com* $\alpha \geq \beta$. *Então* $p^{\alpha-\beta}$ *é a maior potência de* p *que divide* $\begin{pmatrix} p^\alpha \\ p^\beta \end{pmatrix}$.

Demonstração: *Note que* $p^\alpha = (100...000)_p$ *com* α *dígitos zeros e* $p^\beta = (100...000)_p$ *com* β *dígitos zeros. Segue que*

$$p^\alpha - p^\beta = (100...000)_p - (100...000)_p = (0.0...0.(p-1).(p-1)...(p-1).0.0...0)_p$$

com $\alpha - \beta$ *dígitos (p-1). Pelo Teorema2.2.2 temos*

$$E_p((p^\alpha)!) = \frac{p^\alpha - (0+0+0+...+0+1)}{p-1}\ ,\ E_p((p^\beta)!) = \frac{p^\beta - (0+0+0+...+0+1)}{p-1}$$

e $E_p((p^\alpha - p^\beta)!) = \dfrac{p^\alpha - p^\beta - (\alpha-\beta)(p-1)}{p-1}$. *Logo existem* $\theta_1,\ \theta_2$ *e* $\theta_3\ \in \aleph$ *tais que*

$$(p^\alpha)! = p^{(\frac{p^\alpha-1}{p-1})}.\theta_1\ \ ,\ \ (p^\beta)! = p^{(\frac{p^\beta-1}{p-1})}.\theta_2\ \ e\ (p^\alpha - p^\beta)! = p^{(\frac{p^\alpha-p^\beta-(\alpha-\beta)(p-1)}{p-1})}.\theta_3.$$

$$\begin{pmatrix} p^\alpha \\ p^\beta \end{pmatrix} = \frac{(p^\alpha)!}{(p^\beta)!.(p^\alpha - p^\beta)!} = p^{\alpha-\beta}.\theta_4,\ \ com\ \theta_4 = \frac{\theta_1}{\theta_2.\theta_3}.$$ ■

Exemplo 2.7.1 *Qual é a maior potência de 5 que divide* $\begin{pmatrix} 5^{5001} \\ 5^{4001} \end{pmatrix}$?

Solução : Pelo Teorema anterior , temos que $5^{5001-4001} = 5^{1000}$ *é a maior potência que divide* $\begin{pmatrix} 5^{5001} \\ 5^{4001} \end{pmatrix}$.

Exemplo 2.7.2 *Determinar a maior potência de* 7 *que divide* 2100! *?*

Solução: $E_7((2100)!) = E_7((300.7)!) = 300 + E_7((300)!)$ *(por (ii) do Teorema2.7.1). Segue*

$E_7((300!)) = E_7(7.42 + 6)!) = E_7((7.42)!)$ *(por (i) Teorema2.7.2).*

$E_7((7.42)!) = 42 + E_7((42)!) = 42 + E_7((6.7)!) = 42 + 6 + E_7(6!) = 48.$

Portanto $E_7((2100)!) = 300 + 48 = 348.$

Exemplo 2.7.3 *Qual é a maior potência de 7 que divide 2099! ?*

Note que$E_7((2099!)) = E_7((2100 - 1)!)) = E_7((2100!)) - 1$ *(por (ii) do Teorema*

Logo $E_7((2099)!) = 348 - 1 = 347.$

Capítulo 3

O Jogo de Wythoff

Apresentaremos a seguir uma aplicação da Função da Parte Inteira (o Jogo de Wythoff) e estabeleremos conexões com a sequência de Fibonacci e o Número Áureo. No final deste Capítulo discutiremos os Conjugados Algébricos e resolução de alguns exercícios. As bibliografias utilizadas foram: FEITOSA[2012] *e CARNEIRO*[2004].

3.1 O Jogo

Em 1907, o matemático Wythoff inventou o seguinte jogo disputado por duas pessoas:

O jogo consiste de duas pilhas de palitos, com um número arbitrário de palitos inicialmente em cada uma delas. Em sua jogada o jogador tem como opções:

i) *Retirar uma quantidade qualquer n de palitos de uma única pilha, podendo inclusive retirar todos.*

ii) *Retirar uma mesma quantidade qualquer m de palitos das duas pilhas.*

Aquele que após sua jogada deixar as duas pilhas vazias vencerá o jogo.

Denotaremos (x, y), a quantidade x de palitos na primeira pilha e y palitos da segunda pilha.

3.2 Posições Perdedoras

Uma boa estratégia para vencer o jogo é identificar as posições perdedoras. A posição (0,0) é perdedora porque uma vez que um jogador a receba, ele terá perdido o jogo.

Qualquer posição do tipo $(x,0),(0,x)$ *ou* (x,x)*, com* $x > 0$*, será uma posição vencedora. A próxima posição perdedora é* $(1,2)$ *ou* $(2,1)$*, pois*

i) *Suponha que o jogador A retire um palito da primeira pilha, logo em seguida o jogador B retira dois palitos da segunda pilha e vence o jogo.*

ii) *Suponha agora que o jogador A retire um palito da segunda pilha, logo em seguida o jogador B retira um palito de cada uma das pilhas e vence o jogo.*

iii) *Suponha agora que o jogador A retire dois palitos da segunda pilha, logo em seguida o jogador B retira um palito da primeira pilha e vence o jogo.*

Obs: os casos tratados acima foram considerando que a primeira pilha contenha, pelo menos, um palito e a segunda pilha contenha, pelo menos, dois palitos. O caso em que a primeira pilha contenha dois palitos e a segunda pilha um palito é análogo.

A partir dessa nova posição, podemos encontrar a próxima posição perdedora $(3,5)$ *ou* $(5,3)$*. Para verificar basta realizar o mesmo procedimento anterior. Como existe simetria entre duas pilhas, basta procurarmos as posições perdedoras* (x,y) *com* $x < y$*. Listaremos a seguir as primeiras posições perdedoras ordenadas* (x_n,y_n) *com* $x_n < y_n$*.*

n	0	1	2	3	4	5	6	7	8	9	10	11	12
x_n	0	1	3	4	6	8	9	11	12	14	16	17	19
y_n	0	2	5	7	10	13	15	18	20	23	26	28	31

As próximas seções nos ajudarão a estabelecer algum padrão entre os valores (x_n,y_n) *em função de n.*

3.3 Teorema de Beatty

Teorema 3.3.1 *Se* α *e* β *são irracionais positivos satisfazendo* $\frac{1}{\alpha}+\frac{1}{\beta}=1$ *então, as sequências*

$$\lfloor\alpha\rfloor,\ \lfloor 2\alpha\rfloor,\ \lfloor 3\alpha\rfloor,\ \ldots\ ;$$
$$\lfloor\beta\rfloor,\ \lfloor 2\beta\rfloor,\ \lfloor 3\beta\rfloor,\ldots\ ;$$

incluem todos os números naturais exatamente uma vez.

Obs: o Teorema de Beatty sugere uma partição dos naturais, ou seja, cada número natural pertence a uma e somente uma dentre as sequências descritas acima.

Demonstração: *Primeiramente, provemos a unicidade. Suponha que* $\lfloor k\alpha \rfloor = \lfloor l\beta \rfloor = n$, *com* $k, l \in \mathbb{N}$ *e* α , β *irracionais, implicando que*

$$\Rightarrow n < k\alpha < n+1 \, e \, n < l\beta < n+1 \Rightarrow k\alpha > n \, e \, l\beta > n \Rightarrow \alpha > \frac{n}{k} \, e \, \beta > \frac{n}{l}$$

$$\frac{1}{\alpha} < \frac{k}{n} \; e \; \frac{1}{\beta} < \frac{l}{n} \Rightarrow \frac{1}{\alpha} + \frac{1}{\beta} < \frac{k+l}{n}$$

.

Por outro lado temos $\frac{1}{\alpha} + \frac{1}{\beta} > \frac{k+l}{n+1} \Rightarrow \frac{k+l}{n+1} < \frac{1}{\alpha} + \frac{1}{\beta} < \frac{k+l}{n} \Rightarrow \frac{k+l}{n+1} < 1 < \frac{k+l}{n}$.

Temos um absurdo pois a desigualdade anterior diz que o inteiro $k+l$ *está entre dois números consecutivos. Mostremos agora que todo natural aparece nas sequências. Dado* $n \in \aleph$, *existe* $k \in \aleph$ *tal que* $\lfloor k\alpha \rfloor = n \Rightarrow n < k\alpha < n+1 \Rightarrow$
$\frac{n}{k} < \alpha < \frac{n+1}{k} \Rightarrow \frac{k}{n+1} < \frac{1}{\alpha} < \frac{k}{n}$. *Notemos que:*

$$\frac{1}{\alpha} > \frac{k}{n+1} \Rightarrow \frac{1}{\alpha} > \frac{k}{n+1} - \left[\frac{n-k+1}{n.(n+1)}\right] \Rightarrow \frac{1}{\alpha} > \frac{kn-n+k-1}{n.(n+1)} \Rightarrow$$

$$\frac{1}{\alpha} > \frac{n.(k-1)+k-1}{n.(n+1)} \Rightarrow \frac{1}{\alpha} > \frac{(k-1).(n+1)}{n.(n+1)} \Rightarrow \frac{1}{\alpha} > \frac{k-1}{n} \Rightarrow \frac{k-1}{n} < \frac{1}{\alpha} < \frac{k}{n}.$$

Dividamos o intervalo $\left[\frac{k}{n+1}, \frac{k}{n}\right]$ *em duas partes. Se* $\frac{k-1}{n} < \frac{1}{\alpha} < \frac{k}{n}$, *temos* $\lfloor k\alpha \rfloor = n$. *Se por outro lado,* $\frac{k-1}{n} < \frac{1}{\alpha} < \frac{k}{n+1}$, *temos:*

$$\frac{k-1}{n} < 1 - \frac{1}{\beta} < \frac{k}{n+1} \Rightarrow \frac{n+1-k}{n+1} < \frac{1}{\beta} < \frac{n+1-k}{n} \Rightarrow \frac{n}{n+1-k} < \beta < \frac{n+1}{n+1-k} \Rightarrow$$

$n < \beta.(n+1-k) < n+1 \Rightarrow \lfloor (n+1-k)\beta \rfloor = n$.

Em qualquer caso, n faz parte da sequência. ■

Lema 3.3.1 *As sequências* $\{\lfloor n\alpha \rfloor, n \in \mathbb{N}\}$ *e* $\{\lfloor n\beta \rfloor, n \in \mathbb{N}\}$, *são estritamente crescentes, ou seja :* $m > n \Rightarrow \lfloor m\alpha \rfloor > \lfloor n\alpha \rfloor$ *não podendo ocorrer a igualdade.*

Demonstração: $\lfloor (n+1)\alpha \rfloor = \lfloor n\alpha + \alpha \rfloor$ *pelo Teorema 2.1.1 (iii)* $\Rightarrow \lfloor n\alpha + \alpha \rfloor \geq \lfloor n\alpha \rfloor + \lfloor \alpha \rfloor \geq \lfloor n\alpha \rfloor + 1 > \lfloor n\alpha \rfloor$, *o mesmo vale também para* β. ■

Obs: Os irracionais escolhidos são ambos maiores que 1, *mas não podem ser ambos maiores que* 2, *já que a soma de seus inversos é 1. Suponha então, sem perda de generalidade que* $1 < \alpha < 2$, *logo* $\lfloor \alpha \rfloor = 1$.

3.4 Procurando algum padrão

De acordo com a tabela, temos:

$$\begin{array}{ll} \dfrac{y_1}{x_1} = \dfrac{2}{1} = 2 & \dfrac{y_2}{x_2} = \dfrac{5}{3} \cong 1,666 \\ \dfrac{y_3}{x_3} = \dfrac{7}{4} = 1,75 & \dfrac{y_4}{x_4} = \dfrac{10}{6} \cong 1,666 \\ \dfrac{y_5}{x_5} = \dfrac{13}{8} = 1,625 & \dfrac{y_6}{x_6} = \dfrac{15}{9} \cong 1,666 \\ \dfrac{y_7}{x_7} = \dfrac{18}{11} \cong 1,636 & \dfrac{y_8}{x_8} = \dfrac{20}{12} \cong 1,666 \\ \dfrac{y_9}{x_9} = \dfrac{23}{14} \cong 1,642 & \dfrac{y_{10}}{x_{10}} = \dfrac{26}{16} = 1,625 \\ \vdots & \vdots \end{array}$$

Notemos que o quociente $\dfrac{y_n}{x_n}$ *se aproxima de* $1,6$*, logo a inserção dos pontos* (x_n, y_n) *em um gráfico sugere que esses pontos estão próximos de uma reta. Um irracional que se aproxima dessa regularidade é* $\dfrac{1+\sqrt{5}}{2} \cong 1,618$*. Usaremos a seguir o Teorema de Beatty. Se* $\alpha = \dfrac{1+\sqrt{5}}{2} \Rightarrow \dfrac{1}{\frac{1+\sqrt{5}}{2}} + \dfrac{1}{\beta} = 1 \Rightarrow \beta = \dfrac{3+\sqrt{5}}{2}$*. Observe as sequências:*

1) $\left\lfloor \dfrac{1+\sqrt{5}}{2} \right\rfloor, \left\lfloor 2.\left(\dfrac{1+\sqrt{5}}{2}\right) \right\rfloor, \left\lfloor 3.\left(\dfrac{1+\sqrt{5}}{2}\right) \right\rfloor, \left\lfloor 4.\left(\dfrac{1+\sqrt{5}}{2}\right) \right\rfloor, \left\lfloor 5.\left(\dfrac{1+\sqrt{5}}{2}\right) \right\rfloor, \ldots$

2) $\left\lfloor \dfrac{3+\sqrt{5}}{2} \right\rfloor, \left\lfloor 2.\left(\dfrac{3+\sqrt{5}}{2}\right) \right\rfloor, \left\lfloor 3.\left(\dfrac{3+\sqrt{5}}{2}\right) \right\rfloor, \left\lfloor 4.\left(\dfrac{3+\sqrt{5}}{2}\right) \right\rfloor, \left\lfloor 5.\left(\dfrac{3+\sqrt{5}}{2}\right) \right\rfloor, \ldots$

Realizando os cálculos teremos:

1)1, 3, 4, 6, 8, 9, 11, 12, 14, 16, 17, 19, ...

2)2, 5, 7, 10, 13, 15, 18, 20, 23, 26, 28, 31, ...

Esses fatos nos leva a conjecturar:
Se $\alpha = \dfrac{1+\sqrt{5}}{2}$*, então as posições perdedoras são dadas por:*

$$(x_n, y_n) = \left(\left\lfloor n.\left(\frac{1+\sqrt{5}}{2}\right) \right\rfloor, \left\lfloor n.\left(\frac{3+\sqrt{5}}{2}\right) \right\rfloor \right).$$

Notemos $\alpha = \dfrac{1+\sqrt{5}}{2}$ *é a raiz da equação* $\alpha^2 - \alpha - 1 = 0$ *e* $\beta = \alpha^2 = \alpha + 1$.

Lema 3.4.1 *Se* $x_n = \lfloor \alpha.n \rfloor$ *e* $y_n = \lfloor \beta.n \rfloor$ *então* $y_n = x_n + n$.

Demonstração: *Temos que* $\beta = \alpha + 1 \Rightarrow y_n = \lfloor (\alpha+1).n \rfloor = \lfloor \alpha.n + n \rfloor$ *segue pelo Teorema 2.1.1 (ii)* $y_n = \lfloor \alpha.n + n \rfloor = \lfloor \alpha.n \rfloor + n = x_n + n$. ■

Obs: $y_{n+1} = \lfloor(\alpha+1).(n+1)\rfloor = \lfloor\alpha.n+\alpha+n+1\rfloor = \lfloor\alpha.(n+1)+n+1\rfloor = \lfloor\alpha.(n+1)\rfloor+(n+1) = x_{n+1}+(n+1)$.

Teorema 3.4.1 *Se* $\alpha = \dfrac{1+\sqrt{5}}{2}$, *então as posições perdedoras do jogo de Wythoff é dado por:*

$(x_n, y_n) = \left(\left\lfloor n.\left(\dfrac{1+\sqrt{5}}{2}\right)\right\rfloor, \left\lfloor n.\left(\dfrac{3+\sqrt{5}}{2}\right)\right\rfloor\right)$.

Demonstração: *Provemos a afirmação por indução. Ela é facilmente verificável para os casos iniciais apresentados na tabela. Suponha sua validade para todos os inteiros no conjunto* $0, 1, 2, 3, ..., k$. *Provaremos também que é válido para* $k+1$. *Temos pelo Lema 3.3.1 que* x_n *e* y_n *são crescentes e* $x_n < y_n$ *logo a componente* x_{k+1} *da posição perdedora é o menor inteiro não negativo que ainda não apareceu nas situações* (x_i, y_i) *com* $i = 0, 1, 2, 3, ..., k$ *pelo que foi demonstrado no Teorema de Beatty. Segue pelo Lema 3.4.1 que*

$y_n = x_n + n \Rightarrow y_{n+1} = x_{n+1} + (n+1)$. *O que completa a demonstração.* ■

Observe então que todo natural aparecerá uma única vez em uma posição perdedora.

Teorema 3.4.2 *(Teorema Final)*

i) *Qualquer jogada transforma uma posição perdedora em uma posição não-perdedora.*

ii) *Existe uma jogada conveniente que transforma uma posição não-perdedora em uma posição perdedora.*

Demonstração: *i)*(x_n, y_n) *é uma posição perdedora, é claro que* $(x_n - t, y_n)$ *ou* $(x_n, y_n - t)$ *com* $t \in \mathbb{Z}_+$ *são não-perdedoras e caso* $(x_n - t, y_n - t)$ *fosse posição perdedora, digamos* (x_k, y_k) *pelo Lema 3.4.1* $\Rightarrow y_k = x_k + k \Rightarrow y_k - x_k = k$ *por outro lado*

$y_n = x_n + n \Rightarrow y_n - t = x_n - t + n \Rightarrow y_k = x_k + n \Rightarrow y_k - x_k = n = k$. *Absurdo.*

ii) Considere uma posição não-perdedora, se for da forma (m, m), $m > 0$, *é óbvio que* $(m-m, m-m) = (0, 0)$.

Suponha agora (m, k), *com* $m < k$ *não-perdedora.*

1^0 *caso:* $m = x_n$ *e* $k > y_n = x_n + n$. *Neste caso tome* t *tal que*

$k = y_n + t \Rightarrow k$ *-*$t = y_n$.

2^0 *caso:* $m = x_n$ *e* $k < y_n = x_n + n$. *Nesse caso* $k < x_n + n \Rightarrow k < m + n$ *e como* $k > m$ *temos* $k - m < m - m + n \Rightarrow k - m < n$. *Seja* $l = k - m$ *e* $t = x_n - x_l$ *façamos a jogada* $(m-t, k-t) = (x_n - (x_n - x_l), k - (m - x_l)) = (x_l, k - m + x_l) = (x_l, l + x_l) = (x_l, y_l)$.

3^0 *caso:* $m = y_n$. *seja* $t = k - x_n$ *(note* $x_n < y_n = m < k$*). Faça a jogada* $(m, k - t) = (m, x_n) = (y_n, x_n)$. ■

Na próxima seção apresentaremos uma relação entre o jogo de Wythoff e a sequência de Fibonacci.

3.5 Sequência de Fibonacci

A sequência de Fibonacci é definida por $F_n = F_{n-1} + F_{n-2}$, *com* $F_1 = F_2 = 1$. *Logo os termos da sequência de Fibonacci são:*
1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144,...

Proposição 3.5.1 *Para todo* $n \in \mathbb{N}^*$, *tem-se que* $F_n = \frac{1}{\sqrt{5}} \cdot \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right)$.

Demonstração: *A equação característica é* $r^2 = r + 1$. *As raízes da equação característica são* $\frac{1 \pm \sqrt{5}}{2}$. *Então*

$$F_n = C_1.(\frac{1+\sqrt{5}}{2})^n + C_2.(\frac{1-\sqrt{5}}{2})^n$$

Para determinar C_1 *e* C_2 *basta usar* $F_1 = F_2 = 1$. *Obtemos o sistema*

$$\begin{cases} C_1 + C_2 = 1 \\ C_1.(\frac{1+\sqrt{5}}{2}) + C_2.(\frac{1-\sqrt{5}}{2}) = 1 \end{cases}$$

Resolvendo-o obtemos $C_1 = \frac{1+\sqrt{5}}{2\sqrt{5}}$ *e* $C_2 = \frac{1-\sqrt{5}}{2\sqrt{5}}$.
Logo,
$F_n = \frac{1}{\sqrt{5}}.(\frac{1+\sqrt{5}}{2})^n - \frac{1}{\sqrt{5}}.(\frac{1-\sqrt{5}}{2})^n$. ■

Se organizarmos a sequência de Fibonacci da seguinte forma:
$(F_2, F_3), (F_4, F_5), (F_6, F_7), (F_8, F_9), ..., (F_{2n}, F_{2n+1}), ...$ *Então teremos:*

$$(1, 2), (3, 5), (8, 13), (21, 34), (55, 89), ...$$

Notemos que são as posições perdedoras do jogo de Wythoff.

Teorema 3.5.1 *Se (F_{2n}, F_{2n+1}) são termos consecutivos da sequência de Fibonacci então este par forma uma posição perdedora no Jogo de Wythoff.*

Demonstração: *Provemos a afirmação por indução. Ela é facilmente verificável para os casos iniciais apresentados na tabela. Suponha verdadeiro para (F_{2n}, F_{2n+1}) logo teremos $(F_{2n}, F_{2n+1}) = (x_k, y_k)$ segue pelo Lema 3.4.1*

$$y_k = x_k + k \Rightarrow F_{2n+1} = F_{2n} + k$$

Pelo Teorema de Beatty temos F_{2n+2} pertence em algum momento ás posicões perdedoras, tome $x_t = F_{2n+2}$ e $t = F_{2n+1}$.

$$F_{2n+1} + F_{2n} = F_{2n} + F_{2n} + k \;\Rightarrow\; F_{2n+2} = F_{2n+1} + F_{2n} \Rightarrow$$
$$F_{2n+2} + F_{2n+1} = F_{2n+1} + F_{2n+1} + F_{2n} \;\Rightarrow\; F_{2n+3} = F_{2n+2} + F_{2n+1} \Rightarrow$$
$$F_{2n+3} = x_t + t \;\Rightarrow\; (F_{2n+2}, F_{2n+3}) \text{ é uma posição perdedora.}$$

■

Como calcular $\lfloor \alpha^n \rfloor \bmod m$, sendo α irracional. A próxima seção apresentará alguns resultados envolvendo conjugados algébricos.

3.6 Conjugados Algébricos

Suponha que α seja um irracional e que estamos interessados em calcular o resto de $\lfloor \alpha^n \rfloor \bmod m$. Nesse caso, tentaremos encontrar β tal que $0 < \beta < 1$, $\alpha + \beta$ e $\alpha\beta \in \mathbb{Z}$. Para entendermos o propósito disso, considere a equação: $x^2 - ax - b = 0$ onde $\alpha + \beta = a$, $\alpha\beta = b$ e $k_n = \alpha^n + \beta^n$. Como α e β são raízes:

$$\alpha^2 - a\alpha - b = 0 \Rightarrow \alpha^2 = a\alpha + b \Rightarrow \alpha^{n+2} = a\alpha^{n+1} + b\alpha^n$$
$$\beta^2 - a\beta - b = 0 \Rightarrow \beta^2 = a\beta + b \Rightarrow \beta^{n+2} = a\beta^{n+1} + b\beta^n$$

Segue que $\alpha^{n+2} + \beta^{n+2} = a(\alpha^{n+1} + \beta^{n+1}) + b(\alpha^n + \beta^n) \Rightarrow$
$k_{n+2} = ak_{n+1} + bk_n$. Como a e b são inteiros e $k_0 = \alpha^0 + \beta^0 = 2 \in \mathbb{Z}$, $k_1 = \alpha^1 + \beta^1 = a \in \mathbb{Z}$, segue $k_n \in \mathbb{Z}$ para todo natural n. Além disso, $k_n \in \mathbb{Z} \Rightarrow \lfloor \alpha^n \rfloor + \{\alpha^n\} + \lfloor \beta^n \rfloor + \{\beta^n\} \in \mathbb{Z}$

consequentemente $\{\alpha^n\}+\{\beta^n\} \in \mathbb{Z}$ *como* $0 < \{\alpha^n\}+\{\beta^n\} < 2$, *devemos obrigatoriamente ter* $\{\alpha^n\} + \{\beta^n\} = 1$. *Usando que* $0 < \beta < 1$, *também podemos concluir que* $\lfloor \beta^n \rfloor = 0 \Rightarrow k_n = \lfloor \alpha^n \rfloor + 1$. *Conhecendo* k_n, *podemos facilmente determinar o período dos restos dos termos da sequência na divisão por* m.

Exemplo 3.6.1 *Prove que* $\forall n \in \mathbb{N}$ *temos* $3 | \left\lfloor \left(\frac{7+\sqrt{37}}{2} \right)^n \right\rfloor$.

Solução:

Sejam $\alpha = \frac{7+\sqrt{37}}{2}$ *e* $\beta = \frac{7-\sqrt{37}}{2}$. *Temos que :*

$\alpha + \beta = \frac{7+7}{2} = 7$ *e* $\alpha \cdot \beta = \frac{7^2-37}{4} = 3$

α *e* β *são raízes da equação* $x^2 - 7x + 3 = 0 \Rightarrow x^2 - 7x - (-3) = 0$

$k_n = \alpha^n + \beta^n$, $k_0 = 2$ *e* $k_1 = 7$

$k_{n+2} = ak_{n+1} + bk_n \ \forall n \geq 0$

$k_{n+2} = 7k_{n+1} - 3k_n \Rightarrow k_{n+2} \equiv 7k_{n+1} - 3k_n \ (mod\ 3) \Rightarrow k_{n+2} \equiv k_{n+1} \ (mod\ 3)$

Como $k_1 \equiv 7 \equiv 1\ mod\ 3 \Rightarrow k_n \equiv 1\ mod\ 3\ \forall n \geq 1$ *segue que*

$k_n - 1 \equiv 0 \ (mod\ 3) \Rightarrow \lfloor \alpha^n \rfloor = k_n - 1 \equiv\ 0 \ (mod\ 3)$.

3.7 Exemplos

1) A parte inteira de um número real x *é o maior inteiro que é menor do que ou igual a* x. *Denotamos as parte inteira de* x *por* $\lfloor x \rfloor$. *Calcule as partes inteiras seguintas.*

a) $\left\lfloor \sqrt{12} \right\rfloor =$

b) $\left\lfloor \frac{28756}{12777} \right\rfloor =$

c) $\left\lfloor -\frac{2007}{2008} \right\rfloor =$

d) $\lfloor \sqrt[3]{-111} \rfloor =$

Solução:

a) Os números 9 e 16 são quadrados perfeitos e $9 < 12 < 16$. *Então,*

$3 = \sqrt{9} < \sqrt{12} < \sqrt{16} = 4$ *e, portanto,* $\left\lfloor \sqrt{12} \right\rfloor = 3$.

b) Como $12777.2 < 28756 < 12777.3$, *temos* $2 < \dfrac{28756}{12777} < 3$, *portanto,* $\left\lfloor \dfrac{28756}{12777} \right\rfloor = 2$.

c) Como $2007 < 2008$, *temos* $0 < \dfrac{2007}{2008} < 1$, *ou* $-1 < -\dfrac{2007}{2008} < 0$, *portanto* $\left\lfloor -\dfrac{2007}{2008} \right\rfloor = -1$.

d) Como $4^3 = 64 < 111 < 125 = 5^3$, *temos* $(-5)^3 = -5^3 = -125 < -111 < -4^3 = (-4)^3$, *Logo* $\lfloor \sqrt[3]{-111} \rfloor$ = - *5.*

2) Calcule o valor da soma $\left\lfloor \sqrt[4]{1} \right\rfloor + \left\lfloor \sqrt[4]{2} \right\rfloor + \left\lfloor \sqrt[4]{3} \right\rfloor + \left\lfloor \sqrt[4]{4} \right\rfloor + ... + \left\lfloor \sqrt[4]{2008} \right\rfloor$.

Solução:

Observe que para $i \geq 1$ *temos*
$\lfloor \sqrt[4]{n} \rfloor = i \Leftrightarrow i \leq \sqrt[4]{n} < i + 1 \Leftrightarrow i^4 \leq n < (i+1)^4$ *e assim há* $(i+1)^4 - i^4$ *números n tais que* $\lfloor \sqrt[4]{n} \rfloor = i$. *Portanto a soma pedida é*
$1.(2^4 - 1^4) + 2.(3^4 - 2^4) + 3.(4^4 - 3^4) + 4.(5^4 - 4^4) + 5.(6^4 - 5^4) + 6.(2008 - 6^4) + 6 = 9779.$

3)(OBM 1999) Prove que há pelo menos um algarismo diferente de zero entre a 1000.000^a *e a* 3000.000^a *casa decimal de* $\sqrt{2}$ *após a vírgula.*

Solução:

Suponhamos, por absurdo, que todos os algarismos das casas decimais entre a 1000.000^a *casa e a* 3000.000^a *casa decimal de* $\sqrt{2}$ *fossem zero, então:*

$10^{2.10^6} \left\lfloor 10^{10^6} \sqrt{2} \right\rfloor = \left\lfloor 10^{3.10^6} \sqrt{2} \right\rfloor$. *Se* $k = \left\lfloor 10^{10^6} \sqrt{2} \right\rfloor$, *temos:*

$$10^{2.10^6} k \leq 10^{3.10^6} \sqrt{2} < 10^{2.10^6} k + 1$$

mas como $10^{2.10^6}.k \neq 10^{3.10^6} \sqrt{2}$, *(pois se não fosse teríamos* $\sqrt{2} = \dfrac{K}{10^{10^6}}$, *um absurdo, pois* $\sqrt{2}$ *é irracional) então:*

$$\frac{k}{10^{10^6}} < \sqrt{2} < \frac{k}{10^{10^6}} + \frac{1}{10^{3.10^6}} \Rightarrow$$

$$\frac{k^2}{10^{2.10^6}} < 2 < \frac{k^2}{10^{2.10^6}} + \frac{2k}{10^{4.10^6}} + \frac{1}{10^{6.10^6}} \Rightarrow$$

$$k^2 < 2.10^{2.10^6} < k^2 + \frac{2k}{10^{2.10^6}} + \frac{1}{10^{4.10^6}},$$

mas como $K = \left\lfloor 10^{10^6}\sqrt{2} \right\rfloor \in \mathbb{Z}$.

4)Mostre que $\lfloor x+y \rfloor + \lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor 2x \rfloor + \lfloor 2y \rfloor$,*com* $x, y \in \mathbb{R}$.

Solução:

$x = k + \alpha$, *com* $k = \lfloor x \rfloor$ *e* $\alpha = \{x\}$

$y = r + \beta$, *com* $r = \lfloor y \rfloor$ *e* $\beta = \{y\}$

$x + y = k + r + \alpha + \beta \Rightarrow \lfloor x+y \rfloor = k + r + \lfloor \alpha + \beta \rfloor \Rightarrow$

$\lfloor x+y \rfloor + \lfloor x \rfloor + \lfloor y \rfloor = 2k + 2r + \lfloor \alpha + \beta \rfloor$ $(*)$ *por outro lado*

$2x = 2k + 2\alpha \Rightarrow \lfloor 2x \rfloor = 2k + \lfloor 2\alpha \rfloor$

$2y = 2r + 2\alpha \Rightarrow \lfloor 2y \rfloor = 2r + \lfloor 2\beta \rfloor$

segue $\lfloor 2x \rfloor + \lfloor 2y \rfloor = 2k + 2r + \lfloor 2\alpha \rfloor + \lfloor 2\beta \rfloor$ *comparando com* $(*)$ *basta provar que*

$\lfloor \alpha + \beta \rfloor \leq \lfloor 2\alpha \rfloor + \lfloor 2\beta \rfloor$. *Note que*

Se $\alpha + \beta < 1 \Rightarrow \lfloor \alpha + \beta \rfloor = 0 \leq \lfloor 2\alpha \rfloor + \lfloor 2\beta \rfloor$

Se $\alpha + \beta \geq 1 \Rightarrow \alpha \geq \frac{1}{2}$ *ou* $\beta \geq \frac{1}{2} \Rightarrow 2\alpha \geq 1$ *ou* $2\beta \geq 1 \Rightarrow \lfloor 2\alpha \rfloor = 1$

ou $\lfloor 2\beta \rfloor = 1 \Rightarrow \lfloor 2\alpha \rfloor + \lfloor 2\beta \rfloor \geq 1 = \lfloor \alpha + \beta \rfloor$ *(pois* $\alpha + \beta < 2$*).*

5) Mostre que se m e n são inteiros positivos, então $\dfrac{(2m)!(2n)!}{(m)!(n)!(m+n)!}$ *é um inteiro.*

Solução:

Seja p primo e a maior potência de p que divide o numerador é $\sum_{j=1}^{\infty}\left\lfloor\frac{2m}{p^j}\right\rfloor+\sum_{j=1}^{\infty}\left\lfloor\frac{2n}{p^j}\right\rfloor=\sum_{j=1}^{\infty}(\left\lfloor\frac{2m}{p^j}\right\rfloor+\left\lfloor\frac{2n}{p^j}\right\rfloor)$ *e a maior potência de p que divide o denominador é* $\sum_{j=1}^{\infty}(\left\lfloor\frac{m}{p^j}\right\rfloor+\left\lfloor\frac{n}{p^j}\right\rfloor+\left\lfloor\frac{m+n}{p^j}\right\rfloor)$ *pelo exercício anterior com* $x=\dfrac{m}{p^j}$ *e* $y=\dfrac{n}{p^j}$ *temos*

$$\left\lfloor\frac{m}{p^j}+\frac{n}{p^j}\right\rfloor+\left\lfloor\frac{m}{p^j}\right\rfloor+\left\lfloor\frac{n}{p^j}\right\rfloor\leq\left\lfloor\frac{2m}{p^j}\right\rfloor+\left\lfloor\frac{2n}{p^j}\right\rfloor$$

6)(Romênia). Seja n um natural cuja representação binária tem exatamente k algarismos 1. Prove que 2^{n-k} divide $n!$.

Solução:

Seja $n=(\underbrace{111...1}_{k})_2$. *Segue* $E_p(n!)=\dfrac{n-(n_0+n_1+n_2+n_3+...+n_r)}{p-1}$ *segue* $E_2(n!)=\dfrac{n-k}{2-1}=n-k$. *Portanto a maior potência de 2 que divide $n!$ é $n-k$.*

7) Calcule:

a) A maior potência de 104 que divide 10000!

b) A maior potência de 13 que divide 130000!

c) A maior potência de 13 que divide 130010!

d) A maior potência de 13 que divide 129990!

Solução:

a)Temos que $104=2^3.13$. *Segue*

$$E_2(10000!)=\left\lfloor\frac{10000}{2}\right\rfloor+\left\lfloor\frac{10000}{4}\right\rfloor+\left\lfloor\frac{10000}{8}\right\rfloor+\left\lfloor\frac{10000}{32}\right\rfloor+...+\left\lfloor\frac{10000}{512}\right\rfloor$$

$$E_2(10000!)=5000+2500+1250+625+...+4+2+1=9995$$

$$E_{13}(10000!) = \left\lfloor \frac{10000}{13} \right\rfloor + \left\lfloor \frac{10000}{169} \right\rfloor + \left\lfloor \frac{10000}{2197} \right\rfloor = 796 + 59 + 4 = 832$$

Logo $104! = 2^{9995}.13^{832}.\alpha$ *com* $\alpha \in \mathbb{Z}$

$104! = 2^{2496}.13^{832}.\alpha.2^{7499} \Rightarrow$

$$104! = \underbrace{2^3.13.2^3.13.2^3.13...2^3.13}_{832}.\alpha.2^{7499} = 104^{832}.\alpha.2^{7499}$$

b) Note que $E_{13}(130000)! = E_{13}(13.10000)! = 10000 + E_{13}(10000)! =$
$10000 + 832 = 10832$

c) $E_{13}(130010)! = E_{13}(130000 + 10)! = E_{13}(10000)! =$
$10000 + 832 = 10832$

d) $E_{13}(129990)! = E_{13}(130000 - 10)! = E_{13}(10000)! - 1 =$
$10000 + 832 - 1 = 10831$

8) Mostre que $(729^{50})! = 27^{50}.(27^{50})!.(729^{50} - 27^{50})!.\alpha$ *com* $\alpha \in \mathbb{Z}$.

$$\begin{pmatrix} 729^{50} \\ 27^{50} \end{pmatrix} = \begin{pmatrix} 3^{300} \\ 3^{150} \end{pmatrix} = 3^{150}.\alpha$$

Por outro lado $\begin{pmatrix} 3^{300} \\ 3^{150} \end{pmatrix} = \dfrac{(3^{300})!}{(3^{150})!(3^{300} - 3^{150})!} = 3^{150}.\alpha \Rightarrow$

$(3^{300})! = 3^{150}.(3^{150})!.(3^{300} - 3^{150})!\alpha \Rightarrow (729^{50})! = 27^{50}.(27^{50})!.(729^{50} - 27^{50})!\alpha.$

9)(Teste de Seleção do Brasil para a Cone Sul) Prove que para todo inteiro positivo k*, a parte inteira do número* $(7 + 4\sqrt{3})^k$ *é ímpar.*

Solução:

Sejam $\alpha = 7 + 4\sqrt{3}$ *e* $\beta = 7 - 4\sqrt{3}$*. Temos que :*

$\alpha + \beta = 14$ *e* $\alpha\beta = 1$ *logo*

α *e* β *são raízes da equação* $x^2 - 14x + 1 = 0 \Rightarrow x^2 - 14x - (-1) = 0$ *e*
$k_n = \alpha^n + \beta^n$, $k_0 = 2$ *e* $k_1 = 14 \Rightarrow$

$k_{n+2} = ak_{n+1} + bk_n \ \forall n \geq 0$

$k_{n+2} = 14k_{n+1} - k_n \Rightarrow k_{n+2} \equiv 14k_{n+1} - k_n \ (mod\ 2) \Rightarrow k_{n+2} \equiv k_n \ (mod\ 2)$

Como $k_1 \equiv 14 \equiv 0\ mod\ 2 \Rightarrow k_n \equiv 0\ mod\ 2\ \forall n \geq 1$ *segue*

$k_n - 1 \equiv -1\ (mod\ 2)$ *e* $-1 \equiv 1\ mod\ 2 \Rightarrow k_n - 1 \equiv 1\ mod\ 2 \Rightarrow$
$\lfloor \alpha^n \rfloor = k_n - 1 \equiv\ 1\ (mod\ 2)$.

10) Mostre que $n!2^n3^n$ *divide* $(3n)!$.

Solução:
$E_3((3n)!) = n + E_3(n!) \Rightarrow 3^{n+E_3(n!)} = 3^n.3^{E_3(n!)} | (3n)!$

$E_2((2n)!) = n + E_2(n!) \Rightarrow 2^{n+E_2(n!)} = 2^n.2^{E_2(n!)} | (3n)!$

Segue que existem $\alpha, \beta \in \mathbb{N}$ *tais que* $(3n)! = 2^n.3^n.2^{E_2(n!)}.3^{E_3(n!)}.\alpha \Rightarrow$

$(3n)! = 2^n.3^n.n!.\beta \Rightarrow 2^n3^nn! | (3n)!$.

11)(OBMEP 2014) O símbolo $n!$ *é usado para representar o produto dos números naturais de* 1 *até* n*, isto é,* $n! = n.(n-1).(n-2)...2.1$*. Por exemplo,* $4! = 4.3.2.1 = 24$*. Se* $n! = 2^{15}.3^6.5^3.7^2.11.13$*, qual é o valor de* n*?*

Solução:
Temos $E_p(n!) = \dfrac{n - (n_0 + n_1 + n_2 + ... + n_r)}{p-1} \Rightarrow E_2(n!) = \dfrac{n - (n_0 + n_1 + n_2 + ... + n_r)}{2-1}$,
segue
$15 + (n_0 + n_1 + n_2 + ... + n_r) = n$.
Note $E_2(16!) = \left\lfloor \dfrac{16}{2} \right\rfloor + \left\lfloor \dfrac{16}{4} \right\rfloor + \left\lfloor \dfrac{16}{8} \right\rfloor + \left\lfloor \dfrac{16}{16} \right\rfloor = 8 + 4 + 2 + 1 = 15.$

$$E_3(16!) = \left\lfloor \frac{16}{3} \right\rfloor + \left\lfloor \frac{16}{9} \right\rfloor = 5 + 1 = 6.$$

$$E_5(16!) = \left\lfloor \frac{16}{5} \right\rfloor = 3.$$

$$E_7(16!) = \left\lfloor \frac{16}{7} \right\rfloor = 2.$$

$$E_{11}(16!) = \left\lfloor \frac{16}{11} \right\rfloor = 1.$$

$$E_{13}(16!) = \left\lfloor \frac{16}{13} \right\rfloor = 1.$$

Portanto $n = 16$.

Considerações finais

.

Neste Trabalho apresentamos algumas aplicações da Função Parte Inteira:

- *Como decompor em fatores primos um número* $n!$.
- *Estimamos em ordem de grandeza a quantidade de primos menores ou iguais a um número real positivo.*
- *Formulação matemática do Jogo de Wythoff.*

Para decompor $n!$ *em fatores primos utilizamos a fórmula de Legendre e uma outra expressão em função da representação p-ádica do número n escrito na base p. Algumas propriedades acerca do* $E_p(n!)$ *foram exploradas para facilitar os calculos. O Teorema de Kummer é uma ferramenta indispensável na resolução de problemas envolvendo divisilidade e binomial. O Teorema de Chebyshev é um resultado básico sobre a distribuição dos números primos e portanto hoje temos condição de estimar quantos primos há em um intervalo.*

O Jogo de Wythoff foi apresentado na intenção de transformar as aulas de matemática em momentos estimulantes onde os alunos e professores possam interagir num ambiente propocio às discussões que facilite na tomada de decisões e resoluções em diversas situações problemas.

Atualmente trabalho na Escola Estadual Dunga Rodrigues em Várzea Grande, com turmas do ensino fundamental (6^0 *Ano e* 7^0 *Ano) e turmas do ensino médio (*1^0 *Ano,* 2^0 *Ano e* 3^0 *Ano). Em todas as turmas apresentei o jogo de Wythoff e em geral eles reagiram de maneira positiva, manipulando exaustivamente o jogo. A curiosidade maior foi na obtenção de algum padrão para as posições perdedoras do jogo em função de n (n número natural) e na conexão dessas posições com o algoritmo que resolve o jogo.*

Para atender ao objetivo do PROFMAT que é a formação matemática aprofundada, relevante e articulada com o exercício da docência no ensino básico, este trabalho contemplará o Professor através da fundamentação téorica, oportunizando ao mesmo aprofundar seus conhecimentos em Aritmética e o aluno através de resolução de vários problemas presentes na OBM e OBMEP. Portanto há uma tentativa de mudança da prática didática do Professor em sala de aula.

Referências Bibliográficas

[1] *HEFEZ, Abramo. Elementos da Aritmética. Textos Universitários. Sociedade Brasileira de Matemática. 2ª edição. Rio de Janeiro-RJ. 2011.*

[2] *SANTOS, José Plínio de Oliveira. Introdução à Teoria dos Números. Coleção Matemática Universitária. Instituto de Matemática Pura e Aplicada. 1998.*

[3] *MUNIZ NETO, Antonio Caminha. Tópicos de Matemática Elementar. Volume 5. Teoria dos Números. Coleção Professor de Matemática, SBM. Rio de Janeiro - 2012.*

[4] *RIBENBOIM, P.(2012). Números Primos: Velhos Mistérios e Novos Recordes.Coleção Matemática Universitária. 1 ed. Rio de Janeiro: IMPA-2012.*

[5] *MARTINEZ,Fabio B. MOREIRA, Carlos G. SALDANHA, Nicolau. TENGAN, Edurado.Teoria dos Números: , Um passeio com primos e outros números familiares pelo mundo inteiro.Projeto Euclides. IMPA, Rio de Janeiro - 2011.*

[6] *FEITOSA, S. Notas do Curso de Teoria dos Números-nível 2. Disponível no Site: http://www.poti.impa.br/material didático.*

[7] *CARNEIRO, E.(2004). O Teorema de Beatty e o Jogo de Wythoff,Jornada de Matemática da Bahia. Salvador - 2004.*