Universidade Federal do Espírito Santo
Centro Universitário Norte do Espírito Santo
Colegiado do Curso de Matemática Licenciatura

Uilton Pereira Paiva

Funções Aritméticas e Lei da Reciprocidade Quadrática de Gauss

São Mateus
2014

Uilton Pereira Paiva

Funções Aritméticas e Lei da Reciprocidade Quadrática de Gauss

Trabalho submetido ao Colegiado do Curso de Matemática Licenciatura do CEUNES/UFES, como requisito parcial para a obtenção do grau de Licenciado em Matemática.

Orientador:

Prof. Michel Guimarães Coswosck

São Mateus

2014

Uilton Pereira Paiva

Funções Aritméticas e Lei da Reciprocidade Quadrática de Gauss

Trabalho submetido ao Colegiado do Curso de Matemática Licenciatura do CEUNES/UFES, como requisito parcial para a obtenção do grau de Licenciado em Matemática.

Aprovada em 06 de Agosto de 2014.

Comissão Examinadora

Prof. Michel Guimarães Coswosck
Universidade Federal do Espírito Santo
Orientador

Prof. Lúcio Souza Fassarella
Universidade Federal do Espírito Santo

Prof. Paulo Wander Barbosa
Universidade Federal do Espírito Santo

Agradecimentos

Agradeço primeiramente à Deus, que me deu a oportunidade e a graça de lutar por meus objetivos.

A minha mãe, Maria das Graças Pereira Paiva, pelo carinho e compreensão e ao meu pai, José Paiva *(in memoriam)*.

Agradeço ao meu orientador, Prof. Michel Guimarães Coswosck, pelo profissionalismo, caráter, sugestões bibliográficas, conversas esclarecedoras e por ter acreditado no meu potencial. Muito obrigado professor!

A minha noiva Andressa de Andrade Santos, por estar ao meu lado nos momentos bons e ruins, pela força, por sua paciência e compreensão.

Aos colegas e amigos inseparáveis do curso Matemática Licenciatura.

Aos Docentes do curso de Matemática da UFES (Campus São Mateus), em especial aos professores: Wesley Rocha Gripa e Leonardo Delarmelina Secchin, pelo auxilio no processo de digitação e manuseio de softwares e aos professores Paulo Wander Barbosa e Lúcio Souza Fassarella, pela leitura crítica e às sugestões dadas ao trabalho.

A Matemática é a rainha das ciências e a Teoria dos Números é a rainha da Matemática.

Carl Friedrich Gauss

Uma catedral não é uma catedral até que o último andaime tenha sido retirado.

Carl Friedrich Gauss

Resumo

Neste trabalho estudaremos as Funções Aritméticas, mais especificamente, as Funções Multiplicativas. A função maior inteiro, que apesar de não ser uma Função Aritmética, desempenha um grande papel na Teoria dos Números e será de grande importância para chegar na demonstração da Lei da Reciprocidade Quadrática de Gauss.

A Teoria dos Números tem uma longa história, originando-se nas antigas civilizações da humanidade. Diferentemente de outros ramos da matemática, destaca-se não pela linguagem e técnica que desenvolve, mas pelos tipos de problemas e teoremas que possui e pela interdisciplinaridade e imaginação que eles exigem em sua resolução. Por esta razão, a área atrai simpatizantes de todos os ramos da matemática, principalmente depois da demonstração de um dos teoremas mais complexos da matemática, que é o Último Teorema de Fermat, demonstrado pelo matemático inglês Andrew Willes em 1995.

Palavras-chave: Funções Aritméticas, Lei da Reciprocidade Quadrática de Gauss.

Abstract

In this work we study Arithmetic Functions, and more specifically Multiplicative Functions. The greatest integer function, which although not being an Arithmetic Function, plays a role in Number Theory and will be of great importance to get the statement of the Quadratic Reciprocity Law of Gauss.

The Theory of Numbers has a long history, originating in the ancient civilizations of mankind. Unlike other branches of mathematics, it is remarkable not by language and technique that develops, but due to the types of problems and theorems which owns and by interdisciplinarity and imagination that they require for their resolution. For this reason, the area attracts supporters from all branches of mathematics especially after the statement of one of the most complex theorems of mathematics, which is Fermat's last Theorem, demonstrated by the english mathematician Andrew Willes in 1995.

Keywords: Arithmetic Functions, Quadratic Reciprocity Law of Gauss.

Sumário

Introdução

A finalidade deste trabalho é estudar as Funções Aritméticas e a Lei da Reciprocidade Quadrática, a fim de utilizá-los como ferramenta para a resolução de numerosos problemas, em especial, os oriundos de competições de matemática.

Este trabalho foi desenvolvido através de pesquisas bibliográficas, fazendo uso de livros e apostilas.

O primeiro capítulo foi centrado em alguns resultados básicos da Teoria Elementar dos Números, que serão de grande importância para este trabalho, com alguns teoremas apenas enunciados e outros foram enunciados e demonstrados.

O segundo capítulo é dedicado às Funções Aritméticas, descrevendo as definições, provando os teoremas e resolvendo problemas de diversos níveis de dificuldade.

O estudo dos Resíduos Quadráticos, feito no terceiro capítulo, introduzimos o símbolo de Legendre que nos permite obter informações sobre a existência ou não de solução para as congruências quadráticas $x^2 \equiv a(mod\ p)$, com p primo. Apresentamos uma demonstração da Lei da Reciprocidade Quadrática e algumas de suas aplicações.

O interesse pelo assunto, surgiu logo após cursar as disciplinas de Álgebra I e II, ministrada pelo professor Michel Guimarães Coswosck, o qual me incentivou a pesquisar e desenvolver estudos na área de Teoria dos Números.

1 Preliminares

Neste capítulo, apresentaremos alguns resultados básicos da Teoria dos Números que serão utilizados ao longo do trabalho. Assumiremos como conhecidas as propriedades mais elementares de $\mathbb{Z}$.

Para começar, assumiremos o seguinte axioma:

Axioma: Princípio da Boa Ordenação.
Todo subconjunto não vazio S de $\mathbb{Z}$, limitado inferiormente, admite um menor elemento, isto é, existe $n_0 \in S$ tal que $n_0 \leq n$; $\forall n \in S$.

Com base neste axioma, pode se obter duas ferramentas de grande utilidade para lidar com os inteiros:

Princípio de Indução Matemática (Primeira Forma).
Seja $S(n)$ uma sentença aberta em $\{n \in \mathbb{N}; n \geq n_0\}$, com $n_0 \in \mathbb{Z}$ fixo, tal que

i) $S(n_0)$ é uma sentença verdadeira.

ii) Para todo $n \geq n_0$, se $S(n)$ é uma sentença verdadeira, então $S(n+1)$ também é verdadeira.
Então, $S(n)$ é verdadeira para todo $n \geq n_0$.

Princípio de Indução Matemática (Segunda Forma).
Seja $S(n)$ uma sentença aberta em $\{n \in \mathbb{N}; n \geq n_0\}$, com $n_0 \in \mathbb{Z}$ fixo, tal que

i) $S(n_0)$ é uma sentença verdadeira.

ii) Para cada inteiro $m \geq n_0$, $S(m)$ é uma sentença verdadeira sempre que $S(k)$ for verdadeira para $n_0 \leq k < m$.
Então, $S(n)$ é verdadeira para todo $n \geq n_0$.

Teorema 1.0.1. *(Algoritmo da divisão) Dados dois inteiros a e b com $b \neq 0$, existem únicos inteiros q e r tais que $a = bq + r$, com $0 \leq r < |b|$.*

Demonstração. Ver [6], páginas 56 e 57. □

Observação: O inteiro q é chamado quociente e r de resto da divisão de a por b.

1.1 Divisibilidade

Definição 1.1.1. *Sejam a, $b \in \mathbb{Z}$, com $a \neq 0$. Dizemos que "a divide b"(ou que "a é divisor de b"ou que "b é múltiplo de a"), quando existe $c \in \mathbb{Z}$ tal que $b = ac$.*

Representaremos esta propriedade pelo simbolo $a|b$. Se a não divide b, escrevemos $a \nmid b$.

Propriedades

Sejam $a,\ b,\ c,\ n\ \in \mathbb{Z}$, então são válidas as seguintes propriedades:

i) Se $a|b$ e $b|c$, então $a|c$.

ii) Se $a|b$ e $a|c$, então $a|(bx + cy)$, $\forall x, y \in \mathbb{Z}$.

iii) $a|a$, $\forall a \in \mathbb{Z}^*$.

iv) Se $a|n$, então $ba|bn$, $\forall b \in \mathbb{Z}^*$.

v) Se $ab|ac$ e $a \neq 0$, então $b|c$.

vi) $1|a$, $\forall a \in \mathbb{Z}$.

vii) $a|0$, $\forall a \in \mathbb{Z}^*$.

viii) Se $a|b$ e $b \neq 0$, então $|a| \leq |b|$.

ix) Se $a|b$ e $b|a$, então $|a| = |b|$.

Definição 1.1.2. *Sejam a e b dois inteiros não simultaneamente nulos. Diremos que d é um máximo divisor comum de a e b se as seguintes propriedades são verificadas:*
i) $d|a$ e $d|b$, ou seja, d é um divisor comum de a e b.
ii) Se $c \in \mathbb{Z}$ é tal que $c|a$ e $c|b$, então $c|d$, ou seja, se c é um divisor comum de a e b então c é um divisor de d.

Observação: Se d é um máximo divisor comum de a e b então $-d$ também será. Deste modo, denotaremos por (a, b) o máximo divisor comum positivo de a e b. Assim $(a, b) = |d|$.

A partir deste momento, estaremos trabalhando com o máximo divisor comum positivo de a e b, onde a, b são números inteiros não simultaneamente nulos.

Propriedades de Máximo Divisor Comum.

i) Se a e b são inteiros não simultaneamente nulos e $d = (a, b)$, então existem $x_0, y_0 \in \mathbb{Z}$ tais que $d = ax_0 + by_0$.

ii) $(a, 0) = |a|$, se $a \neq 0$.

iii) Se $c|ab$ e $(c, a) = 1$, então $c|b$.

vi) $(a, bc) = 1 \iff (a, b) = (a, c) = 1$, onde a, b e a, c não são simultaneamente nulos.

v) Se a e b não são simultaneamente nulos, então $(a, b) = (a, b + ax)$, $\forall x \in \mathbb{Z}$.

vi) Se $(a, b) = d$, então $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

vii) Se t é um inteiro não nulo, então $(ta, tb) = |t|(a, b)$.

viii) Se a e b são inteiros tais que $a = bq + r$, onde q e r são inteiros, então $(a, b) = (b, r)$.

ix) Se $a, b, c \in \mathbb{Z}$ tais que $a|c$ e $b|c$, então $\left.\frac{ab}{(a, b)}\right| c$.

Definição 1.1.3. *Dados dois inteiros a e b não simultaneamente nulos, diremos que m é um mínimo múltiplo comum de a e b se seguintes condições são verificadas:*
i) $a|m$ e $b|m$, ou seja, m é múltiplo comum de a e b.
ii) Se $c \in \mathbb{Z}$ é tal que $a|c$ e $b|c$, então $m|c$, isto é, se $c \in \mathbb{Z}$ é um múltiplo comum de a e b então c é múltiplo de m.

Observação: Se m é um mínimo múltiplo comum de a e b então $-m$ também será. Deste modo, denotaremos por $[a, b]$, como sendo o mínimo múltiplo comum positivo de a e b, ou seja, $[a, b] = |m|$.

A partir deste momento, estaremos trabalhando com o mínimo múltiplo comum positivo de a e b, onde a, b são números inteiros não simultaneamente nulos.

Teorema 1.1.1. *Se a e b são dois inteiros não simultaneamente nulos então*

$$[a, b](a, b) = |ab|.$$

Demonstração. Ver [19], página 19. □

Definição 1.1.4. *Um inteiro p, com $p \neq 0$ e $p \neq \pm 1$ é dito um número primo se, e somente se, os únicos divisores positivos de p são: 1 e $|p|$. Se p não é primo, dizemos que p é um número composto, ou simplesmente, composto.*

Observação: Se $p|ab$ e p é primo, então $p|a$ ou $p|b$.
De fato, se $p \not| a$, então $(a, p) = 1$, o que implica pela propriedade (iv) de máximo divisor comum que $p|b$.

Teorema 1.1.2. *(Teorema Fundamental da Aritmética) Todo inteiro maior do que 1 pode ser representado de modo único (a menos da ordem dos fatores) como um produto de fatores primos positivos.*

Demonstração. Se n é primo não há nada a ser demonstrado. Suponhamos que n seja um número composto. Seja p_1, onde $p_1 > 1$, o menor dos divisores positivos de n.
Assim p_1 é um número primo, pois caso contrário, existiria p, com $1 < p < p_1$ tal que $p|n$, 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 sendo o menor divisor positivo de n_1. Pelo argumento anterior, p_2 é primo e tem-se que $n = p_1 p_2 n_2$.
Repetindo esse procedimento, obtemos uma sequência decrescente de inteiros positivos $n_1, n_2, ..., n_r$. Como estes inteiros são maiores que 1, este processo deve terminar, pois caso contrário, teríamos

$$n > n_1 > n_2 > n_3 > n_4 > ... > 1.$$

Como os primos na sequência $p_1, p_2, ..., p_r$ não são, necessariamente distintos, n terá, em geral, a forma

$$n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}.$$

Agora vejamos a unicidade. Para isto, usaremos a segunda forma de indução em n.
Para $n = 2$, a afirmação é verdadeira.
Assumiremos então, que a unicidade seja válida para todos os inteiros maiores que 1 e menores que n. Vamos provar que a afirmação é verdadeira para n.
Com efeito, se n é primo, não há nada o que provar.
Suponhamos que n seja um número composto e que possua duas fatorações:

$$n = p_1 p_2 p_3 ... p_s = q_1 q_2 q_3 ... q_r,$$

onde $p_1, p_2, p_3, ..., p_s, q_1, q_2, q_3, ..., q_r$ são números primos.
Como $p_1|q_1 q_2 ... q_r$, segue que $p_1|q_j$, para algum $j \in \{1, 2, ..., r\}$. Sem perda de generalidade, suponhamos que $p_1|q_1$. Como ambos são números primos positivos, segue que $p_1 = q_1$.

Logo $p_1p_2p_3...p_s = q_1q_2q_3...q_r$, implica que

$$m = \frac{n}{p_1} = p_2p_3...p_s = q_2q_3...q_r,$$

Como $1 < m = \frac{n}{p_1} < n$, pela hipótese de indução, segue que $r - 1 = s - 1$, ou seja, $r = s$. As fatorações $p_1p_2p_3...p_s$ e $q_1q_2q_3...q_r$ são iguais, a menos da ordem dos fatores. □

Corolário 1.1.1. *Todo inteiro $n \neq 0, \pm 1$, pode ser escrito sob a forma: $n = \pm p_1^{\alpha_1}p_2^{\alpha_2}...p_r^{\alpha_r}$, com os p_i números primos positivos distintos e os α_i números inteiros positivos. Além disso, essa escrita é única, a menos da ordem dos fatores.*

Uma consequência do Teorema Fundamental da Aritmética é:

Teorema 1.1.3. *(Euclides) Existem infinitos números primos.*

Demonstração. Suponha que exista apenas um número finito de números primos $p_1, p_2, ..., p_r$. Considere o número natural $m = p_1p_2...p_r + 1$. Notemos que $m > 1$. Pelo Teorema Fundamental da Aritmética, existe um primo p tal que $p|m$. Como o conjunto dos números primos é finito, existe $i \in \{1, 2, 3, ..., r\}$ tal que $p = p_i$. Assim, $p|p_1p_2...p_r$ e como $p|m$, segue que $p|1$, o que é um absurdo!
Portanto existem infinitos números primos. □

Teorema 1.1.4. *Sejam a e b inteiros positivos tais que $(a, b) = 1$. Então se $d|ab$ com $d > 0$, existe um único par de divisores positivos d_1 de a e d_2 de b tais que $d = d_1d_2$, onde $(d_1, d_2) = 1$. Reciprocamente, se $d_1|a$, $d_2|b$, $d_1, d_2 > 0$, então $d = d_1d_2 > 0$ e é tal que $d|ab$.*

Demonstração. Considere as fatorações de a e b:

$$a = p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}...p_r^{\alpha_r},$$

$$b = q_1^{\beta_1}q_2^{\beta_2}q_3^{\beta_3}...q_s^{\beta_s}.$$

Como $(a, b) = 1$, segue que os conjuntos $\{p_1, p_2, ..., p_r\}$ e $\{q_1, q_2, ..., q_s\}$ são disjuntos. Desta forma, a fatoração de ab será dada por

$$ab = p_1^{\alpha_1}p_2^{\alpha_2}...p_r^{\alpha_r}q_1^{\beta_1}q_2^{\beta_2}...q_s^{\beta_s}.$$

Assim, se $d|ab$ com $d > 0$ então:

$$d = p_1^{\gamma_1}p_2^{\gamma_2}...p_r^{\gamma_r}q_1^{\theta_1}q_2^{\theta_2}...q_s^{\theta_s},$$

onde $0 \leq \gamma_i \leq \alpha_i;\ i = 1, 2, ..., r$ e $0 \leq \theta_j \leq \beta_j;\ j = 1, 2, ..., s$.
Definimos $d_1 = p_1^{\gamma_1} p_2^{\gamma_2} ... p_r^{\gamma_r}$ e $d_2 = q_1^{\theta_1} q_2^{\theta_2} ... q_s^{\theta_s}$. Deste modo, $d = d_1 d_2$ e $(d_1, d_2) = 1$.
Reciprocamente, sejam $d_1, d_2 \in \mathbb{N}^*$ tais que $d_1 | a$ e $d_2 | b$.
Logo $d_1 = p_1^{\gamma_1} p_2^{\gamma_2} ... p_r^{\gamma_r};\ 0 \leq \gamma_i \leq \alpha_i$, com $i = 1, 2, ..., r$ e $d_2 = q_1^{\theta_1} q_2^{\theta_2} ... q_s^{\theta_s};\ 0 \leq \theta_j \leq \beta_j$, com $j = 1, 2, ..., s$.
Assim $d = d_1 d_2 = p_1^{\gamma_1} p_2^{\gamma_2} ... p_r^{\gamma_r} q_1^{\theta_1} q_2^{\theta_2} ... q_s^{\theta_s}$ é tal que $d | ab$. □

1.2 Congruências

Definição 1.2.1. *Seja m um inteiro tal que $m > 1$. Dois inteiros a e b serão ditos congruentes módulo m se, e somente se, $m|(a - b)$.*
Quando a e b são congruentes módulo m, escrevemos $a \equiv b (mod\ m)$.

Observação: Dois números não congruentes módulo m serão ditos incongruentes módulo m.

Proposição 1.2.1. *Sejam $a, b, m \in \mathbb{Z}$ com $m > 1$. $a \equiv b (mod\ m)$ se, e somente se, os restos de a e b por m são iguais.*

Demonstração. Com efeito, suponha que $a \equiv b (mod\ m)$.
Fazendo Divisão Euclidiana de a por m e b por m, existem $q, l, r, s \in \mathbb{Z}$ tais que

$$a = mq + r, \text{ onde } 0 \leq r < m,$$

$$b = ml + s, \text{ onde } 0 \leq s < m.$$

Notemos que

$$\begin{cases} 0 \leq r < m \\ 0 \leq s < m \end{cases} \Rightarrow 0 \leq |r - s| < m.$$

Por outro lado, $a - b = m(q - l) + (r - s)$.
Como $m|(a - b)$ e $m|(q - l)$, segue que $m|(r - s)$. De $m|(r - s)$, segue que

$$m = |m| \leq |r - s| \text{ ou } |r - s| = 0.$$

Como $m > |r - s|$, segue que $|r - s| = 0$ e portanto $r = s$.
Reciprocamente, suponhamos que a e b deixam o mesmo resto na divisão por m. Assim existem $q, l, r \in \mathbb{Z}$ tais que:

$$a = mq + r, \text{ onde } 0 \leq r < m,$$

$$b = ml + r, \text{ onde } 0 \leq r < m.$$

Assim $a-b = m(q-l)$, o que implica que, $m|(a-b)$ e consequentemente $a \equiv b(mod\, m)$. □

Propriedades de Congruência

Sejam a, b, c, d, m e n inteiros com $m > 1$, $n > 1$ e $r \geq 1$. Temos 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 $a \equiv c(mod\ m)$.

iv) Se $a \equiv b(mod\ m)$ e $c \equiv d(mod\ m)$, então $a \pm c \equiv b \pm d(mod\ m)$.

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

vi) Se $a \equiv b(mod\ m)$, então $a^n \equiv b^n(mod\ m)$, $\forall n \in \mathbb{N}$.

vii) Se $a \equiv b(mod\ m)$ e se $n|m$, então $a \equiv b(mod\ n)$.

viii) Se $ac \equiv bc(mod\ m)$ e $(c, m) = 1$, então $a \equiv b(mod\ m)$.

ix) Se $d = (c, m)$, então $ac \equiv bc(mod\ m) \Longleftrightarrow a \equiv b\left(mod\ \dfrac{m}{d}\right)$.

Definição 1.2.2. *O conjunto dos inteiros $\{a_1, a_2, ..., a_r\}$ é um sistema completo de resíduos módulo m se:*

i) $a_i \not\equiv a_j(mod\ m)$, para $i \neq j$;

ii) Para todo inteiro n, existe um único a_i, tal que, $n \equiv a_i(mod\ m)$.

Observação: É fácil verificar que $\{0, 1, 2, ..., m-1\}$ é um sistema completo de resíduos módulo m e que se r números inteiros distintos formam um sistema completo de resíduos modulo m então $r = m$.

Teorema 1.2.1. *Se (r,m)=1, então $\{a, a + r, a + 2r, ..., a + (m - 1)r\}$ é um sistema completo de resíduos módulo m, $\forall a \in \mathbb{Z}$.*

Demonstração. Sejam $i, j \in \{0, 1, ..., m - 1\}$ tais que

$$a + ir \equiv a + jr(mod\ m).$$

Assim

$$ir \equiv jr(mod\ m).$$

Como $(r, m) = 1$, segue que, $i \equiv j(mod\ m)$. Como $\{0, 1, 2, ..., m - 1\}$ é um sistema completo de resíduos módulo m, com $i, j \in \{0, 1, 2, ..., m - 1\}$, concluímos que $i = j$. Deste modo

$$i \neq j \Rightarrow a + ir \not\equiv a + jr(mod\ m).$$

Assim, os elementos do conjunto $\{a, a+r, a+2r, ..., a+(m-1)r\}$ são incongruentes dois a dois módulo m. $(*)$

Por outro lado, seja $t \in \mathbb{Z}$ qualquer. Como $\{0, 1, 2, ..., m-1\}$ é um sistema completo de resíduos módulo m, existe $i \in \{0, 1, 2, ..., m-1\}$ tal que $t \equiv i(mod\ m)$.

Novamente, pelo fato de $\{0, 1, 2, ..., m-1\}$ ser um sistema completo de resíduos módulo m, temos

$$\begin{aligned} a &\equiv a_1(mod\ m) \\ a+r &\equiv a_2(mod\ m) \\ &\vdots \\ a+(k-1)r &\equiv a_k(mod\ m) \\ &\vdots \\ a+(m-1)r &\equiv a_m(mod\ m), \end{aligned}$$

onde $a_1, a_2, ..., a_m \in \{0, 1, 2, ..., m-1\}$.

Como os elementos do conjunto $\{a, a+r, ..., a+(k-1)r\}$ são incongruentes dois a dois módulo m, segue que $\{a_1, a_2, ..., a_m\} = \{0, 1, ..., m-1\}$.

Se $a_k = i$, então $i = a+(k-1)r\ (mod\ m)$. $(**)$

De $(*)$ e $(**)$, concluímos que $\{a, a+r, a+2r, ..., a+(m-1)r\}$ é um sistema completo de resíduos módulo m, onde $(r, m) = 1$. □

Definição 1.2.3. *Sejam $n, k \in \mathbb{N}$. O número binomial n sobre k, o qual denotaremos por $\binom{n}{k}$, é definido por:*

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

Lema 1.2.1. *Seja p um número primo, então $p \left| \begin{pmatrix} p \\ k \end{pmatrix} \right.$, onde $1 \leq k \leq p-1$.*

Demonstração.

Afirmação: $\begin{pmatrix} n \\ r \end{pmatrix} = \frac{n}{r} \begin{pmatrix} n-1 \\ r-1 \end{pmatrix}$.

Com efeito,

$$\begin{aligned}
\frac{n}{r}\begin{pmatrix} n-1 \\ r-1 \end{pmatrix} &= \frac{n}{r}\frac{(n-1)!}{(r-1)![(n-1)-(r-1)]!} \\
\frac{n}{r}\begin{pmatrix} n-1 \\ r-1 \end{pmatrix} &= \frac{n}{r}\frac{(n-1)!}{(r-1)!(n-r)!} \\
\frac{n}{r}\begin{pmatrix} n-1 \\ r-1 \end{pmatrix} &= \frac{n(n-1)!}{r(r-1)!(n-r)!} \\
\frac{n}{r}\begin{pmatrix} n-1 \\ r-1 \end{pmatrix} &= \frac{n!}{r!(n-r)!} = \begin{pmatrix} n \\ r \end{pmatrix}.
\end{aligned}$$

Assim, pela afirmação anterior, temos:

$$\begin{pmatrix} p \\ k \end{pmatrix} = \frac{p}{k}\begin{pmatrix} p-1 \\ k-1 \end{pmatrix}$$

onde, $1 \leq k \leq p-1$. Assim

$$p\begin{pmatrix} p-1 \\ k-1 \end{pmatrix} = k\begin{pmatrix} p \\ k \end{pmatrix}$$

o que implica que $p\left|k\begin{pmatrix} p \\ k \end{pmatrix}\right.$. Como $(p,k)=1$, pois $1 \leq k \leq p-1$, e p primo, segue que

$$p\left|\begin{pmatrix} p \\ k \end{pmatrix}\right., \text{ onde } 1 \leq k \leq p-1.$$

□

Teorema 1.2.2. *(Teorema de Wilson) Se $p \in \mathbb{Z}_+^*$ é um primo, então*

$$(p-1)! \equiv -1 (mod\ p).$$

Demonstração. Ver [18] pág.: 39. □

Teorema 1.2.3. *(Pequeno Teorema de Fermat) Dado um número primo p, tem-se que $a^p \equiv a (mod\ p)$, $\forall a \in \mathbb{N}^*$.*

Demonstração. Mostrar que $a^p \equiv a (mod\ p)$ é equivalente a mostrar que $p|(a^p - a)$, $\forall a \in \mathbb{N}^*$. Faremos indução sobre a.
De fato, o resultado claramente é válido para $a = 1$.

Suponha que a afirmação seja verdadeira para a, ou seja, $p|(a^p - a)$. Assim

$$(a+1)^p - (a+1) = a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + ... + \binom{p}{p-1}a + 1 - a - 1$$

$$(a+1)^p - (a+1) = (a^p - a) + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + ... + \binom{p}{p-1}a.$$

Pelo lema anterior, temos que $p\left|\binom{p}{k}\right.$, com $1 \leq k \leq p-1$ e pela hipótese de indução, tem-se que, $p|a^p - a$. Logo $p|(a+1)^p - (a-1)$.
Assim a afirmação é verdadeira para $a+1$. Portanto, pelo Princípio de Indução Matemática 1ª forma, a afirmação é verdadeira para todo a natural, ou seja, $a^p \equiv a(mod\ p)$, $\forall a \in \mathbb{N}^*$. □

Corolário 1.2.1. *Se p é um número primo e $a \in \mathbb{N}$, com $(a,p) = 1$ então,*

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

Demonstração. Pelo Pequeno Teorema de Fermat, temos

$$a^p \equiv a(mod\ p) \Rightarrow aa^{p-1} \equiv a(mod\ p)$$

Como $(a,p) = 1$, pela propriedade (viii) de congruência, segue que $a^{p-1} = 1(mod\ p)$. □

Definição 1.2.4. *A função ϕ, chamada de função de Euler, é definida como sendo o número de inteiros positivos menores ou iguais a n que são primos entre si com n, ou seja: $\phi(n) = \sum_{x \in A} 1$, onde $A = \{x \in \mathbb{N}^*;\ x \leq n \text{ e } (x,n) = 1\}$.*

Teorema 1.2.4. *(Teorema de Euler-Fermat) Se a e m são inteiros positivos tais que $(a,m) = 1$, então $a^{\phi(m)} \equiv 1(mod\ m)$.*

Demonstração. Ver [18], pág.: 43. □

Definição 1.2.5. *O conjunto dos inteiros $\{a_1, a_2, ..., a_{\phi(m)}\}$ é um sistema reduzido de resíduos módulo m se:*
i) $a_i \not\equiv a_j(mod\ m)$, para $i \neq j$;
ii) Para cada $a_j \in \{a_1, a_2, ..., a_{\phi(m)}\}$, $(a_j, m) = 1$.

Exemplo 1.2.1. $\{1,3,7,9\}$ é um sistema reduzido de resíduos módulo 10.

Exemplo 1.2.2. Se p é um número primo positivo, então $\{1,2,3,...,p-1\}$ é um sistema reduzido de resíduos módulo p.

Definição 1.2.6. *Chamam-se de Equações Diofantinas às equações polinomiais com coeficientes inteiros, para as quais, estamos interessados somente nas soluções inteiras ou racionais.*

As equações Diofantinas da forma $ax + by = n$, com a, b e n inteiros, são chamadas de equações Diofantinas lineares.

Teorema 1.2.5. *A equação Diofantina $ax + by = m$ admite solução se, e somente se, $(a, b)|m$.*

Demonstração. Suponha que a equação dada admita uma solução x_0, y_0, isto é,

$$ax_0 + by_0 = m.$$

Como $(a, b)|a$ e $(a, b)|b$, segue que $(a, b)|ax_0 + by_0$, ou seja, $(a, b)|m$.
Reciprocamente, suponha que $(a, b)|n$. Então existe um inteiro l tal que $n = (a, b)l$. Por outro lado, existem $m_0, n_0 \in \mathbb{Z}$, tais que, $am_0 + bn_0 = (a, b)$.
Assim

$$n = l(a, b) = a(lm_0) + b(ln_0).$$

Logo os inteiros, $x_0 = lm_0$ e $y = ln_0$ são uma solução da equação. □

Definição 1.2.7. *Congruências lineares são congruências da forma $ax \equiv b(mod\ n)$, onde a, b e n são inteiros dados, com $a \neq 0$, $n > 1$.*

Corolário 1.2.2. *Sejam $a, b, m \in \mathbb{Z}$, com $m > 1$. A congruência linear $ax \equiv b(mod\ m)$ admite solução se, e somente se, $(a, m)|b$.*

Demonstração. Suponha que $x_0 \in \mathbb{Z}$ seja uma solução da congruência linear

$$ax \equiv b(mod\ m).$$

Assim

$$ax_0 \equiv b(mod\ m).$$

Deste modo, existe $r \in \mathbb{Z}$, tal que $ax_0 = mr + b$, ou seja, $ax_0 + m(-r) = b$. Isto implica que a equação diofantina $ax + my = b$ admite solução. Logo $(a, m)|b$. Reciprocamente, suponha que $(a, m)|b$. Assim, a Equação Diofantina $ax + my = b$ admite solução. Seja x_0, y_0 uma solução da equação dada. Assim $ax_0 + my_0 = b$.
Deste modo, $ax_0 \equiv b(mod\ m)$, o que implica que a congruência linear $ax \equiv b(mod\ m)$ admite solução. □

O Teorema de Euler-Fermat nos diz que, dado $a, m \in \mathbb{Z}$ com $m \geq 1$ e $(a, m) = 1$ tem-se que $a^{\phi(m)} \equiv 1(mod\ m)$. Isto implica que o conjunto $S = \{r \in \mathbb{N}^*;\ a^r \equiv 1(mod\ m)\}$ é um conjunto não vazio. Como $S \neq \varnothing$, $S \subset \mathbb{Z}$ e é limitado inferiormente, pelo Princípio da Boa Ordenação, S admite um menor elemento k.

Definição 1.2.8. *O menor inteiro positivo k para o qual $a^k \equiv 1(mod\ m)$, onde $(a, m) = 1$, é chamado de ordem de a módulo m e denotamos por $ord_m a$.*

Exemplo 1.2.3. Como $2 \not\equiv 1(mod\ 7)$, $2^2 \not\equiv 1(mod\ 7)$ e como $2^3 \equiv 1(mod\ 7)$, então $ord_7 2 = 3$.

2 Funções Aritméticas

Neste capítulo, introduziremos o conceito de Funções Aritméticas e nos dedicaremos ao estudo de uma classe de funções aritméticas que são as funções multiplicativas.

Estudaremos, também, a função maior inteiro que, apesar de não ser uma função aritmética, desempenha um grande papel na Teoria dos Números e neste trabalho será utilizado na demonstração da Lei da Reciprocidade Quadrática.

2.1 Definição e exemplos de Funções Aritméticas

Definição 2.1.1. *Uma Função Aritmética é uma função f com domínio no conjunto dos números inteiros positivos e cuja imagem é real ou complexo.*

Exemplos de Funções Aritméticas.

Exemplo 2.1.1. A função τ é definida como sendo o número de inteiros positivos que são divisores de n, ou seja, $\tau(n) = \sum_{d|n} 1$.

Exemplo 2.1.2. A função σ é definida como sendo a soma dos divisores positivos de n, ou seja, $\sigma(n) = \sum_{d|n} d$.

Exemplo 2.1.3. A função ϕ, chamada de função de Euler, é definida como sendo o número de inteiros positivos menores ou iguais a n que são primos com n, ou seja:

$$\phi(n) = \sum_{x \in A} 1$$

onde

$$A = \{x \in \mathbb{N}^*;\ x \leq n \ e\ (x, n) = 1\}.$$

Exemplo 2.1.4. A função λ, chamada de função de Liouville, é definida por:

$$\begin{aligned} \lambda(1) &= 1 \text{ e, para } n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r} \\ \lambda(n) &= (-1)^{\alpha_1 + \alpha_2 + \ldots + \alpha_r}. \end{aligned}$$

Exemplo 2.1.5. A função μ, chamada de função de Möbius, é definida por:

$$\begin{aligned} \mu(1) &= 1 \quad \text{e, para } n = p_1^{a_1}.p_2^{a_2}...p_r^{a_r} \\ \mu(n) &= (-1)^r \quad \text{se} \quad a_1 = a_2 = ... = a_r = 1 \\ \mu(n) &= 0 \quad \text{caso contrário.} \end{aligned}$$

Exemplo 2.1.6. A função v, é definida por: $v(n) = 1$, $\forall n \in \mathbb{N}^*$.

Exemplo 2.1.7. A função N, é definida por: $N(n) = n$, $\forall n \in \mathbb{N}^*$.

Exemplo 2.1.8. A função u, chamada de função nula, é definida por:

$$u(n) = 0, \ \forall n \in \mathbb{N}^*.$$

Definição 2.1.2. *Uma função aritmética não nula f é dita multiplicativa se*

$$f(mn) = f(m)f(n),$$

para todo par de inteiros positivos m e n, onde $(m, n) = 1$.
Uma função aritmética não nula f é dita completamente multiplicativa se

$$f(mn) = f(m)f(n),$$

para todo $m, n \in \mathbb{N}^*$.

Teorema 2.1.1. *Se f é uma função multiplicativa então* $F(n) = \sum_{d|n} f(d)$ *é multiplicativa.*

Demonstração. Sejam *m,n* inteiros positivos tais que $(m, n) = 1$. Pela definição de *F(n)*, temos

$$F(mn) = \sum_{d|mn} f(d).$$

Como $(m, n) = 1$, pelo Teorema 1.1.4, segue que, para cada divisor positivo d de mn, existe único par de divisores positivos, digamos d_1 de m e d_2 de n, tais que $d = d_1 d_2$ e $(d_1, d_2) = 1$. Deste modo, temos

$$F(mn) = \sum_{d|mn} f(d) = \sum_{d_1 d_2|mn} f(d_1 d_2).$$

Como f é multiplicativa, temos

$$\begin{aligned} F(mn) &= \sum_{d_1 d_2 | mn} f(d_1)f(d_2) = \sum_{d_1|m}\sum_{d_2|n} f(d_1)f(d_2) \\ F(mn) &= \sum_{d_1|m}\left(\sum_{d_2|n} f(d_1)f(d_2)\right) \\ F(mn) &= \sum_{d_1|m} f(d_1)\sum_{d_2|n} f(d_2) \\ F(mn) &= F(m)F(n). \end{aligned}$$

□

Corolário 2.1.1. *As funções τ e σ são multiplicativas, bem como λ, v e N.*

Demonstração. Como as funções $v(d) = 1$ e $N(d) = d$ são multiplicativas e

$$\tau(n) = \sum_{d|n} 1 = \sum_{d|n} v(d)$$

e

$$\sigma(n) = \sum_{d|n} d = \sum_{d|n} N(d)$$

concluímos que $\tau(n)$ e $\sigma(n)$ são multiplicativas.

Os casos de λ, v e N são triviais. □

Proposição 2.1.1. *Para p primo e a um inteiro positivo temos*

$$\tau(p^a) = (a+1) \text{ e } \sigma(p^a) = \frac{p^{a+1}-1}{p-1}.$$

Demonstração. Como os divisores de p^a são: $1, p, p^2, ..., p^a$, segue que $\tau(n) = (a+1)$. Por outro lado

$$\begin{aligned} \sigma(p^a) &= 1 + p + p^2 + p^3 + p^4 + \ldots + p^{a-1} + p^a \\ \Rightarrow p \cdot \sigma(p^a) &= p + p^2 + p^3 + p^4 + \ldots + p^a + p^{a+1} \end{aligned}$$

Subtraindo a primeira da segunda, temos $(p-1)\cdot(\sigma(p^a)) = p^{a+1} - 1$, ou seja,

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

□

Proposição 2.1.2. *Se* $n = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdot \ldots \cdot p_r^{a_r}$, *então*

$$\tau(n) = \prod_{i=1}^{r}(a_i + 1)$$

e

$$\sigma(n) = \prod_{i=1}^{r} \frac{p_i^{a_i+1} - 1}{p_i - 1}.$$

Demonstração. Sabemos que $\tau(n)$ e $\sigma(n)$ são funções multiplicativas, assim

$$\tau(n) = \tau(p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_r^{a_r}) = \tau(p_1^{a_1}) \cdot \tau(p_2^{a_2}) \cdot \ldots \cdot \tau(p_r^{a_r}).$$

Pela proposição 1, temos

$$\tau(n) = \tau(p_1^{a_1}) \cdot \tau(p_2^{a_2}) \cdot \ldots \cdot \tau(p_r^{a_r}) = (a_1 + 1) \cdot (a_2 + 1) \cdot \ldots \cdot (a_r + 1) = \prod_{i=1}^{r}(a_i + 1).$$

Por outro lado,

$$\sigma(n) = \sigma(p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_r^{a_r}) = \sigma(p_1^{a_1}) \cdot \sigma(p_2^{a_2}) \cdot \ldots \cdot \sigma(p_r^{a_r}).$$

Novamente, pela proposição 1, temos

$$\begin{aligned} \sigma(n) &= \sigma(p_1^{a_1}) \cdot \ldots \cdot \sigma(p_r^{a_r}) \\ \Rightarrow \sigma(n) &= \left(\frac{p_1^{a_1+1} - 1}{p_1 - 1}\right) \cdot \left(\frac{p_2^{a_2+1} - 1}{p_2 - 1}\right) \cdot \ldots \cdot \left(\frac{p_r^{a_r+1} - 1}{p_r - 1}\right) \\ \Rightarrow \sigma(n) &= \prod_{i=1}^{r} \frac{p_i^{a_i+1} - 1}{p_i - 1}. \end{aligned}$$

□

Teorema 2.1.2. *Para* p *primo e* a *um inteiro positivo tem-se que* $\phi(p^a) = p^a\left(1 - \frac{1}{p}\right)$.

Demonstração. Notemos que $p, 2p, 3p, \ldots, p^{a-1}p$ são inteiros positivos maiores ou iguais a 1 e menores ou iguais a p^a, que são múltiplos de p. Deste modo $(b, p^a) \neq 1$ para $b \in \{\ p, 2p, 3p, \cdots, p^{a-1}p\}$.

Por outro lado, seja $c \in \mathbb{Z}$ tal que $1 \leq c \leq p^a$ e $c \notin \{\ p, 2p, 3p, \cdots, p^{a-1}p\}$.

Afirmação: $(c, p^a) = 1$. Com efeito, suponha que $(c, p^a) = d > 1$, pelo Teorema Fundamental da Aritmética, existe q primo tal que $q|d$. Como $d|c$ e $d|p^a$, segue que $q|c$ e $q|p^a$. Como q é primo e $q|p^a$, segue que $q|p$. Como p e q são primos positivos tais que $q|p$, segue

que p=q. Assim $p|c$, o que é um absurdo, pois c não é múltiplo de p.

Portanto $\phi(p^a) = p^a - p^{a-1} = p^a\left(1 - \frac{1}{p}\right)$. □

Lema 2.1.1. *Se $S \subset \mathbb{Z}$ é um sistema completo de resíduos módulo n, então ele possui exatamente $\phi(n)$ elementos primos com n.*

Demonstração. Sabemos que $\{0, 1, 2, ..., n-1\}$ é um sistema completo de resíduos módulo n. Assim, é fácil ver que tal sistema completo de resíduos módulo n possui $\phi(n)$ elementos que são primos com n.

Por outro lado, todo sistema completo de resíduos módulo n pode ser escrito na forma

$$S = \{a_k = \alpha_k n + k;\ k = 0, 1, 2, ..., n-1\},\ \text{onde } \alpha_k \in \mathbb{Z},\ \forall k = 0, 1, 2, ..., n-1.$$

Então,

$$(a_k, n) = 1 \Leftrightarrow (k, n) = 1,\ \forall k = 0, 1, 2, ..., n-1.$$

Isto implica que, o número de elementos de S que são primos com n é igual ao número de elementos de $\{0, 1, 2, ..., n-1\}$ que são primos com n que é igual a $\phi(n)$. □

Teorema 2.1.3. *A função ϕ é multiplicativa.*

Demonstração. Dados $m, n \in \mathbb{Z}^*$, considere a tabela formada com os inteiros de 1 a mn

$$\begin{array}{cccccc} 1 & 2 & \cdots & r & \cdots & m \\ m+1 & m+2 & \cdots & m+r & \cdots & 2m \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ (n-1)m+1 & (n-1)m+2 & \cdots & (n-1)m+r & \cdots & nm \end{array}$$

Como $(a, mn) = 1$ se, e somente se, $(a, m) = (a, n) = 1$, segue que os inteiros na tabela acima que são primos com mn, são primos com m e n simultaneamente.
Se o primeiro elemento de uma coluna não for primo com m, ou seja, $(r, m) = d > 1$ então, todos os números desta coluna não serão primos com m.
De fato, um elemento arbitrário desta coluna é da forma $im+r$ com $i \in \{0, 1, 2, ..., n-1\}$. Daí

$$(m, r + im) = (m, r + im - mi) = (m, r) = d > 1.$$

Deste modo, existem $\phi(m)$ colunas de números que são primos com m.
Agora, devemos determinar, quantos números das $\phi(m)$ colunas, são primos com n. Como $(m,n)=1$, pelo Teorema 1.2.1 o conjunto $\{r, m+r, 2m+r, ..., (n-1)m+r\}$ forma um sistema completo de resíduos módulo n e assim, pelo Lema 2.1.1, existem $\phi(n)$ destes elementos que são primos com n, para todo $r = 1, 2, ..., m$. Logo o número de elementos simultaneamente primos com m e n é $\phi(m)\phi(n)$. □

Teorema 2.1.4. *Seja $n = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdot \ldots p_r^{a_r}$, a fatoração primária de n, temos:*

$$\phi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_r}\right).$$

Demonstração. Pelo Teorema 2.1.2, segue que

$$\phi(p_i^{a_i}) = p_i^{a_i} - p_i^{a_i - 1} = p_i^{a_i}\left(1 - \frac{1}{p_i}\right).$$

Como $\phi(n)$ é uma função multiplicativa segue que

$$\begin{aligned}
\phi(n) &= \phi(p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_r^{a_r}) = \phi(p_i^{a_i}) \cdot \phi(p_2^{a_2}) \cdot \ldots \cdot \phi(p_r^{a_r}) \\
\phi(n) &= p_1^{a_1} \cdot \left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot p_r^{a_r} \cdot \left(1 - \frac{1}{p_r}\right) \\
\phi(n) &= n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_r}\right).
\end{aligned}$$

□

Teorema 2.1.5. *Para qualquer inteiro n positivo, temos $\sum_{d|n} \phi(d) = n$.*

Demonstração. Sendo $\phi(n)$ uma função multiplicativa, do Teorema 2.1.1,

$$g(n) = \sum_{d|n} \phi(d)$$

também é multiplicativa, de modo que, se $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$ é a fatoração de n, temos

$$g(n) = g(p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}) = g(p_1^{\alpha_1}) g(p_2^{\alpha_2}) ... g(p_r^{\alpha_r}).$$

Para cada valor de i, os divisores positivos de $p_i^{\alpha_i}$ são: $1, p_i, p_i^2, ..., p_i^{\alpha_i}$, ou seja:

$$\begin{aligned}
g(p_i^{\alpha_i}) &= \sum_{d|p_i^{\alpha_i}} \phi(d) \\
g(p_i^{\alpha_i}) &= \phi(1) + \phi(p_i) + \phi(p_i^2) + ... + \phi(p_i^{\alpha_i - 1}) + \phi(p_i^{\alpha_i})
\end{aligned}$$

$$\begin{aligned} g(p_i^{\alpha_i}) &= 1 + (p_i - 1) + (p_i^2 - p_i) + ... + (p_i^{\alpha_{i-1}} - p_i^{\alpha_{i-2}}) + (p_i^{\alpha_i} - p_i^{\alpha_{i-1}}) \\ g(p_i^{\alpha_i}) &= p_i^{\alpha_i} \end{aligned}$$

Portanto $g(n) = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r} = n$, ou seja,

$$\sum_{d|n} \phi(d) = n.$$

□

Proposição 2.1.3. *Seja P o produto dos primos positivos comuns a m e n, então*

$$\phi(mn) = \frac{P\phi(m)\phi(n)}{\phi(P)}.$$

Demonstração. Considerando as fatorações primárias

$$n = p_1^{a_1} \dots p_r^{a_r} q_1^{\alpha_1} \dots q_s^{\alpha_s}$$

e

$$m = p_1^{b_1} \dots p_r^{b_r} Q_1^{\beta_1} \dots Q_v^{\beta_v},$$

com $(q_i, Q_j) = 1,\ \forall i = 1, 2, ..., s$ e $\forall j = 1, 2, ..., v$.
Então

$$P = p_1 \dots p_r.$$

Daí temos

$$\phi(mn) = \phi(p_1^{a_1} \dots p_r^{a_r} q_1^{\alpha_1} \dots q_s^{\alpha_s} p_1^{b_1} \dots p_r^{b_r} Q_1^{\beta_1} \dots Q_v^{\beta_v})$$

$$\phi(mn) = \phi(p_1^{a_1+b_1} \dots p_r^{a_r+b_r} q_1^{\alpha_1} \dots q_r^{\alpha_r} Q_1^{\beta_1} \dots Q_v^{\beta_v})$$

$$\phi(mn) = \phi(p_1^{a_1+b_1}) \dots \phi(p_r^{a_r+b_r}) \phi(q_1^{\alpha_1}) \dots \phi(q_s^{\alpha_s}) \phi(Q_1^{\beta_1}) \dots \phi(Q_v^{\beta_v})$$

$$\phi(mn) = p_1^{a_1+b_1}\left(1 - \frac{1}{p_1}\right) \dots p_r^{a_r+b_r}\left(1 - \frac{1}{p_r}\right) q_1^{\alpha_1}\left(1 - \frac{1}{q_1}\right) \dots$$

$$\dots q_s^{\alpha_s}\left(1 - \frac{1}{q_s}\right) Q_1^{\beta_1}\left(1 - \frac{1}{Q_1}\right) \dots Q_v^{\beta_v}\left(1 - \frac{1}{Q_v}\right)$$

$$\phi(mn) = p_1^{b_1} \dots p_r^{b_r} Q_1^{\beta_1} \dots Q_v^{\beta_v} p_1^{a_1} \dots p_r^{a_r} q_1^{\alpha_1} \dots q_s^{\alpha_s}\left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_r}\right)\left(1 - \frac{1}{q_1}\right) \dots$$

$$\dots \left(1 - \frac{1}{q_s}\right)\left(1 - \frac{1}{Q_1}\right) \dots \left(1 - \frac{1}{Q_v}\right)$$

$$\phi(mn) = m\left[n\left(1-\frac{1}{p_1}\right)\ldots\left(1-\frac{1}{p_r}\right)\left(1-\frac{1}{q_1}\right)\ldots\left(1-\frac{1}{q_s}\right)\right]\left(1-\frac{1}{Q_1}\right)\ldots\left(1-\frac{1}{Q_v}\right)$$

$$\phi(mn) = m\phi(n)\left(1-\frac{1}{Q_1}\right)\ldots\left(1-\frac{1}{Q_v}\right)$$

$$\phi(mn) = \frac{\phi(n)m\left(1-\frac{1}{p_1}\right)\ldots\left(1-\frac{1}{p_r}\right)\left(1-\frac{1}{Q_1}\right)\ldots\left(1-\frac{1}{Q_v}\right)}{\left(1-\frac{1}{p_1}\right)\ldots\left(1-\frac{1}{p_r}\right)}$$

$$\phi(mn) = \frac{\phi(n)\phi(m)}{\left(1-\frac{1}{p_1}\right)\ldots\left(1-\frac{1}{p_r}\right)}$$

$$\phi(mn) = \frac{P\phi(n)\phi(m)}{P\left(1-\frac{1}{p_1}\right)\ldots\left(1-\frac{1}{p_r}\right)}$$

$$\phi(mn) = \frac{P\phi(n)\phi(m)}{\phi(P)}.$$ □

Proposição 2.1.4. *$\phi(n) > \dfrac{\log 2}{\log 2n}n$ para todo $n > 2$.*

Demonstração. Seja $n = p_1^{a_1}\ldots p_r^{a_r}$, a fatoração primária de n. Assim

$$\begin{aligned}
\phi(n) &= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_r}\right)\\
\frac{\phi(n)}{n} &= \left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_r}\right)\\
\frac{\phi(n)}{n} &= \prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right) > \prod_{i=2}^{r+1}\left(1-\frac{1}{i}\right) = \left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\ldots\left(1-\frac{1}{r+1}\right) = \frac{1}{r+1},
\end{aligned}$$

ou seja

$$\phi(n)n > \frac{1}{r+1}. \qquad (*)$$

Por outro lado

$$n \geq p_1 ... p_r > 2^r.$$

Assim

$$2n > 2^{r+1} \Rightarrow \log 2n > \log 2^{r+1} \Rightarrow \log 2n > (r+1)\log 2 \Rightarrow \frac{1}{r+1} > \frac{\log 2}{\log 2n}. \qquad (**)$$

De $(*)$ e $(**)$, concluímos que

$$\frac{\phi(n)}{n} \geq \frac{1}{r+1} > \frac{\log 2}{\log 2n} \Rightarrow \phi(n) > \frac{\log 2}{\log 2n} n.$$

□

A seguinte proposição relaciona as funções σ e ϕ.

Proposição 2.1.5. *Seja n um número inteiro maior do que 1, então*

$$\phi(n)\sigma(n) < n^2.$$

Demonstração. Seja $n = p_1^{a_1} \dots p_r^{a_r}$, a fatoração primária de n. Então

$$\begin{aligned}
\sigma(n) &= \left(\frac{p_1^{a_1+1}-1}{p_1-1}\right)\dots\left(\frac{p_r^{a_r+1}-1}{p_r-1}\right) < \frac{p_1^{a_1+1}\dots p_r^{a_r+1}}{(p_1-1)\dots(p_r-1)} \\
\sigma(n) &< \frac{p_1^{a_1+1}\dots p_r^{a_r+1}}{(p_1-1)\dots(p_r-1)} = \frac{(p_1^{a_1}\dots p_r^{a_r})(p_1\dots p_r)}{(p_1-1)\dots(p_r-1)} = \frac{n(p_1\dots p_r)}{(p_1-1)\dots(p_r-1)} \\
\sigma(n) &< \frac{n(p_1\dots p_r)}{(p_1-1)\dots(p_r-1)} = \frac{n(p_1\dots p_r)}{p_1\left(1-\frac{1}{p_2}\right)p_2\left(1-\frac{1}{p_2}\right)\dots p_r\left(1-\frac{1}{p_r}\right)} \\
\sigma(n) &< \frac{n(p_1\dots p_r)}{p_1\left(1-\frac{1}{p_1}\right)\dots p_r\left(1-\frac{1}{p_r}\right)} = \frac{n(p_1\dots p_r)}{(p_1\dots p_r)\left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_r}\right)} \\
\sigma(n) &< \frac{n(p_1\dots p_r)}{(p_1\dots p_r)\left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_r}\right)} = \frac{n}{\left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_r}\right)}\cdot\frac{n}{n} = \frac{n^2}{\phi(n)}.
\end{aligned}$$

Assim

$$\sigma(n) < \frac{n^2}{\phi(n)},$$

e portanto

$$\sigma(n)\phi(n) < n^2.$$

□

Vejamos um exemplo de função aritmética completamente multiplicativa.

Teorema 2.1.6. *A função λ de Liouville possui as seguintes propriedades:*

a) A função λ de Liouville é completamente multiplicativa.

b) $\sum_{d|n} \lambda(d) = \begin{cases} 1 & \text{se } n \text{ possui raiz quadrada} \\ 0 & \text{caso contrário} \end{cases}$.

Demonstração. a) Sejam $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r}$ e $n = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_r^{\beta_r}$ onde

$$\alpha_1, \alpha_2, \ldots, \alpha_r, \beta_1, \beta_2, \ldots, \beta_r \geq 0.$$

Então

$$m.n = p_1^{\alpha_1+\beta_1} p_2^{\alpha_2+\beta_2} \ldots p_r^{\alpha_r+\beta_r}$$

e

$$\begin{aligned} \lambda(mn) &= (-1)^{\alpha_1+\beta_1+\alpha_2+\beta_2+\ldots+\alpha_r+\beta_r} \\ \lambda(mn) &= (-1)^{\alpha_1+\alpha_2+\ldots+\alpha_r}(-1)^{\beta_1+\beta_2+\ldots+\beta_r} \\ \lambda(mn) &= \lambda(m)\lambda(n). \end{aligned}$$

b) Sendo λ uma função completamente multiplicativa (em particular multiplicativa), pelo Teorema 2.1.1, segue que

$$F(n) = \sum_{d|n} \lambda(d)$$

é uma função multiplicativa. Assim

$$\begin{aligned} F(p^\alpha) &= \sum_{d|p^\alpha} \lambda(d) \\ F(p^\alpha) &= \lambda(1) + \lambda(p) + \lambda(p^2) + \ldots + \lambda(p^\alpha). \end{aligned}$$

Temos dois casos a considerar: Se α é par, teremos que $\alpha = 2k$, para algum $k \in \mathbb{Z}$. Daí segue que:

$$\begin{aligned} F(p^\alpha) &= \lambda(1) + \lambda(p) + \lambda(p^2) + \lambda(p^3) + \ldots + \lambda(p^{2k-1}) + \lambda(p^{2k}) \\ F(p^\alpha) &= 1 + (-1)^1 + (-1)^2 + (-1)^3 + \ldots + (-1)^{2k-1} + (-1)^{2k} \\ F(p^\alpha) &= 1. \end{aligned}$$

Se α é impar, teremos que $\alpha = 2k+1$, para algum $k \in \mathbb{Z}$. Daí temos

$$\begin{aligned} F(p^\alpha) &= \lambda(1) + \lambda(p) + \lambda(p^2) + \lambda(p^3) + \ldots + \lambda(p^{2k}) + \lambda(p^{2k+1}) \\ F(p^\alpha) &= 1 + (-1)^1 + (-1)^2 + (-1)^3 + \ldots + (-1)^{2k} + (-1)^{2k+1} \\ F(p^\alpha) &= 0. \end{aligned}$$

Assim, concluímos que $F(p^\alpha) = \begin{cases} 1 & \text{se } \alpha \text{ é par} \\ 0 & \text{se } \alpha \text{ é ímpar} \end{cases}$.

Se $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r}$, então $F(n) = F(p_1^{\alpha_1})F(p_2^{\alpha_2}) \ldots F(p_r^{\alpha_r}) = 1$ se $\alpha_1, \alpha_2, \ldots, \alpha_r$ forem todos números pares. Caso contrário $F(n) = 0$.

Portanto, $F(n) = \sum_{d|n} \lambda(d) = \begin{cases} 1 & \text{se n possui raiz quadrada} \\ 0 & \text{caso contrário} \end{cases}$. □

Teorema 2.1.7. *A função μ de Möbius é multiplicativa.*

Demonstração. Sejam $m, n \in \mathbb{N}$ tais que $(m, n) = 1$, e mn não é livre de quadrados.
Assim $\mu(mn) = 0$.
Afirmação: Se p é um número primo tal que $p^2|mn$ e mn não é livre de quadrados, então $p^2|m$ ou $p^2|n$.
Com efeito, suponha que $p^2 \nmid m$ e $p^2 \nmid n$. Como $p^2|mn$, $p^2 \nmid m$ e $p^2 \nmid n$, segue que $p|m$ e $p|n$. Logo $p|(m, n)$, ou seja, $p|1$, o que é um absurdo pois p é primo.
Assim, como mn não é livre de quadrado, existe p primo tal que $p^2|mn$. Pela afirmação anterior, temos que $p^2|m$ ou $p^2|n$.
Assim $\mu(m) = 0$ ou $\mu(n) = 0$. Logo $\mu(m).\mu(n) = 0 = \mu(mn)$.
Por outro lado, sejam $m = p_1.p_2...p_r$ e $n = q_1.q_2...q_s$ onde $p_1, ..., p_r, q_1, ..., q_s$ são números primos positivos distintos dois a dois, com $m, n \in \mathbb{N}$, $(m, n) = 1$ e mn livre de quadrados. Deste modo

$$\mu(mn) = \mu(p_1...p_r.q_1...q_s) = (-1)^{r+s} = (-1)^r.(-1)^s = \mu(m).\mu(n).$$

□

Teorema 2.1.8. $F(n) = \sum_{d|n} \mu(d) = \begin{cases} 1 & \textit{se } n = 1 \\ 0 & \textit{se } n > 1 \end{cases}$.

Demonstração. Se $n = 1$ temos

$$F(1) = \sum_{d|1} \mu(d) = \mu(1) = 1.$$

Agora, analisaremos para o caso em que $n > 1$. Como μ é uma função multiplicativa, segue do Teorema 2.1.1, que *F(n)* é também uma função multiplicativa.
Seja $n = p^r$ para algum $r > 1$.
Assim

$$F(n) = \sum_{d|n} \mu(d) = \mu(1) + \mu(p) + \mu(p^2) + \ldots + \mu(p^r) \Rightarrow F(n) = 1 + (-1)^1 = 1 - 1 = 0.$$

Assim, se $n = p_1^{a_1} \ldots p_r^{a_r} > 1$ onde $p_1, \ldots, p_r$ são primos positivos distintos dois a dois, temos:

$$F(n) = F(p_1^{a_1} \ldots p_r^{a_r}) = F(p_1^{a_1}) \ldots F(p_r^{a_r}) = 0.$$

□

2.2 Função Maior Inteiro

Agora veremos uma função que não é aritmética e no entanto desempenha um papel de grande importância na Teoria dos Números, como por exemplo, na demonstração da Lei da Reciprocidade Quadrática.

Definição 2.2.1. *A função maior inteiro ou função degrau, é a que associa a cada real x ao maior inteiro menor ou igual a x. Denotaremos por* $[x]$.

Obs.: Pela definição da função maior inteiro temos $0 \leq x - [x] < 1$. Denotamos $\{x\} = x - [x]$, como sendo a parte fracionária de x.

Exemplo 2.2.1. $[4] = 4$; $[20,0015] = 20$; $[0,768] = 0$; $[-3,887] = -4$; $[\pi] = 3$;
$\left[\frac{1}{2}\right] = [0,5] = 0$; $\left[\frac{5}{3}\right] = [1,666...] = 1$.

Vejamos algumas propriedades da função maior inteiro.

Propriedade 2.2.1. $x = [x] + \{x\},\ \forall x \in \mathbb{R}$.

Prova: Segue direto da definição de parte fracionária de x.

Propriedade 2.2.2. $x - 1 < [x] \leq x < [x] + 1$, *para todo* $x \in \mathbb{R}$.

Prova: Temos

$$0 \leq x - [x] < 1 \Rightarrow -1 < [x] - x \leq 0 \Rightarrow x - 1 < [x] \leq x. \qquad (*)$$

Por outro lado

$$0 \leq x - [x] < 1 \Rightarrow x < 1 + [x]. \qquad (**)$$

De $(*)$ e $(**)$, concluímos o resultado desejado.

Propriedade 2.2.3. *$[n + \{x\}] = n$, onde $n \in \mathbb{Z}$ e $x \in \mathbb{R}$.*

Prova: De fato

$$0 \leq \{x\} < 1 \Rightarrow n \leq n + \{x\} < n + 1 \Rightarrow [n + \{x\}] = n.$$

Propriedade 2.2.4. *$[n + x] = n + [x]$, onde $n \in \mathbb{N}$ e $x \in \mathbb{R}$.*

Prova: De $0 \leq x - [x] < 1$, segue que, $[x] \leq x < [x] + 1$. Assim

$$n + [x] \leq n + x < n + [x] + 1 \Rightarrow [n + x] = n + [x].$$

Propriedade 2.2.5. *Se $a, b \in \mathbb{Z}$ com $b > 0$ então o quociente da divisão de a por b é $q = \left[\frac{a}{b}\right]$.*

Prova: Fazendo Divisão Euclidiana de a por b temos

$$\begin{aligned} a &= bq + r \ ; \ 0 \leq r < b \\ \frac{a}{b} &= q + \frac{r}{b} \ ; \ 0 \leq \frac{r}{b} < 1 \\ \Rightarrow \left[\frac{a}{b}\right] &= \left[q + \frac{r}{b}\right] = q + \left[\frac{r}{b}\right] = q + 0 = q. \end{aligned}$$

Propriedade 2.2.6. $\left[\frac{x}{n}\right] = \left[\frac{[x]}{n}\right]$, *onde $x \in \mathbb{R}$ e $n \in \mathbb{Z}_+^*$.*

Prova: Fazendo Divisão Euclidiana de $[x]$ por n temos, $[x] = nq + r$, onde $0 \leq r < n$. Pela propriedade anterior temos $q = \left[\frac{[x]}{n}\right]$.
Por outro lado

$$\left[\frac{x}{n}\right] = \left[\frac{[x] + \{x\}}{n}\right] = \left[\frac{[x]}{n} + \frac{\{x\}}{n}\right] = \left[\frac{nq}{n} + \frac{r}{n} + \frac{\{x\}}{n}\right] = \left[q + \frac{r + \{x\}}{n}\right].$$

Como $0 \leq \{x\} < 1$ e $0 \leq r \leq n - 1$, segue que

$$0 \leq \{x\} + r < n \Rightarrow 0 \leq \frac{\{x\} + r}{n} < 1 \Rightarrow \left[\frac{\{x\} + r}{n}\right] = 0.$$

Daí

$$\left[\frac{x}{n}\right] = q.$$

Portanto

$$\left[\frac{[x]}{n}\right] = \left[\frac{x}{n}\right].$$

Propriedade 2.2.7. $[-x] = -[x] - 1$, *se* $x \notin \mathbb{Z}$.

Prova: Como $x \notin \mathbb{Z}$ temos

$$0 < x - [x] < 1 \Rightarrow -1 < [x] - x < 0 \Rightarrow -1 - [x] < -x < -[x] \Rightarrow [-x] = -[x] - 1.$$

Propriedade 2.2.8. $[x + y] \leq [x] + [y] + 1$, *onde* $x, y \in \mathbb{R}$.

Prova: Sejam $x = [x] + \{x\}$; $0 \leq \{x\} < 1$ e $y = [y] + \{y\}$; $0 \leq \{y\} < 1$.
Assim,

$$0 \leq \{x\} + \{y\} < 2 \Rightarrow \Big[\{x\} + \{y\}\Big] = 0 \; ou \; \Big[\{x\} + \{y\}\Big] = 1.$$

Deste modo,

$$\Big[\{x\} + \{y\}\Big] \leq 1.$$

Por outro lado,
$x + y \; = [x] + [y] + \{x\} + \{y\}$

$$[x + y] = \Big[\Big([x] + [y]\Big) + \{x\} + \{y\}\Big]$$

$$[x + y] = [x] + [y] + \Big[\{x\} + \{y\}\Big] \leq [x] + [y] + 1.$$

Propriedade 2.2.9. *Se* n *é um inteiro positivo, então* $\left[\frac{n}{a}\right]$ *é o número de inteiros do conjunto* $\{1, 2, 3, ..., n\}$ *que são divisíveis por* a, *onde* $a \in \mathbb{N}^*$.

Prova: Sejam $\{a, 2a, 3a, ..., ia\}$ $(i \in \mathbb{N})$, o conjunto de todos os inteiros entre 1,2,3,...,n que são divisíveis por a. Assim

$$ia \leq n < (i + 1)a \Rightarrow i \leq \frac{n}{a} < i + 1 \Rightarrow \left[\frac{n}{a}\right] = i.$$

Teorema 2.2.1. *O número de dígitos de um inteiro positivo* n *é igual a* $[\log n] + 1$.

Demonstração. Seja n um inteiro positivo com x dígitos. Assim podemos afirmar que

$$10^{x-1} \leq n < 10^x$$

Assim,

$$x - 1 \leq \log n < x \Rightarrow [\log n] = x - 1 \Rightarrow x = 1 + [\log n].$$

□

Apesar da simplicidade, seja do enunciado ou da demonstração do Teorema 2.2.1, este pode ser aplicado em problemas de simples resolução e em problemas mais elaborados como, por exemplo, problemas de origem em competições de matemática. Vejamos três problemas que reforçam esta ideia.

Exemplo 2.2.2. Indique quantos dígitos possui o número 2^{64}. Use $\log 2 \cong 0,3$.
Solução:

$$x = [\log 2^{64}] + 1 = [64 \log 2] + 1 = [19,2] + 1 = 19 + 1 = 20.$$

Exemplo 2.2.3. (Olimpíada da Bélgica - 99) A representação decimal de 2^{1999} consiste de n dígitos e a representação decimal de 5^{1999} de m dígitos. Determine m+n.

Solução:

$$n = [\log 2^{1999}] + 1 = [1999 \log 2] + 1.$$

Por outro lado

$$\begin{aligned} m &= [\log 5^{1999}] + 1 = [1999 \log 5] + 1 = [1999(\log \frac{10}{2})] + 1 = [1999(1 - \log 2)] + 1 \\ m &= [1999 + (-1)1999 \log 2] + 1 = 1999 + [(-1)1999 \log 2] + 1 \\ m &= 2000 - [1999 \log 2] - 1 = 1999 - [1999 \log 2] = 1999 - (n-1) \\ m + n &= 1999 + 1 = 2000. \end{aligned}$$

Exemplo 2.2.4. (Olimpíada da Suíça - 2000) Seja q(n) a soma dos algarismos de n. Qual o valor de $q(q(q(2000^{2000})))$?
Solução:
Como $2000 = 2.10^3 \Rightarrow 2000^{2000} = 2^{2000}.10^{6000}$.
Assim:

$$q(2000^{2000}) = q(2^{2000}.10^{6000}) = q(2^{2000}).$$

Seja *N(n)* o número de dígito de n:

$$N(2^{2000}) = [\log 2^{2000}] + 1 = [2000. \log 2] + 1.$$

Como $\log 2 \cong 0,30103$, então $N(2000^{2000}) = 603$.
Como o maior número que possui 603 dígitos é aquele formado somente por dígitos 9, então:

$$q(2^{2000}) < 9.603 \Rightarrow q(2^{2000}) < 5427.$$

Dentre todos os números menores que 5427, o que possui maior soma dos algarismos é

4999. Assim:

$$q(q(2^{2000})) < q(4999) = 4 + 9 + 9 + 9 = 31.$$

Dentre todos os números menores que 31, o que possui maior soma dos algarismos é 29. Assim:

$$q(q(q(2^{2000}))) < q(29) = 2 + 9 = 11.$$

Sabemos também que $n \equiv q(n) \equiv q(q(n)) \equiv q(q(q(n)))(mod\ 9)$, ou seja,

$$2000^{2000} \equiv (2 + 0 + 0 + 0)^{2000}(mod\ 9) \Rightarrow 2000^{2000} \equiv 2^{2000}(mod\ 9)$$

$$\therefore 2^3 \equiv -1(mod\ 9) \Rightarrow (2^3)^{666} \equiv (-1)^{666} \Rightarrow 2^{1998} \equiv 1(mod\ 9) \Rightarrow 2^{2000} \equiv 4(mod\ 9).$$

Assim, já obtivemos que: $q(q(q(2000^{2000}))) \equiv 4(mod\ 9)$ e que

$$q(q(q(2000^{2000}))) < 11.$$

Como o único número menor que 11 que deixa resto 4 por 9 é 4, então

$$q(q(q(2000^{2000}))) = 4.$$

Teorema 2.2.2. *O expoente de um primo p na fatoração primária de $n!$, onde n é um número natural, é:*

$$a = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + ...$$

Demonstração. Sejam n e k dois números naturais e p um número primo $\leq n$. Os números da sequência $1, 2, 3, ..., n$ que são divisíveis por p^k são da forma lp^k, onde l é um número natural tal que $lp^k \leq n$, ou seja $l \leq \frac{n}{p^k}$. O número de $l's$ é, claramente igual a $\left[\frac{n}{p^k}\right]$.
Por outro lado, é claro que o expoente a do primo p na fatoração em fatores primos do número $n!$ é obtido pela soma do número de termos da sequência $1, 2, 3, ..., n$ que são divisíveis por p mais o número de termos que são divisíveis por p^2 mais o número de termos que são divisíveis por p^3 e assim por diante. Ou seja,

$$a = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + ...$$

□

Vejamos agora, um problema da Olimpíada de matemática da Argentina, ocorrida em 1997. Esta questão apesar de sua aparência hostil, a ferramenta matemática que está por trás da sua resolução é o Teorema 2.2.2.

Exemplo 2.2.5. (Olimpíada da Argentina - 97) Determine o último dígito antes do conjunto de zeros na representação do número: 19!+20!+21!+...+96!+97!.

Solução: Evidentemente, como na fatoração de *n!* existem mais potências de 2 do que de 5. O número de zeros de *n!* corresponde à potência de 5 de *n!*. Calculando, inicialmente, o número de zeros em que terminam *19!* e *20!*. $x_{19!} = \left[\frac{19}{5}\right] = 3$; $x_{20!} = \left[\frac{20}{5}\right] = 4$ Assim, temos que 19! termina em 3 zeros e 20! termina em 4 zeros. Portanto, na soma fornecida todos os números depois de 19! terminam em mais que 3 zeros, implicando que o último dígito de 19! + 20! + 21! + ... + 96! + 97! é igual ao último dígito de *19!*. Determinamos a fatoração de *19!*, ou seja, $19! = 2^a.3^b.5^3.7^c.11^d.13^e.17^f.19^g$.

$$a = \left[\frac{19}{2}\right] + \left[\frac{19}{2^2}\right] + \left[\frac{19}{2^3}\right] + \left[\frac{19}{2^4}\right] = 9 + 4 + 2 + 1 = 16$$

$$b = \left[\frac{19}{3}\right] + \left[\frac{19}{3^2}\right] = 6 + 2 = 8$$

$$c = \left[\frac{19}{7}\right] = 2$$

$$d = \left[\frac{19}{11}\right] = 1$$

$$e = \left[\frac{19}{13}\right] = 1$$

$$f = \left[\frac{19}{17}\right] = 1$$

$$g = \left[\frac{19}{19}\right] = 1$$

Deste modo

$$\begin{aligned} 19! &= 2^{16}.3^8.5^2.7^2.11.13.17.19 \\ 19! &= 2^{13}.3^8.7^2.11.13.17.19.(2^3.5^3) \\ 19! &= (2^{13}.3^8.7^2.11.13.17.19)(1000) \end{aligned}$$

Assim, o último dígito diferente de 0 de *19!* é igual ao dígito das unidades de

$N = 2^{13}.3^8.7^2.11.13.17.19$

- $2^6 \equiv 4(mod.10) \Rightarrow 2^{12} \equiv 6(mod.10) \Rightarrow 2^{13} \equiv 2(mod.10)$
- $3^2 \equiv -1(mod.10) \Rightarrow 3^6 \equiv -1(mod.10) \Rightarrow 3^8 \equiv -9(mod.10) \Rightarrow 3^8 \equiv 1(mod.10)$
- $7^2 \equiv 9(mod.10)$

- $11 \equiv 1(mod.10)$
- $13 \equiv 3(mod.10)$
- $17 \equiv 7(mod.10)$
- $19 \equiv 9(mod.10)$

Multiplicando estas congruências temos

$$2^{13}.3^8.7^2.11.13.17.19 \equiv 2.1.9.1.3.7.9(mod.10) \Rightarrow N \equiv 2(mod.10).$$

Portanto, o último dígitos diferente de 0 de $19! + 20! + 21! + ... + 96! + 97!$ é igual a 2.

2.3 Função Maior inteiro e Pontos Inteiros

O objetivo desta seção é apresentar alguns resultados relacionados a função maior inteiro e pontos inteiros, que serão ferramentas de grande utilidade na resolução de alguns problemas extraídos de diversas olimpíadas de matemática ao redor do mundo.

Teorema 2.3.1. *Sejam a,b,c e d números reais não negativos e seja* $f : [a, b] \longrightarrow [c, d]$ *uma função bijetora não-decrescente, então*

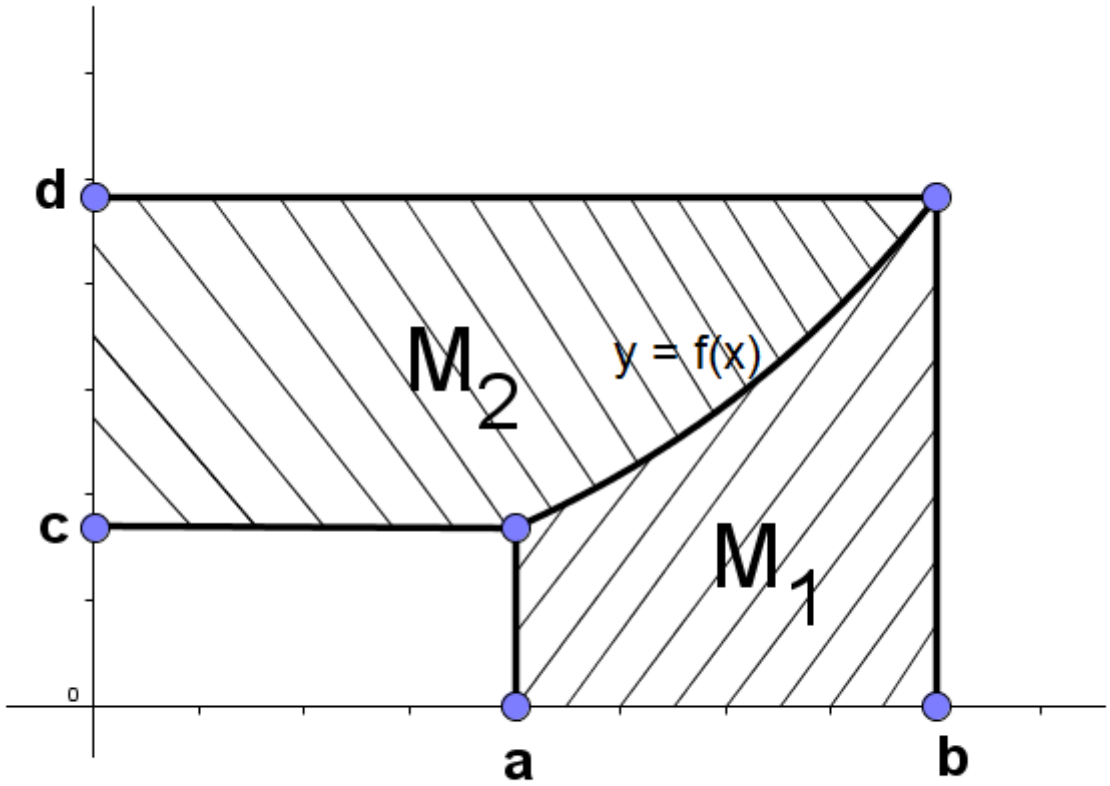
$$\sum_{a \leq k \leq b} [f(k)] + \sum_{c \leq k \leq d} [f^{-1}(k)] - n(G_f) = [b][d] - \alpha(a)\alpha(c)$$

onde k inteiro, $n(G_f)$ *é o número de pontos com coordenadas inteiras não negativas que pertencem ao gráfico da f e* $\alpha : \mathbb{R} \longrightarrow \mathbb{Z}$ *definida por:* $\alpha(x) = [x]$ *se* $x \in \mathbb{R}\backslash\mathbb{Z}$, $\alpha(x) = 0$ *se x=0 e* $\alpha(x) = x - 1$ *se* $x \in \mathbb{Z}\backslash\{0\}$.

Demonstração:
Sejam M uma região delimitada no plano e *n(M)* o número de pontos (x, y) com $x, y \in \mathbb{N}$ e $(x, y) \in M$. Como $f : [a, b] \longrightarrow [c, d]$ é monótona (mais precisamente, não-decrescente) e $f\big([a, b]\big) = [c, d]$ é um intervalo, então f é continua em $[a, b]$ (Ver [11], pág.:182).
Considere os seguintes conjuntos:

$$\begin{aligned}
M_1 &= \{(x, y) \in \mathbb{R}^2,\ a \leq x \leq b \text{ e } 0 \leq y \leq f(x)\} \\
M_2 &= \{(x, y) \in \mathbb{R}^2,\ c \leq y \leq d \text{ e } 0 \leq x \leq f^{-1}(y)\} \\
M_3 &= \{(x, y) \in \mathbb{R}^2,\ 0 \leq x \leq b \text{ e } 0 \leq y \leq d\} \\
M_4 &= \{(x, y) \in \mathbb{R}^2,\ 0 \leq x < a \text{ e } 0 \leq y < c\}.
\end{aligned}$$

Vejamos a seguinte figura:



Então

$$\begin{aligned} n(M_1) &= \sum_{a\leq k\leq b} \big[f(k)\big] \\ n(M_2) &= \sum_{c\leq k\leq d} \big[f^{-1}(k)\big] \\ n(M_3) &= [b].[d] \\ n(M_4) &= \alpha(a).\alpha(c). \end{aligned}$$

Temos então

$$n(M_1) + n(M_2) - n(M_1 \cap M_2) = n(M_1 \cup M_2).$$

Assim

$$n(M_1) + n(M_2) - n(G_f) = n(M3) - n(M_4),$$

ou seja,

$$\sum_{k=a}^{b}\big[f(k)\big]+\sum_{k=c}^{d}\big[f^{-1}(k)\big]-n(G_f)=[b][d]-\alpha(a)\alpha(c). \qquad \square$$

Problema 2.3.1. *(Olimpíada da Coreia) Expresse* $\sum_{k=1}^{n}[\sqrt{k}]$*, em termos de* n *e* $a=\sqrt{n}$*.*

Demonstração. Aplicando o Teorema 2.3.1, considere a função $f:[1,n]\longrightarrow[1,\sqrt{n}]$, dada por $f(x)=\sqrt{x}$. Como $n(G_f)=\big[\sqrt{n}\big]$, temos

$$\sum_{k=1}^{n}[\sqrt{k}]+\sum_{k=1}^{\sqrt{n}}[k^2]-[\sqrt{n}]=[n][\sqrt{n}]-\alpha(1)\alpha(1)=n[\sqrt{n}].$$

Assim

$$\sum_{k=1}^{n}[\sqrt{k}]=(n+1)a-\frac{a(a+1)(2a+1)}{6}=\frac{6a(n+1)-a(a+1)(2a+1)}{6}.$$

$\square$

Problema 2.3.2. *Calcule,* $S_n=\sum_{k=1}^{\frac{n(n+1)}{2}}\left[\frac{-1+\sqrt{1+8k}}{2}\right]$.

Demonstração. Considere a função $f:[1,n]\longrightarrow\left[1,\frac{n(n+1)}{2}\right]$, dada por

$$f(x)=\frac{x(x+1)}{2}.$$

A função f é bijetora não-decrescente. Note que $n(G_f)=n$ e

$$f^{-1}(x)=\frac{-1+\sqrt{1+8x}}{2}.$$

Aplicando a fórmula do Teorema 2.3.1,

$$\sum_{k=1}^{n}\left[\frac{k(k+1)}{2}\right]+\sum_{k=1}^{\frac{n(n+1)}{2}}\left[\frac{-1+\sqrt{1+8k}}{2}\right]-n=\frac{n^2(n+1)}{2}.$$

Assim

$$\begin{aligned}
\sum_{k=1}^{\frac{n(n+1)}{2}} \left[\frac{-1+\sqrt{1+8k}}{2}\right] &= \frac{n^2(n+1)}{2} + n - \frac{1}{2}\sum_{k=1}^{n} k(k+1) \\
\sum_{k=1}^{\frac{n(n+1)}{2}} \left[\frac{-1+\sqrt{1+8k}}{2}\right] &= \frac{n^2(n+1)}{2} + n - \frac{n(n+1)}{4} - \frac{n(n+1)(2n+1)}{12} \\
\sum_{k=1}^{\frac{n(n+1)}{2}} \left[\frac{-1+\sqrt{1+8k}}{2}\right] &= \frac{n(n^2+2)}{3}.
\end{aligned}$$

□

Lema 2.3.1. *Se m, n e s são inteiros positivos com $m \leq n$. Então, dada a sequência $\frac{1m}{n}, \frac{2m}{n}, \frac{3m}{n}, ..., \frac{sm}{n}$ existem $\left[\frac{(m,n)s}{n}\right]$ inteiros.*

Demonstração. Seja *d=(m,n)*. Assim, existem $m_1, n_1 \in \mathbb{Z}$ tal que $m = m_1 d$ e $n = n_1 d$. Assim a sequência dada é igual a:

$$\frac{1m_1}{n_1}, \frac{2m_1}{n_1}, \frac{3m_1}{n_1}, \ldots, \frac{sm_1}{n_1}$$

onde m_1 *e* n_1 são relativamente primos. Deste modo, existem $\left[\frac{s}{n_1}\right]$ números inteiros na sequência dada. Como $n_1 = \frac{n}{d} = \frac{n}{(m,n)}$, segue que, a quantidade de inteiros na sequência dada é $\left[\frac{s(m,n)}{n}\right]$. □

Teorema 2.3.2. *Sejam m, n e s inteiros positivos, com $m \leq n$. Então*

$$\sum_{1\leq k\leq s} \left[\frac{km}{n}\right] + \sum_{1\leq k\leq \frac{ms}{n}} \left[\frac{kn}{m}\right] = s\left[\frac{ms}{n}\right] + \left[\frac{(m,n)s}{n}\right]$$

onde k é inteiro positivo.

Demonstração. Considere a afirmação.

$$f : [1, s] \longrightarrow \left[\frac{m}{n}, \frac{ms}{n}\right], \text{ dada por } f(x) = \frac{m}{n}x.$$

Como f é uma função bijetora não-decrescente com 1, s, $\frac{m}{n}, \frac{ms}{n}$ números reais positivos, pelo Teorema 2.3.1, temos

$$\sum_{1\leq k\leq s} \big[f(k)\big] + \sum_{\frac{m}{n}\leq k\leq \frac{ms}{n}} \big[f^{-1}(k)\big] - n(G_f) = \big[\frac{ms}{n}\big]\big[s\big] - \alpha(1)\alpha\left(\frac{m}{n}\right).$$

Como

$$f^{-1}(x) = \frac{nx}{m} \text{ e } \alpha(1) = 0$$

e pelo Lema 2.3.1, temos

$$n(G_f) = \left[\frac{(m,n)s}{n}\right].$$

Portanto

$$\sum_{1\leq k\leq s}\left[\frac{km}{n}\right] + \sum_{\frac{m}{n}\leq k\leq\frac{ms}{n}}\left[\frac{kn}{m}\right] = s\left[\frac{ms}{n}\right] + \left[\frac{(m,n)s}{n}\right].$$

□

Corolário 2.3.1. *Nas condições do Teorema* 2.3.2*, se s=n, obtemos*

$$\sum_{1\leq k\leq n}\left[\frac{km}{n}\right] + \sum_{\frac{m}{n}\leq k\leq m}\left[\frac{kn}{m}\right] = mn + (m,n).$$

Teorema 2.3.3. *Sejam a, b, c e d números reais positivos e seja* $f : [a,b] \longrightarrow [c,d]$ *uma função bijetora não-crescente. Então*

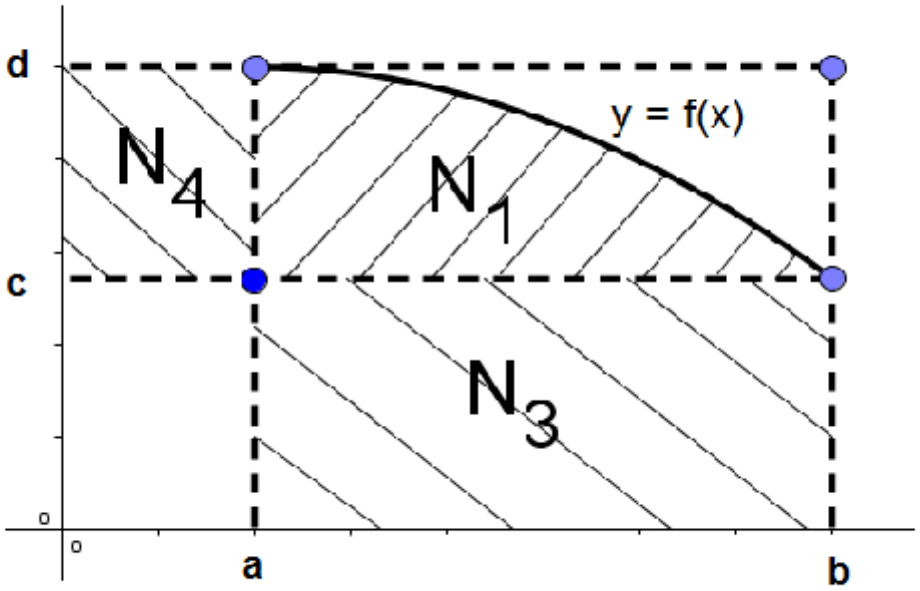
$$\sum_{a\leq k\leq b}\big[f(k)\big] - \sum_{c\leq k\leq d}\big[f^{-1}(k)\big] = [b]\alpha(c) - [d]\alpha(a)$$

onde k é inteiro e α *é a função definida no teorema 2.3.1.*

Demonstração. Sendo f uma função bijetora e não-decrescente em $[a,b]$, considere os conjuntos.

$$\begin{aligned}
N_1 &= \{(x,y)\in\mathbb{R}^2;\ a\leq x\leq b \text{ e } c\leq y\leq f(x)\}\\
N_2 &= \{(x,y)\in\mathbb{R}^2;\ a\leq x\leq f^{-1}(y) \text{ e } c\leq y\leq d\}\\
N_3 &= \{(x,y)\in\mathbb{R}^2;\ a\leq x\leq b \text{ e } 0\leq y\leq c\}\\
N_4 &= \{(x,y)\in\mathbb{R}^2;\ 0\leq x\leq a \text{ e } c\leq y\leq d\}.
\end{aligned}$$

Assim $N_2 = N_1$.



Então

$$\sum_{a\leq k\leq b}[f(k)] = n(N_1) + n(N_3)$$

$$\sum_{c\leq k\leq d}[f^{-1}(k)] = n(N_2) + n(N_4)$$

Como $n(N_1) = n(N_2)$, $n(N_3) = ([b] - \alpha(a))\alpha(c)$ e $n(N_4) = ([d] - \alpha(c))\alpha(a)$, segue que

$$\sum_{a\leq k\leq b}[f(k)] - \sum_{c\leq k\leq d}[f^{-1}(k)] = n(N_3) - n(N_4) = [b]\alpha(c) - [d]\alpha(a).$$

□

Teorema 2.3.4. *Sejam P número primo ímpar e $q \in \mathbb{Z}$, tal que $P \nmid q$ e f uma função $f : \mathbb{Z}_+^* \longrightarrow \mathbb{R}$ que satisfaz as seguintes condições:*

1) $P \nmid f(k);\ k = 1, 2, ..., P-1.$

2) $P|\big(f(k) + f(P-k)\big);\ k = 1, 2, ..., P-1.$

Então

$$\sum_{k=1}^{P-1}\left[f(k)\frac{q}{P}\right] = \frac{q}{P}\sum_{k=1}^{P-1}f(k) - \frac{P-1}{2}.$$

Demonstração. Da condição (2), tem-se que

$$\frac{qf(k)}{P} + \frac{qf(P-k)}{P} \in \mathbb{Z}. \qquad (*)$$

Da condição (1)

$$\frac{qf(k)}{P} \notin \mathbb{Z} \text{ e } \frac{qf(P-k)}{P} \notin \mathbb{Z};\ k = 1, 2, ..., P-1.$$

Então

$$0 < \left\{\frac{qf(k)}{P}\right\} + \left\{\frac{qf(P-k)}{P}\right\} < 2. \qquad (**)$$

Por outro lado, como

$$[x+y] \leq [x] + [y] + 1;\ \forall x, y \in \mathbb{R}$$

temos

$$\begin{aligned}
(x+y) - \{x+y\} &\leq x - \{x\} + y - \{y\} + 1 \\
-\{x+y\} &\leq x - \{x\} + y - \{y\} + 1 - (x+y) \\
\{x+y\} &\geq \{x\} + \{y\} - 1 \\
\{x\} + \{y\} &\leq \{x+y\} + 1.
\end{aligned}$$

Tome

$$x = \frac{qf(k)}{P} \text{ e } y = \frac{qf(P-k)}{P}.$$

Assim

$$\left\{\frac{qf(k)}{P}\right\} + \left\{\frac{qf(P-k)}{P}\right\} \leq 1 + \left\{\frac{qf(k)}{P} + \frac{qf(P-k)}{P}\right\}.$$

De (*), segue que

$$\left\{\frac{qf(k)}{P} + \frac{qf(P-k)}{P}\right\} = 0,$$

ou seja, $\dfrac{qf(k)}{P} + \dfrac{qf(P-k)}{P} \in \mathbb{Z}$. Assim

$$\left\{\frac{qf(k)}{P}\right\} + \left\{\frac{qf(P-k)}{P}\right\} \leq 1. \qquad (***)$$

De $(**)$ e $(***)$, segue que

$$0 < \left\{\frac{qf(k)}{P}\right\} + \left\{\frac{qf(P-k)}{P}\right\} \leq 1.$$

Suponha que

$$0 < \left\{\frac{qf(k)}{P}\right\} + \left\{\frac{qf(P-k)}{P}\right\} < 1.$$

Assim

$$\left[\left\{\frac{qf(k)}{P}\right\} + \left\{\frac{qf(P-k)}{P}\right\}\right] = 0$$

$$\left[\left(\frac{qf(k)}{P}-\left[\frac{qf(k)}{P}\right]\right)+\left(\frac{qf(P-k)}{P}-\left[\frac{qf(P-k)}{P}\right]\right)\right]=0$$
$$\left[\left(\frac{qf(k)}{P}+\frac{qf(P-k)}{P}\right)-\left(\left[\frac{qf(k)}{P}\right]+\left[\frac{qf(P-k)}{P}\right]\right)\right]=0$$
$$\frac{qf(k)}{P}+\frac{qf(P-k)}{P}-\left[\frac{qf(k)}{P}\right]-\left[\frac{qf(P-k)}{P}\right]=0$$

Deste modo

$$\left(\frac{qf(k)}{P}-\left[\frac{qf(k)}{P}\right]\right)+\left(\frac{qf(P-k)}{P}-\left[\frac{qf(P-k)}{P}\right]\right)=0$$
$$\left\{\frac{qf(k)}{P}\right\}+\left\{\frac{qf(P-k)}{P}\right\}=0$$

O que é um absurdo, pois $\left\{\frac{qf(k)}{P}\right\}+\left\{\frac{qf(P-k)}{P}\right\}>0$. Logo

$$\left\{\frac{qf(k)}{P}\right\}+\left\{\frac{qf(P-k)}{P}\right\}=1.$$

Isto implica que

$$\frac{qf(k)}{P}-\left[\frac{qf(k)}{P}\right]+\frac{qf(P-k)}{P}-\left[\frac{qf(P-k)}{P}\right]=1$$
$$\left[\frac{qf(k)}{P}\right]=\frac{qf(k)}{P}+\frac{qf(P-k)}{P}-\left[\frac{qf(P-k)}{P}\right]-1$$
$$\sum_{k=1}^{P-1}\left[\frac{qf(k)}{P}\right]=\sum_{k=1}^{P-1}\frac{qf(k)}{P}+\sum_{k=1}^{P-1}\frac{qf(P-k)}{P}-\sum_{k=1}^{P-1}\left[\frac{qf(P-k)}{P}\right]-\sum_{k=1}^{P-1}1.$$

Como

$$\sum_{k=1}^{P-1}\left[\frac{qf(k)}{P}\right]=\sum_{k=1}^{P-1}\left[\frac{qf(P-k)}{P}\right]$$

e

$$\sum_{k=1}^{P-1}\frac{qf(k)}{P}=\sum_{k=1}^{P-1}\frac{qf(P-k)}{P},$$

obteremos

$$\begin{aligned}2\sum_{k=1}^{P-1}\left[\frac{qf(k)}{P}\right] &= 2\sum_{k=1}^{P-1}\frac{qf(k)}{P}-(P-1)\\ 2\sum_{k=1}^{P-1}\left[\frac{qf(k)}{P}\right] &= \frac{2q}{P}\sum_{k=1}^{P-1}f(k)-(P-1)\\ \sum_{k=1}^{P-1}\left[\frac{qf(k)}{P}\right] &= \frac{q}{P}\sum_{k=1}^{P-1}f(k)-\frac{(P-1)}{2}.\end{aligned}$$

□

Os problemas olímpicos são formulados de modo que não apresente tão claramente os conceitos matemáticos utilizados em sua resolução.

Vejamos agora, um problema de matemática, ocorrido em alguma competição na Alemanha. Notaram que os candidatos relacionaram a questão, com o Teorema 2.3.4, que é um resultado raramente encontrado nos livros didáticos.

Exemplo 2.3.1. (Olimpíada da Alemanha) Seja p um número primo. Prove que

$$\sum_{k=1}^{p-1}\left[\frac{k^3}{p}\right] = \frac{(p-2)(p-1)(p+1)}{4}.$$

Solução:

Seja $f(x) = x^3$ e p um primo qualquer.

Afirmação: $f(x)$ satisfaz as condições do Teorema 2.3.4.

Com efeito, suponha que, $p|f(x)$ com $1 \leq x \leq p-1$. Assim $p|x^3$. Como p é primo segue que $p|x$, o que implica que $p \leq x$. Como $1 \leq x \leq p-1 < p$, ou seja, $x < p$, temos uma contradição. Logo $p \not| f(k)$, com $k \in \{1, 2, 3, ..., p-1\}$.

Por outro lado

$$\begin{aligned} f(k) + f(p-k) &= k^3 + (p-k)^3 \\ f(k) + f(p-k) &= k^3 + p^3 - 3p^2k + 3pk^2 - k^3 \\ f(k) + f(p-k) &= p^3 - 3p^2k + 3pk^2 \\ f(k) + f(p-k) &= p(p^2 - 3pk + 3k^2) \end{aligned}$$

o que implica que $p|\big(f(k) + f(p-k)\big)$. Assim

$$\begin{aligned} \sum_{k=1}^{p-1}\left[\frac{k^3q}{p}\right] &= \frac{q}{p}\sum_{k=1}^{p-1}k^3 - \frac{p-1}{2} \\ \sum_{k=1}^{p-1}\left[\frac{k^3q}{p}\right] &= \frac{q}{p}\left(\frac{p(p-1)}{2}\right)^2 - \frac{p-1}{2} \\ \sum_{k=1}^{p-1}\left[\frac{k^3q}{p}\right] &= \frac{q}{p}.\frac{p^2(p-1)^2}{4} - \frac{p-1}{2} \\ \sum_{k=1}^{p-1}\left[\frac{k^3q}{p}\right] &= \frac{pq(p-1)^2}{4} - \frac{p-1}{2} \\ \sum_{k=1}^{p-1}\left[\frac{k^3q}{p}\right] &= (p-1)\left(\frac{pq(p-1)-2}{4}\right) \end{aligned}$$

$$\sum_{k=1}^{p-1}\left[\frac{k^3q}{p}\right] = \frac{(p-1)(p^2q-pq-2)}{4}.$$

Tomando $q=1$, obteremos:

$$\sum_{k=1}^{p-1}\left[\frac{k^3}{p}\right] = \frac{(p-1)(p^2-p-2)}{4}$$
$$\sum_{k=1}^{p-1}\left[\frac{k^3}{p}\right] = \frac{(p+1)(p-1)(p-2)}{4}.$$

Vejamos um outro exemplo, onde o Teorema 2.3.4, é de grande importância.

Exemplo 2.3.2. Seja p um primo ímpar. Mostre que

$$\sum_{k=1}^{p-1}\frac{k^p-k}{p} \equiv \frac{p+1}{2}(mod\ p).$$

Solução:
Considere a função $f(x)=\dfrac{x^p}{p}$. De forma análoga ao exemplo 2.3.1, mostra-se que $f(x)=\dfrac{x^p}{p}$ satisfaz as condições do Teorema 2.3.4. Assim

$$\sum_{k=1}^{p-1}\left[\frac{k^p}{p^2}\right] = \frac{1}{p}\sum_{k=1}^{p-1}\frac{k^p}{p}-\frac{p-1}{2}$$
$$\sum_{k=1}^{p-1}\left[\frac{k^p}{p^2}\right] = \frac{1}{p}\sum_{k=1}^{p-1}\frac{k^p}{p}-\frac{1}{p^2}\sum_{k=1}^{p-1}k+\frac{1}{p^2}\cdot\frac{(p-1)p}{2}-\frac{p-1}{2}$$
$$\sum_{k=1}^{p-1}\left[\frac{k^p}{p^2}\right] = \frac{1}{p}\sum_{k=1}^{p-1}\frac{k^p-k}{p}-\frac{1}{p}\cdot\frac{(p-1)^2}{2}$$

Então

$$p\sum_{k=1}^{p-1}\left[\frac{k^p}{p^2}\right]=\sum_{k=1}^{p-1}\frac{k^p-k}{p}-\frac{(p-1)^2}{2},$$

o que implica

$$\sum_{k=1}^{p-1}\frac{k^p-k}{p} \equiv \frac{(p-1)^2}{2}(mod\ p)$$

$$\sum_{k=1}^{p-1} \frac{k^p - k}{p} \equiv \frac{p^2+1}{2} (mod\ p)$$
$$\sum_{k=1}^{p-1} \frac{k^p - k}{p} \equiv \frac{p+1}{2} (mod\ p).$$

2.4 O produto de Dirichlet ou Convolução de Dirichlet.

Definição 2.4.1. *Sejam f e g funções aritméticas. Definimos como produto de Dirichlet de f e g, o qual denotaremos por $f * g$, como sendo:*

$$(f * g)(n) = \sum_{ab=n} f(a)g(b) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right).$$

Exemplo 2.4.1.

$(\sigma * \tau)(8) = \sum_{ab=8} \sigma(a)\tau(b)$
$(\sigma * \tau)(8) = \sigma(1)\tau(8) + \sigma(2)\tau(4) + \sigma(4)\tau(2) + \sigma(8)\tau(1)$
$(\sigma * \tau)(8) = 1 \cdot 4 + 3 \cdot 3 + 7 \cdot 2 + 15 \cdot 1$
$(\sigma * \tau)(8) = 42$

Exemplo 2.4.2.

$(\phi * \mu)(10) = \sum_{ab=10} \phi(a)\mu(b)$
$(\phi * \mu)(10) = \phi(1)\mu(10) + \phi(2)\mu(5) + \phi(5)\mu(2) + \phi(10)\mu(1)$
$(\phi * \mu)(10) = 1 \cdot (-1)^2 + 1 \cdot (-1)^1 + 4 \cdot (-1)^1 + 4 \cdot 1$
$(\phi * \mu)(10) = 1 - 1 - 4 + 4$
$(\phi * \mu)(10) = 0$

Propriedade 2.4.1. *Sejam f, g e h funções aritméticas. Então são válidas as seguintes propriedades:*

1) $f * g = g * f$ *(comutativa).*

2) $f * (g * h) = (f * g) * h$ *(associativa).*

1) Prova:

De fato

$$(f * g)(n) = \sum_{ab=n} f(a)g(b) = \sum_{ba=n} g(b)f(a) = (g * f)(n), \quad \forall n \in \mathbb{N}^*.$$

Logo $f * g = g * f$.

2) Prova:

De fato, tome $A = g * h$. Então, para todo $n \in \mathbb{N}^*$ temos:

$$[f*(g*h)](n) = (f*A)(n) = \sum_{ab=n} f(a)A(b) = \sum_{ab=n} f(a) \sum_{cd=b} g(c)h(d) = \sum_{acd=n} f(a)g(c)h(d). \ (*)$$

Por outro lado, tome $B = f * g$. Então, para todo $n \in \mathbb{N}^*$ temos

$$[(f * g) * h](n) = (B * h)(n) = \sum_{a_1b_1=n} B(a_1)h(b_1) = \sum_{a_1b_1=n} \Bigg(\sum_{a_2b_2=b_1} f(a_2)g(b_2) \Bigg) h(b_1)$$

$$[(f*g)*h](n) = \sum_{a_1a_2b_2=n} f(a_2)g(b_2)h(b_1). \qquad (**)$$

De $(*)$ e $(**)$, obtemos $[(f * g) * h](n) = [f * (g * h)](n)$; $\forall n \in \mathbb{N}^*$.
Logo $(f * g) * h = f * (g * h)$.

Definição 2.4.2. *Definiremos como função identidade para o produto de Dirichlet como sendo:*

$$I(n) = \left[\frac{1}{n}\right];\ n \in \mathbb{N}^*.$$

Observação 1) $I(1) = 1$ e $I(n) = 0;\ n \in \mathbb{N}$ com $n \geq 2$.

Observação 2) Para toda função aritmética f temos $f * I = I * f = f$.

Prova da observação 2:

De fato, tome $n \in \mathbb{N}^*$ qualquer. Seja $D(n) = \{1, a_1, ..., a_r, \frac{n}{a_r}, \frac{n}{a_{r-1}}, ..., \frac{n}{a_1}, n\}$ os divisores positivos de n. Deste modo

$$(f * g)(n) = \sum_{ab=n} f(a)I(b)$$

$$(f * g)(n) = f(1)I(n) + f(a_1)I(\frac{n}{a_1}) + f(a_2)I(\frac{n}{a_2}) + ... + f(a_{r-1})I(\frac{n}{a_{r-1}}) + f(a_r)I(\frac{n}{a_r}) +$$
$$+ f(\frac{n}{a_r})I(a_r) + ... + f(\frac{n}{a_1})I(a_1) + f(n)I(1)$$

$$(f * g)(n) = f(n)I(1) = f(n) \cdot 1 = f(n);\ \forall n \in \mathbb{N}^*.$$

Portanto $f * I = f$.

Definição 2.4.3. *Seja f uma função aritmética não nula, uma função g que satisfaz a propriedade $f * g = g * f = I$, é dita uma função inversa da f com respeito ao produto de Dirichlet.*

Teorema 2.4.1. *Se f é uma função aritmética com $f(1) \neq 0$, então existe uma única função aritmética f^{-1} chamada inversa convolutiva da função f definida da seguinte maneira:*

$$f * f^{-1} = f^{-1} * f = I.$$

Donde f^{-1} está dada pela fórmula de recorrência:

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

e

$$f^{-1}(n) = \frac{-1}{f(1)} \sum_{d|n;\ d<n} f\left(\frac{n}{d}\right) f^{-1}(d); \quad \forall n > 1.$$

Demonstração:

Mostraremos, por indução, que dada uma função aritmética f, a equação $(f * f^{-1})(n) = I(n)$ tem uma única solução para f^{-1} calculada em n.

Para $n = 1$, definimos $f(1)f^{-1}(1) = 1$.

Como $f(1) \neq 0$, então existe uma única solução dada: $f^{-1}(1) = \frac{1}{f(1)}$.

Para $n = 2$, temos

$$\begin{aligned}
(f^{-1} * f)(2) &= \sum_{d|2} f^{-1}(d) f\left(\frac{2}{d}\right) \\
(f^{-1} * f)(2) &= f^{-1}(1) f\left(\frac{2}{1}\right) + f^{-1}(2) f\left(\frac{2}{2}\right) \\
(f^{-1} * f)(2) &= \frac{1}{f(1)} f(2) + f^{-1}(2) f(1) \\
(f^{-1} * f)(2) &= \frac{f(2)}{f(1)} + f^{-1}(2) f(1)
\end{aligned}$$

Como $(f^{-1} * f)(n) = I(n)$ segue que $(f^{-1} * f)(2) = I(2) = 0$, ou seja,

$$\frac{f(2)}{f(1)} + f^{-1}(2) f(1) = 0$$

$$f^{-1}(2) f(1) = -f(2) f^{-1}(1)$$

$$f^{-1}(2) = -\frac{1}{f(1)} f(2) f^{-1}(1)$$

$$f^{-1}(2) = -\frac{1}{f(1)} \sum_{d|2;\ d<2} f\left(\frac{2}{d}\right) f^{-1}(d).$$

Suponhamos que a inversa convolutiva de f esteja definida para todo $m \in \mathbb{N}^*$ com $1 < m < n$.
Assim

$$0 = I(n) = (f^{-1} * f)(n) = \sum_{d|n} f^{-1}(d) f\left(\frac{n}{d}\right)$$

$$0 = f^{-1}(n) f\left(\frac{n}{n}\right) + \sum_{d|n;\ d<n} f^{-1}(d) f\left(\frac{n}{d}\right)$$

$$f^{-1}(n) f(1) = - \sum_{d|n;\ d<n} f^{-1}(d) f\left(\frac{n}{d}\right)$$

$$f^{-1}(n) = -\frac{1}{f(1)} \sum_{d|n;\ d<n} f^{-1}(d) f\left(\frac{n}{d}\right).$$

Deste modo fica estabelecido a existência e a unicidade de f^{-1} dada por indução matemática 2ª forma.

□

Proposição 2.4.1. *Sejam f e g funções aritméticas não nulas. Então* $(f*g)^{-1} = f^{-1}*g^{-1}$.

Prova:

De fato
$(f * g)^{-1} * (f * g) = I$
$(f * g)^{-1} * (f * g) * f^{-1} * g^{-1} = I * f^{-1} * g^{-1}$
$(f * g)^{-1} * ((f * f^{-1} * g * g^{-1}) = f^{-1} * g^{-1}$
$(f * g)^{-1} * I = f^{-1} * g^{-1}$
$(f * g)^{-1} = f^{-1} * g^{-1}$.

□

Lema 2.4.1. *Para todo inteiro positivo n temos*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{se } n = 1 \\ 0 & \text{se } n > 1. \end{cases}$$

Demonstração:

Para $n = 1$, nada o que provar. Como a função de Möbius é multiplicativa, pelo Teorema 2.1.1, $g(n) = \sum_{d|n} \mu(d)$ é uma função multiplicativa. Com isto, basta mostrar o lema para

$n = p^k$, onde p é um número primo.

Com efeito,

$$\sum_{d|p^k} \mu(d) = \sum_{j=0}^{k} \mu(p^j) = \mu(1) + \mu(p) + \mu(p^2) + ... + \mu(p^k)$$

$$\sum_{d|p^k} \mu(d) = 1 + (-1) = 0.$$

□

Observação: O lema acima nos diz que $\sum_{d|p^k} \mu(d) = \left[\frac{1}{n}\right] = I(n)$.

Lema 2.4.2. $\mu^{-1} = v$.

Demonstração:

$$(\mu * v)(n) = \sum_{d|n} \mu(d) v\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \cdot 1 = \sum_{d|n} \mu(d) = I(n);\ \forall n \geq 1.$$

Assim $\mu * v = I$. Portanto $\mu^{-1} = v$.

□

Teorema 2.4.2. *(Relação entre as funções de ϕ e μ) Para todo inteiro $n \geq 1$ temos*

$$\phi(n) = n \sum_{d|n} \frac{\mu(d)}{d}.$$

Demonstração:

Para todo $n \in \mathbb{N}$ com $n \geq 1$, tem-se:

$\phi(n) = (\phi * I)(n)$

$\phi(n) = [\phi * (v * \mu)](n)$

$\phi(n) = [(\phi * v) * \mu](n)$

$\phi(n) = \sum_{d|n} (\phi * v)(d).\mu\left(\frac{n}{d}\right)$

$\phi(n) = \sum_{d|n} \left(\sum_{q|d} \phi(q) v\left(\frac{d}{q}\right) \right) \mu\left(\frac{n}{d}\right)$

$\phi(n) = \sum_{d|n} \left(\sum_{q|d} \phi(q) \right) \mu\left(\frac{n}{d}\right)$

Pelo Teorema 2.1.5, segue que, $\sum_{q|d} \phi(q) = d$.

Assim

$$\phi(n) = \sum_{d|n} d \cdot \mu\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d)\frac{n}{d} = n\sum_{d|n} \frac{\mu(d)}{d}.$$

□

Teorema 2.4.3. *(Fórmula de Inversão de Möbius) Se duas funções aritméticas f e g satisfazem uma das duas condições*

$$f(n) = \sum_{d|n} g(d),\ \forall n \quad ou \quad g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right),\ \forall n,$$

então elas satisfazem as duas condições.

Demonstração:

Suponha que $f(n) = \sum_{d|n} g(d),\ \forall n$. Assim, podemos escrever:

$$\begin{aligned} f(n) &= \sum_{d|n} g(d) \cdot 1 \\ f(n) &= \sum_{d|n} g(d) v\left(\frac{n}{d}\right) \\ f(n) &= (g * v)(n) \end{aligned}$$

$$\begin{aligned} (f * \mu)(n) &= [(g * v) * \mu](n) \\ (f * \mu)(n) &= [g * (v * \mu)](n) \\ (f * \mu)(n) &= (g * I)(n) = g(n),\ \text{ou seja,} \\ g(n) &= \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right). \end{aligned}$$

Reciprocamente, suponha que $g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right)$.

Assim, podemos escrever:

$$\begin{aligned} g(n) &= (\mu * f)(n) \\ g(n) &= (\mu * f)(n) \\ (g * v)(n) &= [(f * \mu) * v](n) \\ (g * v)(n) &= [f * (\mu * v)](n) \\ (g * v)(n) &= (f * I)(n),\ \text{ou seja,} \end{aligned}$$

$$\begin{aligned} f(n) &= \sum_{d|n} g(d)v\left(\frac{n}{d}\right). \\ \text{Logo, } f(n) &= \sum_{d|n} g(d). \end{aligned}$$

□

Teorema 2.4.4. *Se f e g são duas funções multiplicativas, então $f * g$ também é multiplicativa.*

Demonstração:
Seja $h = f * g$. Assim, dados m e $n \in \mathbb{N}^*$ com $(m, n) = 1$, temos:

$$h(mn) = (f * g)(mn) = \sum_{d|mn} f(d)g\left(\frac{mn}{d}\right).$$

Pelo Teorema 1.1.4, cada divisor d de mn, pode ser representado na forma $d = ab$, onde $a|m$ e $b|n$ e $(a, b) = 1$. Assim

$$\begin{aligned} h(mn) &= \sum_{a|m;b|n} f(ab)g\left(\frac{mn}{ab}\right) \\ h(mn) &= \sum_{a|m;b|n} f(a)f(b)g\left(\frac{m}{a}\right)g\left(\frac{n}{b}\right) \\ h(mn) &= \left(\sum_{a|m} f(a)g\left(\frac{m}{a}\right)\right)\left(\sum_{b|n} f(b)g\left(\frac{n}{b}\right)\right) \\ h(mn) &= [(f * g)(m)] \cdot [(f * g)(n)] \\ h(mn) &= h(m)h(n). \end{aligned}$$

□

Teorema 2.4.5. *Seja f uma função multiplicativa não nula. f será completamente multiplicativa se, e somente se, $f^{-1}(n) = \mu(n)f(n)$.*

Demonstração:
($\Rightarrow$) Seja $g(n) = \mu(n)f(n)$. Assim

$$\begin{aligned} (f * g)(n) &= \sum_{d|n} f\left(\frac{n}{d}\right)g(d) = \sum_{d|n} f\left(\frac{n}{d}\right)\mu(d)f(d) \\ (f * g)(n) &= \sum_{d|n} \mu(d)f\left(\frac{n}{d}\right)f(d) = \sum_{d|n} \mu(d)f(n) \\ (f * g)(n) &= f(n)\sum_{d|n} \mu(d) = f(n)I(n). \end{aligned}$$

Como f é uma função multiplicativa não nula, segue que, $f(1) = 1 = I(1)$. Assim,

$$(f * g)(1) = f(1) = I(1) = 1 \text{ e } (f * g)(n) = f(n)I(n) = 0, \ \forall n > 1.$$

Deste modo, $(f * g)(n) = I(n); \ \forall n \in \mathbb{N}$.
Como a inversa convolutiva de f é única, segue que

$$f^{-1}(n) = g(n) = (\mu f)(n).$$

($\Leftarrow$) Reciprocamente, suponhamos que $f^{-1}(n) = \mu(n)f(n)$, onde f é uma função multiplicativa. Assim de $f^{-1}(n) = \mu(n)f(n)$ temos:

$$[f * (\mu.f)](n) = I(n)$$

$$[(\mu.f) * f](n) = I(n).$$

Assim

$$\sum_{d|n} \mu(d)f(d)f\left(\frac{n}{d}\right) = I(n).$$

Seja p um primo positivo qualquer.
Afirmação: $f(p^\alpha) = [f(p)]^\alpha, \ \forall \alpha \in \mathbb{N}^*$.
Faremos indução sobre α.
Para $\alpha = 2$ temos

$$\sum_{d|p^2} \mu(d)f(d)f\left(\frac{p^2}{d}\right) = I(p^2) = 0$$

$$\sum_{d|p^2} \mu(d)f(d)f\left(\frac{p^2}{d}\right) = \mu(1)f(1)f(p^2) + \mu(p)f(p)f\left(\frac{p^2}{p}\right) + \mu(p^2)f(p^2)f\left(\frac{p^2}{p^2}\right) = 0$$

$$f(p^2) + (-1)f(p)f(p) = 0 \ \Rightarrow \ f(p^2) = [f(p)]^2.$$

Suponha que a afirmação seja verdadeira para α. Assim

$$\sum_{d|p^{\alpha+1}} \mu(d)f(d)f\left(\frac{p^{\alpha+1}}{d}\right) = I(p^{\alpha+1}) = 0$$

$$\mu(1)f(1)f(p^{\alpha+1}) + \mu(p)f(p)f\left(\frac{p^{\alpha+1}}{p}\right) = 0$$

$$f(p^{\alpha+1}) + (-1)f(p)f(p^\alpha) = 0$$

$$f(p^{\alpha+1}) = f(p)f(p^\alpha)$$

Por hipótese, segue que

$$f(p^{\alpha+1}) = f(p)[f(p)]^\alpha$$

$$f(p^{\alpha+1}) = [f(p)]^{\alpha+1}.$$

Logo, pelo princípio de indução matemática 1ª forma, a afirmação é verdadeira para todo $\alpha \in \mathbb{N}^*$.

Sejam $m, n \in \mathbb{N}^*$ quaisquer, tais que a fatoração de m e n são dadas por:
$m = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$ e $n = p_1^{\beta_1} p_2^{\beta_2} ... p_r^{\beta_r}$.
Assim

$$\begin{aligned}
f(mn) &= f(p_1^{\alpha_1+\beta_1} p_2^{\alpha_2+\beta_2} ... p_r^{\alpha_r+\beta_r}) \\
f(mn) &= f(p_1^{\alpha_1+\beta_1}) f(p_2^{\alpha_2+\beta_2}) ... f(p_r^{\alpha_r+\beta_r}) \\
f(mn) &= [f(p_1)]^{\alpha_1+\beta_1} [f(p_2)]^{\alpha_2+\beta_2} ... [f(p_r)]^{\alpha_r+\beta_r} \\
f(mn) &= [f(p_1)]^{\alpha_1} [f(p_2)]^{\alpha_2} ... [f(p_r)]^{\alpha_r} [f(p_1)]^{\beta_1} [f(p_2)]^{\beta_2} ... [f(p_r)]^{\beta_r} \\
f(mn) &= f(p_1^{\alpha_1}) f(p_2^{\alpha_2}) ... f(p_r^{\alpha_r}) f(p_1^{\beta_1}) f(p_2^{\beta_2}) ... f(p_r^{\beta_r}) \\
f(mn) &= f(p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}) f(p_1^{\beta_1} p_2^{\beta_2} ... p_r^{\beta_r}) \\
f(mn) &= f(m) f(n).
\end{aligned}$$

Portanto f é completamente multiplicativa.

□

Corolário 2.4.1. $N^{-1} = \mu.N$

Demonstração.
Notemos que, $N = Id$ é completamente multiplicativa. Portanto o resultado segue do Teorema 2.4.5. □

Lema 2.4.3. *(Inversa convolutiva da função ϕ de Euler)*

$$\phi^{-1}(n) = \sum_{d|n} d\mu(d).$$

Demonstração:
Notemos que

$$(\phi * v)(n) = \sum_{d|n} \phi(d) v\left(\frac{n}{d}\right)$$

$$(\phi * v)(n) = \sum_{d|n} \phi(d)$$

$$(\phi * v)(n) = n$$

$$(\phi * v)(n) = N(n); \quad \forall n \in \mathbb{N}^*.$$

Daí

$$\phi * v = N$$

$$\phi = N * v^{-1}$$

$$\phi = N * \mu$$

$$\phi^{-1} = (N * \mu)^{-1}$$

$$\phi^{-1} = \mu^{-1} * N^{-1}$$

$$\phi^{-1} = v * (\mu.N)$$

Deste modo, para qualquer $n \in \mathbb{N}^*$ temos

$$\phi^{-1}(n) = [(\mu.N) * v](n)$$

$$\phi^{-1}(n) = \sum_{d|n} (\mu.N)(d) v\left(\frac{n}{d}\right)$$

$$\phi^{-1}(n) = \sum_{d|n} \mu(d) N(d).1$$

$$\phi^{-1}(n) = \sum_{d|n} d\mu(d). \qquad \square$$

Proposição 2.4.2. *Se f é uma função multiplicativa então*

$$\sum_{d|n} \mu(d) f(d) = \prod_{p|n;\ p\ primo} (1 - f(p)).$$

Demonstração:

Seja g a função multiplicativa definida por

$$g(n) = \sum_{d|n} \mu(d) f(d)$$

Considere, $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$. Assim

$$\begin{aligned} g(n) &= g(p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}) \\ g(n) &= g(p_1^{\alpha_1}) g(p_2^{\alpha_2}) ... g(p_r^{\alpha_r}) \\ g(n) &= \sum_{d|p_1^{\alpha_1}} \mu(d) f(d). \sum_{d|p_2^{\alpha_2}} \mu(d) f(d) ... \sum_{d|p_r^{\alpha_r}} \mu(d) f(d) \end{aligned}$$

$$\begin{aligned} g(n) &= (\mu(1)f(1)+\mu(p_1)f(p_1))(\mu(1)f(1)+\mu(p_2)f(p_2))...(\mu(1)f(1)+\mu(p_r)f(p_r)) \\ g(n) &= (1-f(p_1))(1-f(p_2))...(1-f(p_r)) \\ \sum_{d|n}\mu(d)f(d) &= \prod_{p|n;\ p\ primo}(1-f(p)). \end{aligned}$$

□

Corolário 2.4.2. $\phi^{-1}(n) = \prod_{p|n;\ p\ primo}(1-p)$.

Demonstração:

Tome $f = N$. Assim

$$\sum_{d|n}\mu(d)f(d) = \sum_{d|n}\mu(d)N(d) = \prod_{p|n;\ p\ primo}(1-N(p)) = \prod_{p|n;\ p\ primo}(1-p).$$

Como

$$\sum_{d|n}\mu(d)N(d) = \sum_{d|n}d\mu(d) = \phi^{-1}(n)$$

segue que

$$\phi^{-1}(n) = \prod_{p|n;\ p\ primo}(1-p).$$

□

3 Resíduos Quadráticos

Neste capítulo, apresentaremos a "Lei da Reciprocidade Quadrática de Gauss", que teve a primeira demonstração feita por Gauss em 1796, aos dezoito anos e encontra-se no livro *Desquisitiones Arithmeticae*. Este resultado já era conhecido por Fermat, Euler e Legendre.

Em 1785, Legendre publicou uma demonstração deficiente. Contam que Gauss forneceu pelo menos 8 demonstrações e a literatura, até o momento, menciona 221 demonstrações.

3.1 Congruência Quadrática

Vamos considerar a congruência quadrática,

$$Ax^2 + Bx + C \equiv 0(mod\ p) \tag{3.1}$$

onde p é um número primo ímpar e $p \nmid A$ (se $p|A$, então a congruência acima se reduz a congruência linear). Sendo p ímpar e $p \nmid A$ então $p \nmid 4A$.
Multiplicando ambos os membros da congruência acima por $4A$, obteremos:

$$4A(Ax^2 + Bx + C) \equiv 0(mod\ p). \tag{3.2}$$

No entanto

$$4A(Ax^2 + Bx + C) = 4A^2x^2 + 4ABx + 4AC = (2Ax + B)^2 - (B^2 - 4AC).$$

Deste modo, podemos reescrever a congruência (3.1) como

$$(2Ax + B)^2 \equiv (B^2 - 4AC)(mod\ p),$$

na qual é da forma $y^2 \equiv a(mod\ p)$, onde $y = 2Ax + B$ e $a = B^2 - 4AC$. Deste modo tem-se que a congruência (3.1) possui solução se, e somente se, a congruência $y^2 \equiv a(mod\ p)$ também possui.

Exemplo 3.1.1. Resolva a congruência $3x^2 - 4x + 7 \equiv 0(mod\ 13)$.

Solução:

$$\begin{aligned} 3x^2 - 4x + 7 &\equiv 0(mod\ 13) \\ 36x^2 - 48x + 84 &\equiv 0(mod\ 13) \\ (6x - 4)^2 &\equiv (16 - 84)(mod\ 13) \\ (6x - 4)^2 &\equiv 10(mod\ 13). \end{aligned}$$

Tome $y = 6x - 4$. Então

$$y^2 \equiv 10(mod\ 13).$$

Como

$$1^2 \equiv 1(mod\ 13)$$

$$2^2 \equiv 4(mod\ 13)$$

$$3^2 \equiv 9(mod\ 13)$$

$$4^2 \equiv 3(mod\ 13)$$

$$5^2 \equiv 12(mod\ 13)$$

$$6^2 \equiv 10(mod\ 13)$$

$$7^2 \equiv 10(mod\ 13)$$

$$8^2 \equiv 12(mod\ 13)$$

$$9^2 \equiv 3(mod\ 13)$$

$$10^2 \equiv 9(mod\ 13)$$

$$11^2 \equiv 4(mod\ 13)$$

$$12^2 \equiv 1(mod\ 13).$$

Segue que $y \equiv 6(mod\ 13)$ e $y \equiv 7(mod\ 13)$, são as soluções de $y^2 \equiv 10(mod\ 13)$. Assim $6x - 4 \equiv 6(mod\ 13)$ e $6x - 4 \equiv 7(mod\ 13)$.

Deste modo

$$6x - 4 \equiv 6(mod\ 13) \Rightarrow 6x \equiv 10(mod\ 13) \Rightarrow 6x \equiv 36(mod\ 13) \Rightarrow x \equiv 6(mod\ 13).$$

Analogamente

$$6x - 4 \equiv 7(mod\ 13) \Rightarrow 6x \equiv 11(mod\ 13) \Rightarrow 6x \equiv 24(mod\ 13) \Rightarrow x \equiv 4(mod\ 13).$$

Note que a congruência quadrática acima possui exatamente duas soluções incongruentes módulo p. No entanto, nem toda congruência quadrática admite solução.

Exemplo 3.1.2. Resolva, se possível, a congruência quadrática $3x^2+7x+5 \equiv 0(mod\ 13)$.

Solução:

$$3x^2 + 7x + 5 \equiv 0(mod\ 13) \Rightarrow 36x^2 + 84x + 60 \equiv 0(mod\ 13) \Rightarrow (6x + 7)^2 \equiv -11(mod\ 13)$$

$$\Rightarrow (6x + 7)^2 \equiv 2(mod\ 13).$$

Tome $y = 6x + 7$. Assim $y^2 \equiv 2(mod\ 13)$.
Por outro lado, dado $a \in \mathbb{Z}$ qualquer, tem-se que

$$a \equiv i(mod\ 13)$$

onde $i \in \{0, 1, 2, ..., 12\}$. Facilmente, note-se que, pela lista de congruência do Ex.: 3.1.1,

$$a^2 \not\equiv 2(mod\ 13).$$

Portanto a congruência quadrática $y^2 \equiv 2(mod\ 13)$ não possui solução e consequentemente $3x^2 + 7x + 5 \equiv 0(mod\ 13)$ não admite solução.

Teorema 3.1.1. *Para p primo ímpar e $a \in \mathbb{Z}$ tal que $(a, p) = 1$, a congruência*

$$x^2 \equiv a(mod\ p)$$

caso tenha solução, tem exatamente duas soluções incongruentes módulo p.

Demonstração:
Suponha que a congruência dada tenha uma solução x_1. É claro que $-x_1$ também será uma solução, pois, $(-x_1)^2 = x_1^2 \equiv a(mod\ p)$.
Afirmação 1) $x_1 \not\equiv -x_1(mod\ p)$. De fato, se $x_1 \equiv -x_1(mod\ p)$, então $2x_1 \equiv 0(mod\ p)$, ou seja, $p|2x_1$. Como p é primo ímpar, segue que $p|x_1$. Deste modo $p|x_1^2$.

Por outro lado, de $x_1^2 \equiv a(mod\ p)$, segue que, $p|(x_1^2 - a)$. Como $p|x_1^2$, segue que $p|a$, o que é um absurdo, pois $(a, p) = 1$.

Afirmação 2) A congruência $x^2 \equiv a(mod\ p)$, admite apenas duas soluções incongruentes módulo p. Com efeito, seja y uma solução de $x^2 \equiv a(mod\ p)$. Assim $y^2 \equiv a(mod\ p)$. Como x_1 é solução, temos

$$x_1^2 \equiv y^2 \equiv a(mod\ p)$$

$$x_1^2 - y^2 = (x_1 - y)(x_1 + y) \equiv 0(mod\ p).$$

Logo $p|(x_1 - y)$ ou $p|(x_1 + y)$.

Daí $y \equiv x_1(mod\ p)$ ou $y \equiv -x_1(mod\ p)$.

Portanto, caso exista solução, existem apenas duas soluções incongruentes módulo p.

□

Teorema 3.1.2. *(Lagrange) Seja $f(x) = c_n x^n + c_{n-1}x^{n-1} + ... + c_1 x + c_0$ um polinômio com coeficientes inteiros, p um número primo tal que $(c_n, p) = 1$. Então a congruência $f(x) \equiv 0(mod\ p)$, possui no máximo n soluções incongruentes módulo p.*

Demonstração:

Faremos indução sobre n=grau$(f(x))$. Se $n = 1$ teremos

$$f(x) = c_1 x + c_0 \equiv 0(mod\ p),\ \text{com}\ (c_1, p) = 1.$$

Assim $c_1 x \equiv -c_0(mod\ p)$. Como $(c_1, p) = 1$ e $1|(-c_0)$, então a congruência linear admite uma única solução incongruente módulo p. Deste modo o resultado é verdadeiro para $n = 1$.

Suponhamos que o resultado seja válido para qualquer polinômio com coeficientes inteiros $h(x)$ com grau$(h(x)) = n - 1$.

Queremos mostrar que a afirmação é verdadeira para polinômios de grau n.

Com efeito, suponha que $f(x)$ é um polinômio com coeficientes inteiros, com grau$(f(x)) = n$, possua $n + 1$ soluções incongruentes módulo p. Sejam $x_0, x_1, x_2, ..., x_n$ soluções incongruentes módulo p da congruência $f(x) \equiv 0(mod\ p)$. Notemos que

$$\begin{aligned} f(x) - f(x_0) &= (c_n x^n + c_{n-1}x^{n-1} + ... + c_1 x + c_0) - (c_n x_0^n + c_{n-1}x_0^{n-1} + ... + c_1 x_0 + c_0) \\ f(x) - f(x_0) &= c_n(x^n - x_0^n) + c_{n-1}(x^{n-1} - x_0^{n-1}) + ... + c_1(x - x_0). \end{aligned}$$

Como $(x - x_0)|(x^i - x_0^i)$, segue que $x^i - x_0^i = (x - x_0)l_i(x)$, para algum polinômio com coeficientes inteiros $l_i(x)$. Onde $i \in \{1, 2, 3, ..., n\}$.

Assim

$$f(x) - f(x_0) = c_n(x - x_0)l_n(x) + c_{n-1}(x - x_0)l_{n-1}(x) + ... + c_1(x - x_0).$$

Deste modo, podemos escrever

$$f(x) - f(x_0) = (x - x_0)l(x)$$

onde $l(x)$ é um polinômio com coeficientes inteiros de grau $n-1$, tendo como coeficiente líder c_n.
Desta forma

$$f(x_k) - f(x_0) = (x_k - x_0)l(x_k) \equiv 0(mod\ p),$$

ou seja, $(x_k - x_0)l(x_k) \equiv 0(mod\ p)$, com $k \in \{1, 2, 3, ..., n\}$.
Como $x_k \not\equiv x_0(mod\ p)$, para $k \in \{1, 2, 3, ..., n\}$, então $(x_k - x_0, p) = 1$. Logo

$$(x_k - x_0)l(x_k) \equiv 0(mod\ p) \Rightarrow l(x_k) \equiv 0(mod\ p),\ \text{com}\ k \in \{1, 2, ..., n\}.$$

Isto implica que $l(x)$ é um polinômio com coeficientes inteiros de grau $n-1$, na qual, a equação $l(x) \equiv 0(mod\ p)$ possui n soluções incongruentes módulo p, o que é uma contradição, com a hipótese de indução. Portanto $f(x) \equiv 0(mod\ p)$ admite no máximo n soluções incongruentes módulo p.
Assim pelo principio de Indução Matemática Primeira Forma, concluímos o resultado desejado.

□

Observação: Se grau$(f(x)) = n > p$, então a congruência $f(x) \equiv 0(mod\ p)$ admite no máximo p soluções incongruentes módulo p.
De fato, isto ocorre devido ao fato de um sistema completo de resíduos módulo p qualquer possuir p elementos.

Teorema 3.1.3. *Seja $f(x) = c_nx^n + c_{n-1}x^{n-1} + ... + c_1x + c_0$ um polinômio de grau n com coeficientes inteiros. Se a congruência $f(x) \equiv 0(mod\ p)$, possui mais do que n soluções, onde p é um número primo, então $p|c_j$ com $j \in \{0, 1, 2, ..., n\}$.*

Demonstração:
Suponha que exista um coeficiente de $f(x)$ que não seja divisível por p. Seja j o maior índice para o qual $p \nmid c_j$.
Assim

$$c_nx^n + c_{n-1}x^{n-1} + ... + c_1x + c_0 \equiv 0(mod\ p)$$

é equivalente a

$$c_j x^j + c_{j-1}x^{j-1} + ... + c_1 x + c_0 \equiv 0(mod\ p).$$

Por outro lado, como

$$c_j x^j + c_{j-1}x^{j-1} + ... + c_1 x + c_0 \equiv 0(mod\ p)$$

onde $(c_j, p) = 1$, uma vez que, p é primo e $p \nmid c_j$. Assim, pelo Teorema de Lagrange, segue que, tal congruência admitirá no máximo $j \leq n$ soluções incongruentes módulo p, ou seja, $f(x) \equiv 0(mod\ p)$ possui no máximo $j \leq n$ soluções incongruentes módulo p, o que é uma contradição. Portanto $p|c_j$ para $j \in \{0, 1, 2, ..., n\}$.

□

Definição 3.1.1. *Sejam a e m inteiros com $m > 0$ e $(a, m) = 1$. Dizemos que a é um resíduo quadrático módulo m se a congruência $x^2 \equiv a(mod\ m)$ possuir solução. Caso $x^2 \equiv a(mod\ m)$ não tenha solução, dizemos que a não é um resíduo quadrático módulo m ou que a é um resíduo não quadrático.*

Exemplo 3.1.3. 3 é um resíduo quadrático módulo 13, pois $4^2 \equiv 3(mod\ 13)$.

Exemplo 3.1.4. 2 é um resíduo quadrático módulo 7, pois $4^2 \equiv 2(mod\ 7)$.

3.2 Símbolo de Legendre e o Critério de Euler

Definição 3.2.1. *Seja p um primo ímpar positivo. O simbolo de Legendre é definido por:*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{se } a \text{ é um resíduo quadrático módulo } p \\ -1 & \text{se } a \text{ é um resíduo não quadrático módulo } p \\ 0 & \text{se } p|a. \end{cases}$$

Observação: $\left(\frac{a^2}{p}\right) = 1$, pois a é solução da congruência $x^2 \equiv a^2(mod\ p)$. Em particular $\left(\frac{1}{p}\right) = 1$.

Exemplo 3.2.1. Como

$$1^2 \equiv 1(mod\ 7)$$

$$2^2 \equiv 4(mod\ 7)$$

$$3^2 \equiv 2(mod\ 7)$$

$$4^2 \equiv 2(mod\ 7)$$

$$5^2 \equiv 4(mod\ 7)$$

$$6^2 \equiv 1(mod\ 7)$$

seque que

$$\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = 1$$

e

$$\left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1$$

Teorema 3.2.1. *Seja p um primo ímpar positivo. Então*

i) Se $(a,p) = (b,p) = 1$ e $a \equiv b(mod\ p)$, então $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
ii) Dentre os números do conjunto $\{1, 2, ..., p-1\}$, $\frac{p-1}{2}$ destes são resíduos quadráticos módulo p e $\frac{p-1}{2}$ não são.

Demonstração:

i) Como $a \equiv b(mod\ p)$, segue imediatamente que a congruência $x^2 \equiv a(mod\ p)$ admite solução se, e somente se, $x^2 \equiv b(mod\ p)$ também admite solução. Portanto $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

ii) Como $\{1, 2, 3, ..., p-1\}$ é um sistema reduzido de resíduos módulo p, para contarmos a quantidade de elementos de $\{1, 2, 3, ..., p-1\}$ que são resíduos quadráticos módulo p, basta calcular, quantos dentre os números $1^2, 2^2, 3^2, ..., (p-1)^2$ são dois a dois incongruentes módulo p. No entanto, notemos que $1 \leq i \leq \frac{p-1}{2}$, então $i^2 \equiv (p-1)^2(mod\ p)$.

Por outro lado, se $1 \leq i < j \leq \frac{p-1}{2}$, então $i^2 \not\equiv j^2(mod\ p)$, uma vez que

$$j^2 - i^2 = (j-i)(j+i) \text{ e } 0 < j-i < j+i < p.$$

Logo, existem exatamente $\frac{p-1}{2}$ resíduos quadráticos módulo p e daí existem

$$p - \frac{(p-1)}{2} = \frac{p-1}{2} \text{ resíduos não quadráticos módulo } p.$$

□

Teorema 3.2.2. *(Critério de Euler) Seja p um primo positivo ímpar e seja $a \in \mathbb{Z}$ tal que $p \nmid a$. Então a é um resíduo quadrático módulo p se, e somente se, $a^{\frac{p-1}{2}} \equiv 1(mod\ p)$.*

Demonstração:

Sendo $\left(\frac{a}{p}\right) = 1$, então a congruência $x^2 \equiv a(mod\ p)$ admite uma solução b.

Como $(b, p) = 1$, pelo Pequeno Teorema de Fermat, obtemos

$$a^{\frac{p-1}{2}} \equiv (b^2)^{\frac{p-1}{2}} = b^{p-1} \equiv 1(mod\ p).$$

Assim, $a^{\frac{p-1}{2}} \equiv 1(mod\ p)$.
Reciprocamente, suponha que $\left(\frac{a}{p}\right) = -1$.
Afirmação 1) $(p-1)! \equiv a^{\frac{p-1}{2}}(mod\ p)$.
De fato, neste caso para cada $a_0 < p$, a congruência $a_0 x \equiv a(mod\ p)$ admite uma solução x_0, $1 \leq x_0 < p$ e $x_0 \neq a_0$, pois $\left(\frac{a}{p}\right) = -1$. Daí segue que os fatores de $(p-1)!$ podem ser agrupados dois a dois, sem exceção, de maneira que, cada um dos produtos resultantes seja côngruo ao número a, módulo p. Sendo $p-1$ os fatores então

$$(p-1)! \equiv a^{\frac{p-1}{2}}(mod\ p).$$

Com base na afirmação demonstrada e no fato que $a^{\frac{p-1}{2}} \equiv 1(mod\ p)$, por hipótese, segue que $(p-1)! \equiv 1(mod\ p)$.
Mas em virtude do Teorema de Wilson, temos $(p-1)! \equiv -1(mod\ p)$, o que nos leva a concluir, que $1 \equiv -1(mod\ p)$, o que não é possível, pois por hipótese, $p > 2$.

□

Corolário 3.2.1. *Seja p um primo ímpar positivo e $p \nmid a$ então,* $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}(mod\ p)$.

Demonstração. Se a é um resíduo quadrático módulo p, então $a^{\frac{p-1}{2}} \equiv 1(mod\ p)$ e $\left(\frac{a}{p}\right) = 1$. Assim $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}(mod\ p)$.

Caso a não seja resíduo não quadrático módulo p, pelo Teorema 3.2.2, temos $a^{\frac{p-1}{2}} \not\equiv 1(mod\ p)$. Como $a^{p-1} - 1 = (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1)$ e $a^{p-1} - 1 \equiv 1(mod\ p)$, para $(a, p) = 1$, concluímos que $a^{\frac{p-1}{2}} \equiv \pm 1(mod\ p)$. Logo, caso $\left(\frac{a}{p}\right) = -1$, deveremos ter

$$a^{\frac{p-1}{2}} \equiv -1(mod\ p),$$

ou seja, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}(mod\ p)$.

□

Corolário 3.2.2. *Seja p um primo ímpar positivo, onde $p \nmid a$, $p \nmid b$, então*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Demonstração:

Pelo critério de Euler temos

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} (mod\ p).$$

ou seja

$$\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) (mod\ p).$$

Como p é primo ímpar positivo e os valores do símbolo de Legendre são 1 ou -1, segue que

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

□

Corolário 3.2.3. *Se p é um primo ímpar positivo, então* $\left(\frac{-1}{p}\right) = 1 \Leftrightarrow p \equiv 1(mod\ 4)$.

Demonstração

Pelo critério de Euler temos

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} (mod\ p).$$

Como por hipótese $\left(\frac{-1}{p}\right) = 1$, segue que $(-1)^{\frac{p-1}{2}} \equiv 1(mod\ p)$. Assim $\frac{p-1}{2} = 2r$ para algum $r \in \mathbb{Z}$. Isto implica que $p = 4r + 1$, ou seja, $p \equiv 1(mod\ 4)$.

Reciprocamente, suponha que $p \equiv 1(mod\ 4)$. Assim existe $l \in \mathbb{Z}$, tal que, $p - 1 = 4l$. Daí $\frac{p-1}{2} = 2l$. Portanto, pelo critério de Euler temos

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} = (-1)^{2l} \equiv 1(mod\ p),$$

ou seja, $\left(\frac{-1}{p}\right) \equiv 1(mod\, p)$. Portanto $\left(\frac{-1}{p}\right) = 1$. □

Corolário 3.2.4. *Se p é um primo ímpar positivo, então* $\left(\frac{-1}{p}\right) = -1 \Leftrightarrow p \equiv 3(mod\ 4)$.

Demonstração:

Decorre do Corolário 3.2.3. □

Exemplo 3.2.2. Mostre que não existem x e y inteiros tais que $y^2 = x^3 + 7$.

Solução:

Suponhamos, por absurdo, que existam $x, y \in \mathbb{Z}$ tais que $y^2 = x^3 + 7$.
Se x é par, então $4|x^3$. Deste modo

$$y^2 \equiv 7(mod\ 4)$$

$$y^2 \equiv 3(mod\ 4),$$

o que é um absurdo. Assim x é ímpar.

Por outro lado

$$y^2 + 1 = x^3 + 8 = (x + 2)(x^2 - 2x + 4)$$

$$y^2 + 1 = x^3 + 8 = (x + 2)[(x - 1)^2 + 3]$$

Como $x - 1$ é par então $4|(x - 1)^2$, o que implica que $(x - 1)^2 + 3 \equiv 3(mod\ 4)$. Assim $a = (x-1)^2+3$ é um número da forma $4l+3$. Pelo Teorema Fundamental da Aritmética, existe q primo tal que $q|a$. Como $q \equiv 1(mod\ 4)$ ou $q \equiv 3(mod\ 4)$, a é da forma $4l + 3$ e o produto de elementos da forma $4l + 1$ resulta em um número da mesma forma, então existe um número primo p da forma $4k + 3$ tal que $p|[(x - 1)^2 + 3]$.
Como $y^2+1 = (x+2)[(x-1)^2+3]$, segue que $y^2+1 \equiv 0(mod\ p)$, isto é, $y^2 \equiv -1(mod\ p)$. Assim y é solução da congruência quadrática $b^2 \equiv -1(mod\ p)$. Logo $\left(\frac{-1}{p}\right) = 1$. $(*)$
No entanto, pelo critério de Euler temos

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}}(mod\ p).$$

Como $p = 4k + 3$ para algum $k \in \mathbb{Z}$, segue que, $\frac{p-1}{2} = 2k + 1$. Assim

$$\left(\frac{-1}{p}\right) \equiv -1(mod\ p). \qquad (**)$$

De $(*)$ e $(**)$, obtemos $1 \equiv -1(mod\ p)$ onde p é um primo ímpar, o que é um absurdo!
Portanto não existem $x, y \in \mathbb{Z}$ tais que $y^2 = x^3 + 7$.

Exemplo 3.2.3. Mostre que existem infinitos primos da forma $4n + 1$ com $n \in \mathbb{N}$.

Solução:

Suponhamos que $S = \{p_1 = 5, p_2 = 13, p_3, ..., p_r\}$ seja o conjunto de todos os primos da

forma $4k+1$.

Consideremos o número $N=(2p_1p_2...p_r)^2+1$. Pelo Teorema Fundamental da Aritmética, existe q primo tal que $q|N$. Assim

$$(2p_1p_2...p_r)^2+1 \equiv 0(mod\ q)$$

Isto significa que a congruência $x^2 \equiv -1(mod\ q)$ admite solução. Pelo corolário 3.2.3, segue que $q \equiv 1(mod\ 4)$. Assim $q \in S$, e consequentemente $q|1$, o que é um absurdo! Portanto existem infinitos números primos da forma $4n+1$ com $n \in \mathbb{N}$.

Teorema 3.2.3. *Se p é um primo ímpar positivo, então*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & se\ p \equiv \pm 1(mod\ 8) \\ -1 & se\ p \equiv \pm 3(mod\ 8). \end{cases}$$

Demonstração:

Pelo critério de Euler temos

$$\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}}(mod\ p). \qquad (*)$$

Como p é primo ímpar temos as seguintes possibilidades:

i) $p \equiv 1(mod\ 8)$.

Neste caso $p=1+8l$ para algum $l \in \mathbb{Z}$. Assim $p+1=2+8l$.

Logo

$$\frac{p^2-1}{8} = \frac{(p+1)(p-1)}{8} = \frac{(8l+2)(8l)}{8} = 8l^2+2l = 2l(4l+1).$$

ii) $p \equiv 7(mod\ 8)$.

Neste caso $p=7+8r$ para algum $r \in \mathbb{Z}$. Daí $p+1=8+8r$.

Logo

$$\frac{p^2-1}{8} = \frac{(p+1)(p-1)}{8} = \frac{8(r+1)(6+8r)}{8} = 2(3+4r)(r+1).$$

Logo, se $p \equiv \pm 1(mod\ 8)$, temos que, $\dfrac{p^2-1}{8}$ é um número par.

iii) $p \equiv 3(mod\ 8)$.

Neste caso $p=3+8s$ para algum $s \in \mathbb{Z}$. Daí $p+1=4+8s$.

Logo

$$\frac{p^2-1}{8} = \frac{(p+1)(p-1)}{8} = \frac{(4+8s)(2+8s)}{8} = \frac{4(1+2s)2(1+4s)}{8} = (2s+1)(4s+1).$$

iv) $p \equiv 5(mod\ 8)$

Neste caso, $p = 5 + 8t$ para algum $t \in \mathbb{Z}$. Assim $p + 1 = 6 + 8t$.

Logo

$$\frac{p^2-1}{8} = \frac{(p+1)(p-1)}{8} = \frac{(6+8t)(4+8t)}{8} = \frac{2(3+4t)4(1+2t)}{8} = (2t+1)(4t++3).$$

Portanto, se $p \equiv \pm 3(mod\ 8)$ então $\frac{p^2-1}{8}$ é um número ímpar.

Notemos que, se i é ímpar

$$p - i \equiv -i(mod\ p)$$

$$p - i \equiv i(-1)^i(mod\ p)$$

e se i é par então

$$i \equiv i(-1)^i(mod\ p).$$

Logo se consideramos as $\frac{p-1}{2}$ congruências

$$p - 1 \equiv 1(-1)^1(mod\ p)$$

$$2 \equiv 2(-1)^2(mod\ p)$$

$$p - 3 \equiv 3(-1)^3(mod\ p)$$

$$4 \equiv 4(-1)^4(mod\ p)$$

$$p - 5 \equiv 5(-1)^5(mod\ p)$$

$$\vdots$$

$$t \equiv \frac{p-1}{2}(-1)^{\frac{p-1}{2}}(mod\ p)$$

Caso tenhamos $\frac{p-1}{2}$ um número par então $t = \frac{p-1}{2} \equiv \frac{p-1}{2}(-1)^{\frac{p-1}{2}}(mod\ p)$.

Caso contrário, teremos $t = p - \frac{p-1}{2} \equiv \frac{p-1}{2}(-1)^{\frac{p-1}{2}}(mod\ p)$.

É de fácil observação que os números na coluna da esquerda, das congruências acima, são números pares.

Como existem $\frac{p-1}{2}$ números pares então $\{p-1, 2, p-3, 4, ..., t\} = \{2, 4, 6, 8, ..., p-1\}$.

Multiplicando, membro a membro, todas as congruências teremos

$$\begin{aligned} 2 \cdot 4 \cdot 6 \cdot 8...(p-1) &\equiv \left(\frac{p-1}{2}\right)!(-1)^{1+2+3+...+\frac{p-1}{2}}(mod\ p) \\ 2 \cdot 4 \cdot 6 \cdot 8...(p-1) &\equiv \left(\frac{p-1}{2}\right)!(-1)^{\frac{p^2-1}{8}}(mod\ p). \end{aligned}$$

No entanto

$$\begin{aligned} 2\cdot 4\cdot 6\cdot 8...(p-1) &= 2^{\frac{p-1}{2}}\left(1\cdot 2\cdot 3...\frac{p-1}{2}\right) \\ 2\cdot 4\cdot 6\cdot 8...(p-1) &= 2^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!. \end{aligned}$$

Logo

$$\begin{aligned} 2^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! &\equiv (-1)^{\frac{p^2-1}{8}}\left(\frac{p-1}{2}\right)!(mod\ p) \\ 2^{\frac{p-1}{2}} &\equiv (-1)^{\frac{p^2-1}{8}}(mod\ p). \end{aligned} \qquad (**)$$

De $(*)$ e $(**)$, concluímos que, $\left(\frac{2}{p}\right) \equiv (-1)^{\frac{p^2-1}{8}}(mod\ p)$.

Logo, se $p \equiv \pm 1(mod\ 8)$, então $\frac{p^2-1}{8}$ é par e consequentemente, $\left(\frac{2}{p}\right) = 1$.
Se $p \equiv \pm 3(mod\ 8)$, então $\frac{p^2-1}{8}$ é ímpar e consequentemente, $\left(\frac{2}{p}\right) = -1$.
Portanto

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{se } p \equiv \pm 1(mod\ 8) \\ -1 & \text{se } p \equiv \pm 3(mod\ 8). \end{cases}$$

□

Exemplo 3.2.4. Mostre que $9973|(2^{4986}+1)$.

Solução:
É fácil verificar que 9973 é um número primo utilizando o (crivo de Eratóstenes) e que

$9973 \equiv 5(mod\ 8)$. Pelo Teorema 3.2.3, segue que $\left(\frac{2}{9973}\right) = -1$ $(*)$

Por outro lado, pelo critério de Euler temos

$$\left(\frac{2}{9973}\right) \equiv 2^{\frac{9973-1}{2}}(mod\ 9973),$$

ou seja,

$$\left(\frac{2}{9973}\right) \equiv 2^{4986}(mod\ 9973). \qquad (**)$$

De $(*)$ e $(**)$, concluímos que $2^{4986} \equiv -1(mod\ 9973)$. Portanto $9973|(2^{4986}+1)$.

3.3 Lema de Gauss e Lei da Reciprocidade Quadrática

Lema 3.3.1. *(Lema de Gauss): Sejam $p, a \in \mathbb{N}^*$ com p primo ímpar e $(a,p)=1$. Sejam $r_1, r_2, ..., r_{\frac{p-1}{2}}$, os restos da divisão dos números $a, 2a, 3a, ..., \frac{(p-1)}{2}a$ por p, respectivamente. Se k é o número dos r_i que são maiores do que $\frac{p-1}{2}$, então*

$$\left(\frac{a}{p}\right) = (-1)^k.$$

Demonstração:

Como $(a,p)=1$, os números $a, 2a, 3a, ..., \frac{(p-1)}{2}a$, são dois a dois incongruentes módulo p, pois se $ma \equiv na(mod\ p)$, com $m, n \leq \frac{p-1}{2}$ e $m \neq n$, então $m \equiv n(mod\ p)$, o que é um absurdo! Deste modo $r_1, r_2, ..., r_{\frac{p-1}{2}} \in \{1, 2, 3, ..., p-1\}$, e são distintos dois a dois.

Sejam $\{b_1, b_2, ..., b_k\}$ os elementos do conjunto $\{r_1, r_2, ..., r_{\frac{p-1}{2}}\}$ que são maiores do que $\frac{p-1}{2}$ e $\{c_1, c_2, ..., c_l\}$ os elementos do conjunto $\{r_1, r_2, ..., r_{\frac{p-1}{2}}\}$ que são menores ou iguais a $\frac{p-1}{2}$.

Notemos que $k + l = \frac{p-1}{2}$. Como $b_i > \frac{p-1}{2}$ então $p - b_i < p - \frac{p-1}{2} = \frac{p+1}{2}$, ou seja $p - b_i < \frac{p+1}{2}$, $\forall i \in \{1, 2, 3, ..., k\}$. Além disso, se $p - b_i = c_j$ então $-b_i \equiv c_j(mod\ p)$, o que não pode ocorrer, pois se $-b_i \equiv c_j(mod\ p)$ teríamos

$$\begin{cases} -b_i \equiv -ra(mod\ p) & , r \in \left\{1, 2, 3, ..., \frac{p-1}{2}\right\} \\ c_j \equiv sa(mod\ p). \end{cases}$$

Daí implica que $-ra \equiv sa(mod\ p)$. Como $(a,p)=1$, segue que,

$-r \equiv s(mod\, p)$, o que implica que, $p|r+s$, o que é um absurdo, pois $r \leq \frac{p-1}{2}$ e $s \leq \frac{p-1}{2}$

$$\Rightarrow r + s \leq p - 1 \Rightarrow r + s < p.$$

Assim, $p - b_1, p - b_2, ..., p - b_k$ são distintos dos números $c_1, c_2, ..., c_l$.

Como $k + l = \frac{p-1}{2}$, segue que

$$\{p - b_1, p - b_2, ..., p - b_k\} \cup \{c_1, c_2, ..., c_l\} = \left\{1, 2, ..., \frac{p-1}{2}\right\}.$$

Desta forma, $c_1 c_2 ... c_l (p - b_1)(p - b_2)...(p - b_k) = \left(\frac{p-1}{2}\right)!$.

Por outro lado, pela definição dos r_i, temos

$$b_1b_2...b_kc_1c_2...c_l = r_1r_2...r_{\frac{p-1}{2}} \equiv (a)(2a)(3a)...\frac{(p-1)}{2}a(mod\ p)$$

$$b_1b_2...b_kc_1c_2...c_l \equiv a^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!(mod\ p)$$

e portanto

$$b_1b_2...b_kc_1c_2...c_l \equiv a^{\frac{p-1}{2}}(p-b_1)(p-b_2)...(p-b_k)c_1c_2...c_l(mod\ p)$$

donde

$$b_1b_2...b_k \equiv a^{\frac{p-1}{2}}(p-b_1)(p-b_2)...(p-b_k)(mod\ p).$$

Como $(p, p-b_i) = 1$, para todo i, existe d_i tal que $d_i(p-b_i) \equiv 1(mod\ p)$.
Logo

$$d_1d_2...d_kb_1b_2...b_k \equiv a^{\frac{p-1}{2}}d_1d_2...d_k(p-b_1)(p-b_2)...(p-b_k)(mod\ p)$$

$$d_1d_2...d_kb_1b_2...b_k \equiv a^{\frac{p-1}{2}}(mod\ p). \qquad (*)$$

Como $d_i(p-b_i) \equiv 1(mod\ p)$, segue $d_ib_i \equiv -1(mod\ p)$. Deste modo

$$d_1d_2...d_kb_1b_2...b_k \equiv (-1)^k(mod\ p). \qquad (**)$$

De $(*)$ e $(**)$, concluímos que $a^{\frac{p-1}{2}} \equiv (-1)^k(mod\ p)$. Como $\left(\frac{a}{p}\right) = 1$ ou -1, p é primo ímpar, concluímos que $\left(\frac{a}{p}\right) = (-1)^k$.

□

Teorema 3.3.1. *Se p é um primo ímpar positivo e a é um inteiro ímpar tal que $p \nmid a$ então $\left(\frac{a}{p}\right) = (-1)^M$, onde $M = \left[\frac{a}{p}\right] + \left[\frac{2a}{p}\right] + ... + \left[\frac{(p-1)}{2}\cdot\frac{a}{p}\right]$.*

Demonstração:
Fazendo divisão Euclidiana de $a, 2a, 3a, ..., \frac{(p-1)}{2}a$ por p, obteremos $r_1, r_2, ..., r_{\frac{p-1}{2}}$, respectivamente, tais que

$$\begin{aligned} a &= p\left[\frac{a}{p}\right] + r_1 \\ 2a &= p\left[\frac{2a}{p}\right] + r_2 \\ &\vdots \\ \frac{(p-1)}{2}a &= p\left[\frac{(p-1)}{2}\cdot\frac{a}{p}\right] + r_{\frac{p-1}{2}}. \end{aligned}$$

Notemos que $r_1, r_2, ..., r_{\frac{p-1}{2}}$, são os b_i e c_j definidos na demonstração do Lema de Gauss. Somando membro a membro das igualdades acima obteremos:

$$a\left(1+2+3+...+\frac{(p-1)}{2}\right) = p\left(\left[\frac{a}{p}\right]+\left[\frac{2a}{p}\right]+...+\left[\frac{(p-1)}{2}\cdot\frac{a}{p}\right]\right)+(r_1+r_2+...+r_{\frac{p-1}{2}})$$

$$a\cdot\frac{(p^2-1)}{8} = pM+I+S \qquad (*)$$

onde $I = b_1 + b_2 + ... + b_k$ e $S = c_1 + c_2 + ... + c_l$. Vimos também na demonstração do Lema de Gauss que

$$\{p-b_1, p-b_2, ..., p-b_k\} \cup \{c_1, c_2, ..., c_l\} = \left\{1, 2, ..., \frac{p-1}{2}\right\}.$$

Portanto

$$1+2+3+...+\frac{(p-1)}{2} = \frac{(p^2-1)}{8} = c_1+c_2+...+c_l+kp-(b_1+...+b_k),$$

isto é, $\frac{(p^2-1)}{8} = S+kp-I.$ $(**)$

Subtraindo-se membro a membro, as equações $(*)$ e $(**)$, obteremos

$$\frac{(p^2-1)}{8}\cdot(a-1) = p(M-k)+2I$$

Como, por hipótese, a e p são ímpares então o termo $\frac{(p^2-1)}{8}\cdot(a-1)$ será par e portanto $p(M-k)$ será par. Como $p(M-k)$ é par e p é ímpar, segue que, $M-k$ é um número par. Assim M e k possuem a mesma paridade, ou seja, M e k são ambos números pares ou ambos números ímpares.

Portanto pelo Lema de Gauss, concluímos que, $\left(\frac{a}{p}\right) = (-1)^k = (-1)^M$.

□

Como aplicação do Teorema 3.3.1, mostraremos que a equação Diofantina não linear $x^2 + 13y = 5$ não admite soluções inteiras.

Exemplo 3.3.1. Mostre que a equação diofantina $x^2 + 13y = 5$ não admite soluções inteiras.

Solução:

De fato, suponha que a equação diofantina dada possua solução. Assim existem $x_0, y_0 \in \mathbb{Z}$ tais que $x_0^2+13y_0 = 5$. Daí $x_0^2 \equiv 5(mod\ 13)$. Isto implica que a congruência $x^2 \equiv 5(mod\ 13)$ admite solução, ou seja, 5 é um resíduo quadrático módulo 13, ou ainda, $\left(\frac{5}{13}\right) = 1$. $(*)$

Por outro lado

$$M = \left[\frac{5}{13}\right] + \left[\frac{2\cdot 5}{13}\right] + \left[\frac{3\cdot 5}{13}\right] + \left[\frac{4\cdot 5}{13}\right] + \left[\frac{5\cdot 5}{13}\right] + \left[\frac{6\cdot 5}{13}\right] = 5$$

Portanto

$$\left(\frac{5}{13}\right) = (-1)^M = (-1)^5 = -1. \qquad (**)$$

De $(*)$ e $(**)$, obtemos uma contradição. Portanto a equação diofantina dada não admite soluções inteiras.

O Teorema 3.3.1, nos formece uma fórmula para calcular o símbolo de Legendre a um número primo ímpar positivo qualquer. No entanto, isso pode ser muito trabalhoso para números primos "grandes". Veremos agora, a Lei da Reciprocidade Quadrática de Gauss, que nos permitirá fazer esse cálculo de maneira muito mais eficiente. Esta lei foi conjecturada na primeira metade do século XVIII e houve várias tentativas em demonstrá-lo. Legendre, em 1785, publicou uma demonstração deficiente. Mas no dia 8 de abril de 1796, a Lei da Reciprocidade Quadrática foi finalmente demonstrada, por um jovem matemático, de apenas 18 anos, chamado Joham Carl Friedrich Gauss. O Teorema da Lei da Reciprocidade Quadrática foi chamado por Gauss de Teorema Áureo. Ele ficou tão entusiasmado com tal resultado que ele apresentou oito demonstrações distintas a respeito deste resultado ao longo de sua vida.

A Lei da Reciprocidade Quadrática de Gauss nos diz que: dados as congruência

$$\begin{cases} x^2 \equiv p(mod\ q) \\ x^2 \equiv q(mod\ p) \end{cases}$$

são ambas solúveis ou ambas insolúveis, no entanto se $p \equiv q \equiv 3(mod\ 4)$ então uma das congruência será solúvel e a outra será insolúvel.

A demonstração que daremos a seguir foi dada pelo matemático alemão Ferdinand Gotthold Max Eisenstein (1823-1852).

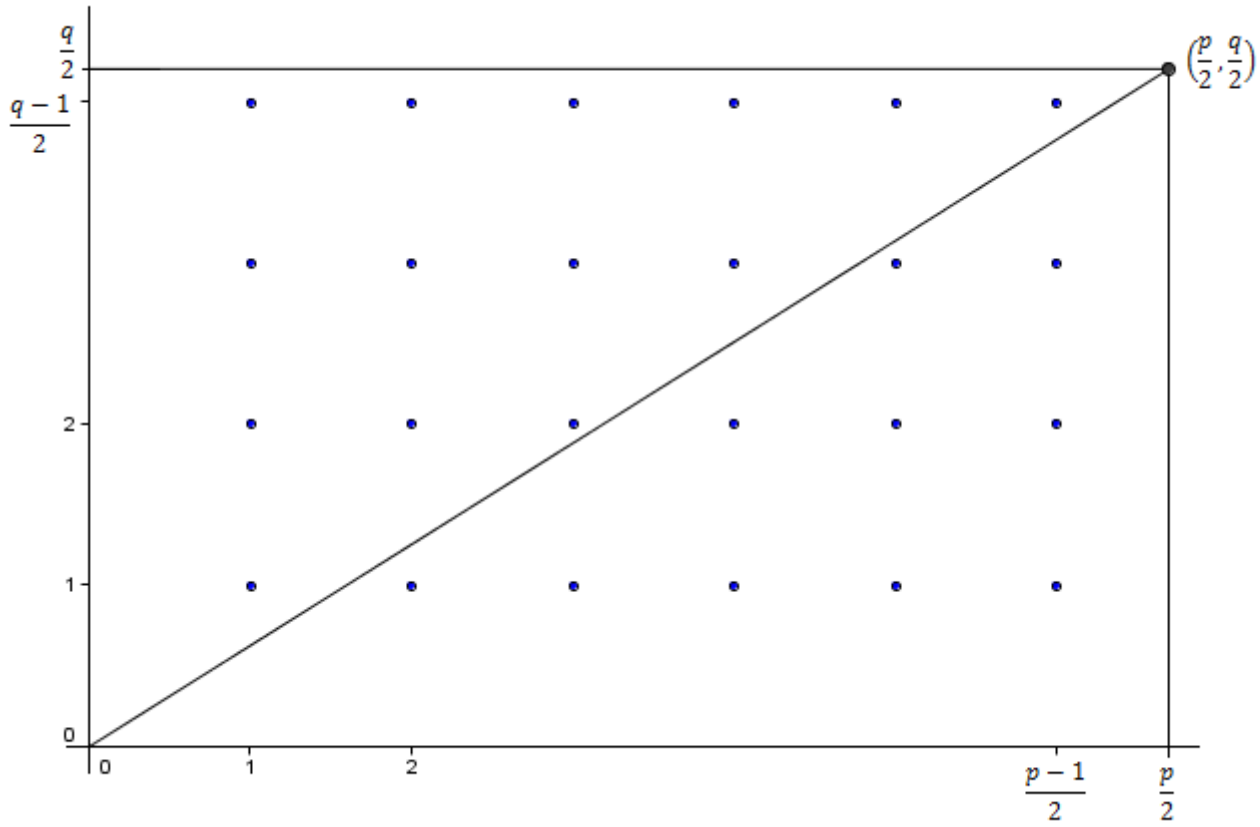
Em termos do símbolo de Legendre, a Lei da Reciprocidade Quadrática é formulada do seguinte modo:

Teorema 3.3.2. *(Lei da Reciprocidade Quadrática de Gauss) Se p e q são primos ímpares positivos distintos, então*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{q-1}{2}\cdot\frac{p-1}{2}}.$$

Demonstração:

Consideremos o retângulo de vértices $(0,0)$, $\left(\frac{p}{2},0\right)$, $\left(\frac{p}{2},\frac{q}{2}\right)$ e $\left(0,\frac{q}{2}\right)$. Marcamos, em seu interior, os pontos (x,y) com $x \in \left\{1,2,...,\frac{p-1}{2}\right\}$ e $y \in \left\{1,2,...,\frac{q-1}{2}\right\}$, conforme a seguinte figura:



É claro que o número de pontos interiores a este retângulo, cujas coordenadas são números inteiros, é igual a $\frac{p-1}{2}\cdot\frac{q-1}{2}$. $(*)$

Por outro lado, consideremos à equação da reta que passa por $(0,0)$ e $\left(\frac{p}{2},\frac{q}{2}\right)$, é $y=\frac{qx}{p}$.

Como $(i,p)=1$, com $i \in \left\{1,2,3,...,\frac{p-1}{2}\right\}$, isto implica que esta reta não contém nenhum dos pontos inteiros cujas coordenadas são números inteiros.

A reta $y=\frac{qx}{p}$ intercepta a reta $x=k$, paralela ao eixo y no ponto $(k,\frac{kq}{p})$. Como $\frac{kq}{p} \notin \mathbb{Z}$, para $k \in \left\{1,2,3,...,\frac{p-1}{2}\right\}$ qualquer, o número $\left[\frac{kq}{p}\right]$ é a quantidade de pontos da reta $x=k$ que estão abaixo da reta $y=\frac{qx}{p}$ e no interior do retângulo.

Logo o total M de pontos cujas coordenadas são números inteiros que estão abaixo da reta $y=\frac{qx}{p}$ e no interior do retângulo é:

$$M=\left[\frac{q}{p}\right]+\left[\frac{2q}{p}\right]+\left[\frac{3q}{p}\right]+...+\left[\frac{p-1}{2}\cdot\frac{q}{p}\right]$$

Analogamente, a reta $y = \frac{qx}{p}$ intercepta a reta $y = k$, paralela ao eixo x no ponto $\left(\frac{pk}{q}, k\right)$. Como $\frac{kp}{q} \notin \mathbb{Z}$ para $k \in \left\{1, 2, ..., \frac{q-1}{2}\right\}$, o número $\left[\frac{kp}{q}\right]$ é a quantidade de pontos da reta $y = k$ que estão acima da reta $y = \frac{qx}{p}$, e que estão no interior do retângulo. Logo o número N dos pontos que estamos considerando é:

$$N = \left[\frac{p}{q}\right] + \left[\frac{2p}{q}\right] + \left[\frac{3p}{q}\right] + ... + \left[\frac{q-1}{2} \cdot \frac{p}{q}\right]$$

Portanto de $(*)$ temos

$$M + N = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

No entanto pelo Teorema 3.3.1, segue que

$$\left(\frac{q}{p}\right) = (-1)^M \text{ e } \left(\frac{p}{q}\right) = (-1)^N,$$

o que implica

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{M+N} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

□

Corolário 3.3.1. *Se p e q são primos ímpares positivos distintos. Então*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1 & \text{se } p \equiv 1 (mod\ 4) \text{ ou } q \equiv 1 (mod\ 4) \\ -1 & \text{se } p \equiv q \equiv 3 (mod\ 4). \end{cases}$$

Demonstração:
O número $\frac{p-1}{2} \cdot \frac{q-1}{2}$ é par se, e somente se, um dos inteiros p ou q for da forma $4k+1$; Se ambos forem da forma $4k+3$, então $\frac{p-1}{2} \cdot \frac{q-1}{2}$ é ímpar.

□

Corolário 3.3.2. *Se p e q são primos ímpares positivos distintos. Então*

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{se } p \equiv 1 (mod\ 4) \text{ ou } q \equiv 1 (mod\ 4) \\ -\left(\frac{q}{p}\right) & \text{se } p \equiv q \equiv 3 (mod\ 4). \end{cases}$$

Demonstração:
Pela lei da Reciprocidade Quadrática de Gauss temos $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$. Multipli-

cando ambos os membros da igualdade acima por $\left(\frac{q}{p}\right)$ obtemos

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right)$$

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)^2 = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right)$$

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right).$$

Se $p \equiv 1(mod\ 4)$ ou $q \equiv 1(mod\ 4)$, pelo corolário 3.3.1, temos

$$(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1.$$

Assim, $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$.
Se $p \equiv q \equiv 3(mod\ 4)$, novamente pelo corolário 3.3.1, temos:

$$(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1,$$

ou seja, $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

□

O exemplo a seguir, mostrará como a Lei da Reciprocidade Quadrática pode ser útil em questões envolvendo equações Diofantinas não lineares.

Exemplo 3.3.2. Mostre que a equação diofantina $x^2 - 241y = 2561$ admite soluções inteiras.

Solução:
Mostrar que a equação diofantina dada possui solução é equivalente a mostrar que

$$\left(\frac{2561}{241}\right) = 1.$$

De fato, notemos inicialmente que 241 é um número primo e que $2561 \equiv 151(mod\ 241)$. Logo pelo Teorema 3.2.1, temos,

$$\left(\frac{2561}{241}\right) = \left(\frac{151}{241}\right) = 1.$$

Pela Lei da Reciprocidade Quadrática temos:

$$\left(\frac{151}{241}\right)\left(\frac{241}{151}\right) = (-1)^{9000} = 1.$$

Portanto

$$\left(\frac{151}{241}\right) = \left(\frac{241}{151}\right) = \left(\frac{90}{151}\right) = \left(\frac{3^2 \cdot 2 \cdot 5}{151}\right) = \left(\frac{3^2}{151}\right)\left(\frac{2}{151}\right)\left(\frac{5}{151}\right)$$

$$\Rightarrow \left(\frac{151}{241}\right) = \left(\frac{2}{151}\right)\left(\frac{5}{151}\right) = \left(\frac{5}{151}\right) = \left(\frac{151}{5}\right) = \left(\frac{1}{5}\right) = 1.$$

Exemplo 3.3.3. Mostre que $1! + 2! + 3! + ... + n!$ nunca é um quadrado perfeito quando $n > 3$.

Solução:

Seja $N = 1! + 2! + 3! + ... + n!$.

Suponhamos que $N = x^2$, para algum $x \in \mathbb{N}$. Sendo $n > 3$, $N > 5$.

Então

$$\left(\frac{N}{5}\right) = \left(\frac{x^2}{5}\right) = 1.$$

Por outro lado, sendo $N = 1! + 2! + 3! + 4! + ... + n!$, temos, $N \equiv 3(mod\ 5)$.

Daí

$$\left(\frac{N}{5}\right) = \left(\frac{3}{5}\right).$$

No entanto,

$$\left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1,$$

o que implica que

$$\left(\frac{N}{5}\right) = -1,$$

o que é uma contradição!

Exemplo 3.3.4. Se p é um primo ímpar onde $p > 3$. Então

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{se } p \equiv \pm 1(mod\ 12) \\ -1 & \text{se } p \equiv \pm 5(mod\ 12). \end{cases}$$

Solução:

Sendo $3 \equiv 3(mod\ 4)$, pelo corolário 3.3.2, temos

$$\left(\frac{3}{p}\right) = \begin{cases} \left(\frac{p}{3}\right) & \text{se } p \equiv 1(mod\ 4) \\ \\ -\left(\frac{p}{3}\right) & \text{se } p \equiv 3(mod\ 4). \end{cases}$$

No entanto, $p \equiv 1(mod\ 3)$ ou $p \equiv 2(mod\ 3)$. Assim

$$\left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1 \text{ ou } \left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1$$

Deste modo

$$\left(\frac{p}{3}\right) = \begin{cases} 1 \text{ se } p \equiv 1(mod\ 3) \\ -1 \text{ se } p \equiv 2(mod\ 3) \end{cases} . \qquad (*)$$

Isto implica que $\left(\frac{3}{p}\right) = 1$ se, e somente se,

$$p \equiv 1(mod\ 4) \text{ e } p \equiv 1(mod\ 3)$$

$$p \equiv 3(mod\ 4) \text{ e } p \equiv 2(mod\ 3).$$

A expressão $p \equiv 1(mod\ 4)$ e $p \equiv 1(mod\ 3)$ é equivalente a $p \equiv 1(mod\ 12)$. Enquanto que $p \equiv 3(mod\ 4)$ e $p \equiv 2(mod\ 3)$ é equivalente a $p \equiv 11 \equiv -1(mod\ 12)$.
De $(*)$, temos também que

$$\left(\frac{3}{p}\right) = -1 \Longleftrightarrow p \equiv 1(mod\ 4) \text{ e } p \equiv 2(mod\ 3) \text{ ou } p \equiv 3(mod\ 4) \text{ e } p \equiv 1(mod\ 3).$$

A expressão $p \equiv 1(mod\ 4)$ e $p \equiv 2(mod\ 3)$ é equivalente a $p \equiv 5(mod\ 12)$. Enquanto que $p \equiv 3(mod\ 4)$ e $p \equiv 1(mod\ 3)$ é equivalente a $p \equiv 7 \equiv -5(mod\ 12)$.
Portanto,

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{se } p \equiv \pm 1(mod\ 12) \\ -1 & \text{se } p \equiv \pm 5(mod\ 12). \end{cases}$$

Exemplo 3.3.5. Se p é um primo ímpar onde $p > 3$. Então

$$\left(\frac{-3}{p}\right) = \begin{cases} 1 & \text{se } p \equiv 1(mod\ 6) \\ -1 & \text{se } p \equiv 5(mod\ 6). \end{cases}$$

Solução:
Como o símbolo de Legendre é multiplicativo, segue que

$$\left(\frac{-3}{p}\right) = \left(\frac{-1 \cdot 3}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{3}{p}\right)$$

Daí

$$\left(\frac{-3}{p}\right) = \begin{cases} \left(\frac{-1}{p}\right) & \text{se } p \equiv \pm 1(mod\ 12) \\ -\left(\frac{-1}{p}\right) & \text{se } p \equiv \pm 5(mod\ 12). \end{cases}$$

Se $p \equiv 1(mod\ 12)$ então $p = 1 + 12t$, para algum $t \in \mathbb{Z}$. Isto implica que

$$p \equiv 1(mod\ 4) \Rightarrow \left(\frac{-1}{p}\right) = 1 \Rightarrow \left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right) = 1.$$

Se $p \equiv -1(mod\ 12)$ então $p = 11 + 12l$, para algum $l \in \mathbb{Z}$. Isto implica que

$$p \equiv 3(mod\ 4) \Rightarrow \left(\frac{-1}{p}\right) = -1 \Rightarrow \left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right) = -1.$$

Se $p \equiv 5(mod\ 12)$ então $p = 5 + 12s$, para algum $s \in \mathbb{Z}$. Isto implica que

$$p \equiv 1(mod\ 4) \Rightarrow \left(\frac{-1}{p}\right) = 1 \Rightarrow \left(\frac{-3}{p}\right) = -\left(\frac{-1}{p}\right) = -1.$$

Se $p \equiv -5(mod\ 12)$ então $p = 7 + 12r$, para algum $r \in \mathbb{Z}$. Isto implica que

$$p \equiv 3(mod\ 4) \Rightarrow \left(\frac{-1}{p}\right) = -1 \Rightarrow \left(\frac{-3}{p}\right) = -\left(\frac{-1}{p}\right) = 1.$$

Logo

$$\left(\frac{-3}{p}\right) = \begin{cases} \left(\frac{-1}{p}\right) & \text{se } p \equiv 1(mod\ 12) \text{ } ou \text{ } p \equiv 7(mod\ 12) \\ -\left(\frac{-1}{p}\right) & \text{se } p \equiv -1(mod\ 12) \text{ } ou \text{ } p \equiv 5(mod\ 12). \end{cases}$$

Como $p \equiv 1(mod\ 12)$ *ou* $p \equiv 7(mod\ 12)$ é equivalente a $p \equiv 1(mod\ 6)$ e $p \equiv -1(mod\ 12)$ *ou* $p \equiv 5(mod\ 12)$ é equivalente a $p \equiv 5(mod\ 6)$, segue que.

$$\left(\frac{-3}{p}\right) = \begin{cases} 1 & \text{se } p \equiv 1(mod\ 6) \\ -1 & \text{se } p \equiv 5(mod\ 6). \end{cases}$$

Exemplo 3.3.6. Mostre que existem infinitos primos da forma $6n + 1$.

Solução:

Suponhamos que exista um número finito de primos da forma $6n + 1$. Sejam eles: $p_1, p_2, ..., p_r$. Seja $N = (2p_1p_2...p_r)^2 + 3$. Pelo Teorema Fundamental da Aritmética, existe p primo ímpar tal $p|N$. Assim $(2p_1p_2...p_r)^2 \equiv -3(mod\ p)$. Isto implica que a congruência $x^2 \equiv -3(mod\ p)$ admite solução, ou seja, $\left(\frac{-3}{p}\right) = 1$. Pelo exemplo anterior temos $p \equiv 1(mod\ 6)$. Isto implica que $p \in \{p_1, p_2, ..., p_r\}$.

Seja $p = p_i$, para algum i. Então $p|(2p_1p_2...p_r)^2$ e como $p|N$, segue que $p|3$, donde implica que $p = 3$, o que é um absurdo. Pois $3 \not\equiv 1(mod\ 6)$.

Chamamos de número de Fermat, os números da forma $F_n = 2^{2^n} + 1$, onde $n \in \mathbb{N}$.

Em 1640, Fermat por ter observado que os números $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ e $F_4 = 65537$ são primos, então ele afirmou que esses números eram todos primos. No entanto, em 1732, Leonhard Euler mostrou que

$$F_5 = 2^{2^5} + 1 = 4294967297 = 641 \cdot 6700417,$$

portanto F_5 é um número composto, desmentindo a afirmação de Fermat.

Em 1877, o matemático francês Jean François Théophile Pepín, utilizando a Lei da Reciprocidade Quadrática, demonstrou um elegante teste para determinar sob que condições, o número de Fermat F_n é um número primo.

Teorema 3.3.3. *(Teste de Pepín) O número de Fermat F_n é um número primo se, e somente se, $3^{\frac{F_n-1}{2}} \equiv -1(mod\ F_n),\ \forall n \geq 1$.*

Demonstração:
($\Rightarrow$) Assuma que $F_n = 2^{2^n} + 1$ é um número primo.
Como $F_n \equiv 1(mod\ 4)$, pela Lei da Reciprocidade Quadrática temos $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right)$, mas

$$F_n \equiv (-1)^{2^n} + 1 \equiv 2(mod\ 3).$$

Deste modo

$$\left(\frac{F_n}{3}\right) = \left(\frac{2}{3}\right) = -1. \text{ Então } \left(\frac{3}{F_n}\right) = -1. \qquad (*)$$

Por outro Lado, pelo Critério de Euler,

$$\left(\frac{3}{F_n}\right) \equiv 3^{\frac{F_n-1}{2}}(mod\ F_n). \qquad (**)$$

Assim, de $(*)$ e $(**)$, obtemos, $3^{\frac{F_n-1}{2}} \equiv -1(mod\ F_n)$.
($\Leftarrow$) Reciprocamente, suponha que $3^{\frac{F_n-1}{2}} \equiv -1(mod\ F_n)$.
Assim $3^{\frac{F_n-1}{2}} \equiv -1(mod\ p)$, para algum p primo tal que $p|F_n$. Então $3^{F_n-1} \equiv 1(mod\ p)$, o que implica que $ord_p 3|(F_n - 1)$, ou seja, $ord_p 3|2^{2^n}$.
Consequentemente, $ord_p 3 = 2^k$ para algum inteiro positivo k. Vamos mostrar que $k = 2^n$. Suponha que $k < 2^n$. Então $2^n \geq k + 1$, ou seja, $2^n - k - 1 \geq 0$. Sendo $3^{2^k} \equiv 1(mod\ p)$, temos $(3^{2^k})^{2^{2^n-k-1}} \equiv 1(mod\ p)$. Isto implica que $3^{2^{2^n-1}} \equiv 1(mod\ p)$, isto é,

$$3^{\frac{F_n-1}{2}} \equiv 1(mod\ p).$$

Assim $1 \equiv -1(mod\ p)$, donde implica que $p = 2$, o que é uma contradição. Logo $k = 2^n$.

Assim $ord_p 3 = 2^{2^n} = F_n - 1$.
Por outro lado, pelo Pequeno Teorema de Fermat temos

$$3^{p-1} \equiv 1(mod\ p),\ \text{ou seja } ord_p^3 \leq p-1.$$

Deste modo

$$F_n - 1 = ord_p^3 \leq p-1 \Rightarrow F_n \leq p.$$

onde $p|F_n$. Logo $F_n = p$ é um primo.

□

O seguinte exemplo ilustra o Teste de Pepín.

Exemplo 3.3.7. Mostre que $F_4 = 2^{2^4} + 1 = 65537$ é primo.

Solução:
Pelo Teste de Pepín, é suficiente mostrar que

$$3^{\frac{F_4-1}{2}} = 3^{2^{15}} = 3^{32768} \equiv -1(mod\ F_4).$$

De fato

$$3^8 \equiv 6561(mod\ F_4)$$

$$3^{20} \equiv 19390(mod\ F_4)$$

$$3^{40} \equiv -13669(mod\ F_4)$$

$$3^{60} \equiv -10282(mod\ F_4)$$

$$3^{200} \equiv -28787(mod\ F_4)$$

$$3^{500} \equiv 26868(mod\ F_4)$$

$$3^{32000} \equiv 27748(mod\ F_4).$$

Então

$$\begin{aligned} 3^{32768} &= 3^{32000} \cdot 3^{500} \cdot 3^{200} \cdot 3^{60} \cdot 3^8 \equiv (27748)(26868)(-28787)(-10282)(6561)(mod\ F_4) \\ 3^{32768} &\equiv -1(mod\ F_4). \end{aligned}$$

Portanto F_4 é primo.

Conclusão

A Teoria dos Números é um ramo da matemática pura que estuda as propriedades dos números, em particular, a dos números inteiros, bem como os numerosos problemas que surge no seu estudo. Este ramo envolve muitos problemas que são facilmente compreendidos mesmo por não matemáticos, por exemplo, o Último Teorema de Fermat. É uma área da matemática que tem uma longa história, originando-se nas antigas civilizações. O francês Pierre de Fermat tinha um fascínio especial pelos números, por isso dedicava parte do seu tempo em resolver as questões de aritméticas do livro *Arithmetica* da autoria de Claude Gaspar Bochet. Este estudo levara-o a pensar e equacionar novas questões, sempre tentando alcançar novos resultados. Por esta razão, Fermat pode ser considerado um dos fundadores da Teoria dos Números.

Por outro lado, as Funções Aritméticas possuem um papel significativo no que diz respeito a vários resultados importantíssimo com relação aos números primos.

É bem provável que a Lei da Reciprocidade Quadrática, foi um dos primeiros resultados profundos da teoria dos números moderna. Como disse o matemático alemão Erich Hecke: *"A Teoria dos Números moderna começou com o descobrimento da Lei da Reciprocidade"*.

Este trabalho caracteriza-se pelo calibre dos exemplos discutidos, boa parte dos quais oriundos de várias competições de matemática ao redor do mundo. Espero que o presente trabalho sirva de apoio e motivação aos interessados no assunto.

Referências

[01] ABDO, R. *Teoria Analítica dos Números.* [S.l.]: Notas de Estudo, rfabd89@yahoo.com.br.

[02] BRAND, A. J. *Introduction to Analytic Number Theory.* [S.l.]: Department ref mathematcs University of II Lionis.Math 531 lectures notes, fall, 2005.

[03] DAN, A.; FERREIRA, C. *Curso de Álgebra para o curso de licenciatura.* [S.l.]: Apostila do curso de licenciatura da UFMG, 1984. (2º semestre).

[04] DAVID, M. B. *Elementary number theory.* 5. ed. [S.l.]: McGrawhill Edition.

[05] GONÇALVES, A. *Introdução à Álgebra.* 5. ed. Rio de Janeiro: IMPA, 2005. (projeto Euclides).

[06] HEFEZ, A. *Curso de Álgebra.* 1. ed. Rio de Janeiro: IMPA, 2002. (3, v. 1).

[07] HEFEZ, A. *Elementos da Aritmética.* 1. ed. Rio de Janeiro: Sociedade brasileira de matemática, 2004.

[08] HYGINO, H. D. *Fundamentos de Aritmética.* 1. ed. São Paulo: Editora Atual, 1991.

[09] HYGINO, H. D.; IEZZI, G. *Álgebra Moderna.* 4. ed. São Paulo: Editora Atual, 2003.

[10] KOSHY, T. *Elementary Number Theory Wilth Aplications.* 2. ed. [S.l.]: Elsevier, 2007.

[11] LIMA, E. L. *Curso de Análise.* 7. ed. Projeto Euclides, Rio de Janeiro: IMPA, 1989.

[12] MOREIRA, C. G.; MARTINEZ, F. E. B.; SALDANHA, N. C. *Tópicos de Teoria dos Números.* 1. ed. Rio de Janeiro: SBM, 2012. (Profmat).

[13] MOREIRA, C. G.; TENGAN, E.; SALDANHA, N. *Teoria dos Números: Um passeio com primos e outros números familiares pelo mundo inteiro.* 1. ed. Projeto Euclides, Rio de Janeiro: IMPA, 2010.

[14] NETO, A. C. M. *Tópicos de Matemática Elementar, teoria dos números.* 1. ed. Rio de Janeiro: Coleção professor de matemática, 2012.

[15] OLIVEIRA, F. Introdução à Teoria dos Números. Lisboa: FCT, Universidade Nova

de Lisboa.

[16] OLIVEIRA, M. R. de; PINHEIRO, M. R. da R. *Elementos da Matemática.* 3. ed. Fortaleza: Vestseller, 2010.

[17] PIMENTEL, F. R. Teoria dos Números. [S.l.]: Apostila do curso de Teoria dos números da UFOP, 2005.

[18] SANDIFER. *Mathematical Association of America.* Ed.: Archimedes What Did He do Besides Cry Eureka.

[19] SANTOS, J. P. de Oliveira dos. *Introdução à Teoria dos Números.* 3. ed. Rio de Janeiro: IMPA, 2011. (coleção matemática universitária).

[20] SHOKRANIAN, S.; SOARES, M.; GODINHO, H. *Teoria dos Números.* Brasília: Editora da Universidade de Brasília, 1994.

[21] SIDKI, S. Introdução à Teoria dos Números. 1. ed. Rio de Janeiro: IMPA, 1975.

[22] TITU, A.; DORIN, A. *Number theory structures, examples and problems.* [S.l.]: Kindle Edition, 2009.