Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
PPGM - Departamento de Matemática
Mestrado Profissional em Matemática
em Rede Nacional PROFMAT

O Teorema de Dirichlet: Primos em progressão aritmética

por

José Carlos Silva Júnior

sob orientação do

Prof. Dr. Bruno Henrique Carvalho Ribeiro

Dissertação apresentada ao Corpo Docente do Mestrado Profissional em Matemática em Rede Nacional PROFMAT-CCEN-UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Agosto/2017
João Pessoa - PB

Catalogação na publicação
Seção de Catalogação e Classificação

S586t Silva Júnior, José Carlos.
O teorema de Dirichlet: primos em progressão aritmética / José Carlos Silva Júnior. - João Pessoa, 2017.
63 f. : il.

Orientação: Bruno Henrique Carvalho Ribeiro.
Dissertação (Mestrado) - UFPB/CCEN.

1. Matemática. 2. Progressões aritméticas. 3. Números primos. 4. Teorema de Dirichlet. I. Ribeiro, Bruno Henrique Carvalho. II. Título.

UFPB/BC

O Teorema de Dirichlet: Primos em progressão aritmética

por

José Carlos Silva Júnior

Dissertação apresentada ao Corpo Docente do Mestrado Profissional em Matemática em Rede Nacional PROFMAT CCEN-UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Área de Concentração: Teoria dos números

Aprovada por:

Prof. Dr. Bruno Henrique Carvalho Ribeiro - UFPB (Orientador)

Prof. Dr. Eudes Mendes Barboza - UPE

Prof. Dr. Esteban Pereira da Silva - UFPB

Agosto/2017

Agradecimentos

Primeiramente a Deus por ter permitido mais uma obra concluída em minha vida e por me conceder fé e perseverança nos momentos difíceis.

Aos meus pais José Carlos e Cleide Rodrigues pelos ensinamentos e por todo o Amor concedido durante toda a minha vida.

Aos meus irmãos Juliana e João Paulo por todos os momentos de felicidade que me deram força e coragem para continuar a batalha nos estudos.

A minha companheira Virgínia Leite pela paciência nos momentos de dificuldade e pelo Amor que sempre me acalmou.

Ao meu orientador professor Dr. Bruno Ribeiro por sua disposição, pela paciência e por todo o ensinamento que me passou.

A todos os meus amigos da turma 2015 do PROFMAT que estiveram comigo desde o início. Em especial, a David, Mailson, Diego, Rômulo, Manoel, Ramon e Erielson por todo apoio nas longas jornadas de estudo.

Dedicatória

Ao meu filho Pietro

Resumo

Neste trabalho apresentaremos alguns resultados básicos da teoria dos números com o objetivo de explorar o estudo dos primos em progressões aritméticas cujas razões e primeiros termos são primos entre si. Traremos demonstrações de alguns casos particulares do Teorema de Dirichlet sobre primos em PA, além de apresentarmos alguns resultados mais antigos e outros descobertos bem recentemente sobre a forma como os primos se distribuem em determinadas progressões aritméticas.

Palavras-chave: Progressões aritméticas; Números primos; Teorema de Dirichlet.

Abstract

In this work we will present some basic results of the number theory with the objective of exploring the study of primes in arithmetic progressions whose commom difference and first term are coprime. We will present proofs of some particular cases of Dirichlet's theorem on PA primes, in addition to presenting some older results and other recent findings about how the primes distribute themselves in certain arithmetic progressions.

Keywords: Arithmetic progressions; Prime numbers; Dirichlet's Theorem.

Sumário

Introdução

A forma como os números primos estão distribuídos tem provocado fascínio desde a antiguidade. Em pequenos intervalos de números, eles aparecem de modo aparentemente aleatório, o que tem chamado a atenção de muitos estudiosos. O Teorema Fundamental da Aritmética diz que todo número natural maior que 1 é primo ou pode ser escrito como produto de primos. Assim, por um lado os números primos são suficientes para representar todos os números naturais, por outro lado, não sabemos como eles estão distribuídos ao longo dos naturais. Os mistérios envolvendo os números primos têm atraído matemáticos pelo mundo inteiro e esse conjunto numérico tem sido uma fonte inesgotável de problemas em Teoria dos Números o que tem gerado grandes avanços na Matemática.

Do ponto de vista da estrutura multiplicativa, o conjunto dos números primos gera todo o conjunto dos números naturais. Este fato nos leva a pensar se existe uma forma de como os primos estão distribuídos nos naturais. Uma forma de olharmos para esse problema é investigando a existência de números primos em progressões aritméticas, já que elas têm saltos de tamanho conhecido uma vez que se conhece a sua razão. Este tema, primos em progressões aritméticas, apesar de envolver dois conceitos básicos estudados no ensino fundamental e no ensino médio, também nos leva a conceitos da Teoria Analítica dos Números.

Um dos problemas envolvendo números primos é o de encontrar progressões aritméticas contendo uma infinidade de números primos. Neste trabalho, pretendemos responder a seguinte pergunta: Quais progressões aritméticas contém primos e quantos são esses primos?

Podemos facilmente observar que na sequência numérica $1, 2, 3, 4, 5, \ldots$ estão todos os números primos já na sequência $2, 4, 6, 8, 10, \ldots$ apenas o 2 é primo. Observe que essas sequências são progressões aritméticas da forma $a + dn$, com a e d inteiros fixos e $n \in \mathbb{N} \cup 0$. Se a e d possuem um fator comum $q > 1$ então q divide todos os termos da progressão aritmética, que, portanto, têm todos os termos compostos, exceto possivelmente o próprio a, no caso em que $q = a$ é um número primo. Isto nos sugere analisar os casos onde os números a e d não possuem nenhum fator em comum. Nessa direção nos diz Ribenboim:

> Um teorema clássico e de grande importância para a matemática foi demonstrado por DIRICHLET em 1837. Afirma-se:
>
> Se $d \geq 2$ e $a \neq 0$ são números inteiros primos entre si, então a progressão aritmética
>
> $$a, a + d, a + 2d, a + 3d, a + 4d, \ldots$$

> contém uma infinidade de números primos. (Ribenboim, 2014, p. 190). [5]

Uma demonstração mais simples deste teorema envolve conceitos mais profundos pertencentes à Teoria Analítica dos Números e, por isso, não será demonstrado aqui. Casos particulares do teorema de Dirichlet serão o objeto de estudo do nosso trabalho e, para isso, iremos estudar alguns tópicos de Teoria dos Números e algumas propriedades dos Polinômios ciclotômicos objetivando demonstrar a infinidade de primos em algumas progressões aritméticas.

Para uma melhor leitura e compreensão do texto o nosso trabalho foi organizado em dois capítulos.

No capítulo 1 serão abordados alguns conceitos mais básicos da Teoria dos Números. Começamos com o Princípio da Boa Ordenação e, como consequência, apresentamos a propriedade Arquimediana, o Princípio de Indução, alguns critérios de divisibilidade e o Teorema da Divisão Euclidiana. Apresentaremos também algumas propriedades do máximo divisor comum e dos números primos. Por fim, apresentaremos o estudo das congruências e algumas propriedades básicas.

No capítulo 2, seção 1, falaremos um pouco mais sobre congruências, onde apresentaremos o Teorema de Euler e o Teorema de Wilson, alguns resultados para o estudo da resolução das congruências lineares como o Teorema Chinês dos Restos e o Teorema de Thue, além de um breve estudo das congruências quadráticas e dos resíduos quadráticos, finalizando com a Lei da Reciprocidade Quadrática. O objetivo aqui é mostrar a infinidade de primos em algumas progressões aritmética como $\{2n+1\}_{n\in\mathbb{N}}$, $\{4n+1\}_{n\in\mathbb{N}}$, $\{4n+3\}_{n\in\mathbb{N}}$, $\{6n+5\}_{n\in\mathbb{N}}$, $\{3n+2\}_{n\in\mathbb{N}}$, $\{8n+5\}_{n\in\mathbb{N}}$, $\{3n+1\}_{n\in\mathbb{N}}$, $\{6n+1\}_{n\in\mathbb{N}}$,$\{8n+3\}_{n\in\mathbb{N}}$, $\{2^r n+1\}_{n\in\mathbb{N}}$. Já na seção 2 apresentaremos dois casos particulares do Teorema de Dirichlet, porém, mais gerais que os casos apresentados na seção 1. O primeiro caso é $\{q^s n+1\}_{n\in\mathbb{N}}$. Para o segundo caso apresentaremos algumas propriedades dos polinômios ciclotômicos objetivando demonstrar a infinidade de primos na progressão aritmética $\{dn+1\}_{n\in\mathbb{N}}$. Por fim, na seção 3, apresentaremos alguns fatos e algumas curiosidades sobre primos em Progressões aritméticas.

Capítulo 1

Preliminares

Neste capítulo iremos abordar alguns conceitos básicos para um melhor entendimento dos conteúdos explorados no capítulo 2. O nosso objetivo neste capítulo é tornar este trabalho um texto autocontido onde o leitor não precisará consultar outros materiais para o seu entendimento. No que segue utilizaremos como conhecidos e sem mais comentários o Princípio da Boa Ordenação, a propriedade Arquimediana e o Princípio de Indução.

1.1 Números inteiros

Binômio de Newton

Considere a expressão $(1+X)^n$, onde X é uma indeterminada e n é um número natural. O desenvolvimento dessa potência é um polinômio de grau n em X cujos coeficientes são números naturais:

$$(1+X)^n = \binom{n}{0} + \binom{n}{1}X + \binom{n}{2}X^2 + \ldots + \binom{n}{n-1}X^{n-1} + \binom{n}{n}X^n.$$

Proposição 1.1.1 *[Binômio de Newton] Sejam a e b números reais e seja $n \in \mathbb{N}$. Tem-se que* $(a+b)^n = a^n + \binom{n}{1}a^{n-1}b + ... + \binom{n}{n-1}ab^{n-1} + b^n$

Demonstração: Se $b = 0$, o resultado é direto. Se $b \neq 0$, substituindo x por $\frac{a}{b}$ na expansão de $(1+x)^n$ obtemos

$$\left(1+\frac{a}{b}\right)^n = 1 + \binom{n}{1}\frac{a}{b} + \binom{n}{2}\left(\frac{a}{b}\right)^2 + \ldots + \binom{n}{n-1}\left(\frac{a}{b}\right)^{n-1} + \binom{n}{n}\left(\frac{a}{b}\right)^n.$$

Multiplicando ambos os lados por b^n temos

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

Como $\binom{n}{i} = \binom{n}{n-i}$, segue que

$$(a+b)^n = a^n + \binom{n}{1}a^{n-1}b + ... + \binom{n}{n-1}ab^{n-1} + b^n$$

■

Corolário 1.1.1 *Dados $a, b \in \mathbb{R}$ e $n \in \mathbb{N}$. Tem-se que* $(a-b)^n = a^n - \binom{n}{1}a^{n-1}b + ... + (-1)^{n-1}\binom{n}{n-1}ab^{n-1} + (-1)^n b^n$

Demonstração: Basta trocar b por $-b$ no teorema (1.1.1).

■

1.1.1 Divisibilidade

Dados dois números a e b, $a \neq 0$, diremos que a *divide* b e escrevemos $a|b$, quando existir $c \in \mathbb{Z}$ tal que $b = ca$. Neste caso, diremos também que a é um *divisor* ou um *fator* de b ou ainda que b é um *múltiplo* de a ou que b é *divisível* por a.

Proposição 1.1.2 *Se $a, b, c \in \mathbb{Z}$ são tais que $a|b$ e $a|c$, então para todo $m, n \in \mathbb{Z}$ $a|mb + yc$.*

Demonstração: Se $a|b$ e $a|c$, então temos que $b = k_1 a$ e $c = k_2 a$ para alguns $k_1, k_2 \in \mathbb{Z}$. Multiplicando as duas equações, respectivamente, por m e n, em seguida somando-as temos: $m(k_1 a)+n(k_2 a) = (mk_1+nk_2)a = mb+nc$. Portanto, $a|mb+nc$.

■

Observe que a proposição acima pode ser facilmente generalizada como segue:

Proposição 1.1.3 *Se $c \mid a_1, \ldots, a_n$, então $c \mid (a_1 x_1 + \ldots + a_n x_n)$, para quaisquer $x_1, \ldots, x_n \in \mathbb{Z}$*

Proposição 1.1.4 *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}\cup 0$. Temos que $a+b$ divide $a^{2n+1}+b^{2n+1}$.*

Demonstração: Vamos provar esse resultado por indução sobre n. Note que a afirmação é verdadeira para $n = 0$, pois claramente $a + b$ divide $a^1 + b^1 = a + b$. Suponhamos, agora, que $(a + b)|(a^{2n+1} + b^{2n+1})$. Escrevamos:

$$\begin{aligned} a^{2(n+1)+1} + b^{2(n+1)+1} &= a^2 a^{2n+1} - b^2 a^{2n+1} + b^2 a^{2n+1} + b^2 b^{2n+1} \\ &= (a^2 - b^2)a^{2n+1} + b^2(a^{2n+1} + b^{2n+1}) \end{aligned}$$

Como $a+b$ divide $a^2-b^2 = (a+b)(a-b)$ e, por hipótese de indução, $a+b|a^{2n+1}+b^{2n+1}$, decorre das igualdades acima e da proposição(1.1.2), que $a + b|a^{2(n+1)+1} + b^{2(n+1)+1}$. Portanto, pelo Princípio de Indução o resultado vale para todo $n \in \mathbb{N}$.

■

Proposição 1.1.5 *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Temos que $(a + b)|(a^{2n} - b^{2n})$.*

Demonstração: (Por indução)

A afirmação é verdadeira para $n = 1$, pois $a + b$ divide $a^2 - b^2 = (a - b)(a + b)$. Suponhamos, agora, que $(a + b)|a^{2n} - b^{2n}$. Escrevamos:

$$\begin{aligned} a^{2(n+1)} - b^{2(n+1)} &= a^2a^{2n} - b^2a^{2n} + b^2a^{2n} - b^2b^{2n} \\ &= (a^2 - b^2)a^{2n} + b^2(a^{2n} - b^{2n}). \end{aligned}$$

Como $(a+b)|a^2 - b^2$ e, por hipótese, $(a+b)|a^{2n} - b^{2n}$, decorre das igualdades acima e da Proposição(1.1.2) que $(a + b)|a^{2(n+1)} + b^{2(n+1)}$, o que estabelece, pelo Princípio da Indução, o resultado para todo $n \in \mathbb{N}$.

■

Divisão Euclidiana

Teorema 1.1.1 *[Divisão Euclidiana] Sejam a e b dois números inteiros, com $b \neq 0$. Existem dois, únicos, números inteiros q e r tais que*

$$a = bq + r, \text{ com } 0 \leq r < |b|$$

Demonstração: Considere o conjunto

$$X = \{x = a - by, y \in \mathbb{Z}\} \cap (\mathbb{N} \cup \{0\}).$$

Primeiramente provaremos a existência. Ora, o conjunto X é não vazio pois pela propriedade arquimediana, existe $n \in \mathbb{Z}$ tal que $n(-b) > -a$, logo $a - nb > 0$. Além disso, por definição, o conjunto X é limitado inferiormente por 0. Logo, pelo princípio da boa ordenação, temos que X possui um menor elemento que denotaremos por r. Como $r \in X$, existe $q \in \mathbb{Z}$ tal que

$$r = a - bq. \tag{1.1}$$

Evidentemente que $r \geq 0$. Vamos mostrar que $r < |b|$. Suponhamos, por absurdo, que $r \geq |b|$. Portanto, existe $m \in \mathbb{N} \cup \{0\}$ tal que

$$r = |b| + m. \tag{1.2}$$

Por (1.1) e (1.2) temos que $m = a - b(q \pm 1)$, onde $(q \pm 1) \in \mathbb{Z}$. Logo, $m \in X$ mas, $0 \leq m < r$. Isto é um absurdo já que r é o menor elemento de X.

Para provarmos a unicidade suponhamos que $a = bq + r$ e $a = bq' + r'$, onde $q, q', r, r' \in \mathbb{Z}, 0 \leq r < |b|$ e $0 \leq r' < |b|$. Assim, temos que $-|b| < -r \leq r' - r \leq r' < |b|$. Logo $|r' - r| < |b|$. Por outro lado, $b(q - q') = r' - r$, o que implica

$$|b||q - q'| = |r' - r| < |b|.$$

Como $b \neq 0$ temos que $|b| \neq 0$, então a desigualdade acima só vale quando $|q-q'| = 0$ e desse modo $q = q'$, consequentemente $r = r'$.

■

Nas condições do teorema acima, os números q e r são chamados, respectivamente, de *quociente* e de *resto* da divisão de a por b. Dado um número natural b, a unicidade do quociente e do resto na divisão euclidiana por b nos permitem definir duas importantes funções que descrevemos a seguir.

Denotado por $q_b(a)$ o quociente da divisão do número a por b, definimos a *função quociente* por b como segue:

$$\begin{aligned} q_b : \mathbb{Z} &\to \mathbb{Z} \\ a &\mapsto q_b(a) \end{aligned}$$

O inteiro $q_b(a)$ pode ser interpretado como o maior inteiro menor ou igual do que o número racional $\frac{a}{b}$. Será chamado de *parte inteira* do número racional $\frac{a}{b}$ e será denotado pelo símbolo $\left[\frac{a}{b}\right]$.

A segunda função determinada pela divisão euclidiana é a *função resto*, definida a seguir

$$\begin{aligned} r_b : \mathbb{Z} &\to \mathbb{Z} \\ a &\mapsto r_b(a) \end{aligned}$$

Veremos uma aplicação da função resto que será bastante utilizada do decorrer deste trabalho.

Proposição 1.1.6 *Fixado um número natural $m \geq 2$, pode-se sempre escrever um número qualquer n, de modo único, na forma $n = mk+r$, onde $k, r \in \mathbb{Z}$ e $0 \leq r < m$.*

Por exemplo, todo número inteiro n pode ser escrito em uma, e somente uma, das seguintes formas: $2k$ ou $2k+1$. Ou, ainda, todo número inteiro n pode ser escrito em uma, e somente uma, das seguintes formas: $3k$, $3k+1$, ou $3k+2$. Ou, ainda, todo número inteiro n pode ser escrito em uma, e somente uma, das seguintes formas: $4k$, $4k+1$, $4k+2$, ou $4k+3$.

1.1.2 Máximo Divisor Comum

Dados dois números inteiros a e b, arbitrários, um número inteiro d será dito um *divisor comum* de a e b se $d|a$ e $d|b$. Diremos que um número inteiro $d \geq 0$ é o *máximo divisor comum* (mdc) de a e b, se possuir as seguintes propriedades:

i) d é um divisor comum de a e b, e

ii) d é divisível por todo divisor comum de a e b. (Se c é um divisor comum de a e b, então $c|d$).

Observe que o mdc de dois números, quando existe, é único. (Veremos que sempre existe o mdc de dois inteiros). Denotaremos mdc de a e b por (a, b). Observe ainda que dados $a, b \in \mathbb{Z}$

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

Propriedades do MDC

Lema 1.1.1 *Dados $a, b, n \in \mathbb{Z}$. Se existe $(a, b + na)$, então (a, b) existe e $(a, b) = (a, b + na)$.*

Demonstração: Sejam $f = (a, b+na)$ e $g = (a, b)$, então $f \mid a$ e $f \mid (b+na)$. Pela proposição (1.1.2) segue que $f|(b - na + na)$. Logo $f \mid a$ e $f \mid b$. Como $g = (a, b)$ então $f \mid g$. Por outro lado, já que $g = (a, b)$ então $g \mid a$ e $g \mid b$. Novamente, pela proposição (1.1.2) $g \mid a$ e $g \mid (b + na)$. Portanto, $g \mid f$, pois $f = (a, b + na)$. Como $f, g \geq 0$, $f \mid g$ e $g \mid f$ temos que $f = g$.

■

Antes de apresentarmos outros resultados, definamos os conjuntos

$$I(a, b) = \{xa + yb; x, y \in \mathbb{Z}\}$$

onde $a, b \in \mathbb{Z}$ e

$$d\mathbb{Z} = \{ld; l \in \mathbb{Z}\}.$$

Teorema 1.1.2 *Se $a, b \in \mathbb{Z}$, ambos não nulos simultaneamente e $d = minI(a, b) \cap \mathbb{N}$, então*

i) d é o mdc de a e b; e

ii) $I(a, b) = d\mathbb{Z}$.

Demonstração:
i) Seja c um divisor de a e b, logo c divide todos os números inteiros da forma $xa+yb$. Portanto, c divide todos os elementos de $I(a, b)$ e, obviamente, de $I(a, b) \cap \mathbb{N}$ assim, $c|d$. Vamos mostrar agora que d divide todos os elementos de $I(a, b)$. Seja $z \in I(a, b)$ e suponha, por absurdo, que $d \nmid z$. Logo, pela divisão euclidiana de z por d temos,

$$z = dq + r, com\ 0 < r < d. \tag{1.3}$$

Como $z = xa + yb$ e $d = ma + nb$, para alguns $x, y, n, m \in \mathbb{Z}$, segue-se de (2.30) que

$$\begin{aligned} r = z - dq &= (xa + yb) - (ma + nb)q \\ &= xa - maq + yb - nqb \\ &= (x - mq)a + (y - nq)b. \end{aligned}$$

Logo $r \in I(a, b) \cap \mathbb{N}$, o que é um absurdo, pois $d = minI(a, b) \cap \mathbb{N}$ e $r < d$. Portanto d divide todos os elementos de $I(a, b)$. Em particular, $d|a$ e $d|b$. Portanto $d = (a, b)$.
ii) Inicialmente observe que todo elemento de $I(a, b)$ é divisível por d, assim temos que $I(a, b) \subset d\mathbb{Z}$. Por outro lado, para todo $ld \in d\mathbb{Z}$, com $l \in \mathbb{Z}$, temos que existem $m, n \in \mathbb{Z}$ tal que $ld = l(ma + nb) = (lm)a + (ln)b \in I(a, b)$. Portanto, $d\mathbb{Z} \subset I(a, b)$. Logo, $I(a, b) = d\mathbb{Z}$.

■

Corolário 1.1.2 *Quaisquer que sejam $a, b \in \mathbb{Z}$, não ambos nulos, e $n \in \mathbb{N}$, tem-se que*

$$(na, nb) = n(a, b)$$

Demonstração: Sabemos que $I(na, nb) = nI(a, b)$ e como $\min(nI(a, b) \cap \mathbb{N}) = n \min(I(a, b) \cap \mathbb{N})$, pelo teorema (1.1.2) $minI(a, b) \cap \mathbb{N} = (a, b)$ e $min(nI(a, b) \cap \mathbb{N}) = (na, nb)$, logo

$$(na, nb) = n(a, b).$$

■

Corolário 1.1.3 *Dados $a, b \in \mathbb{Z}$, não ambos nulos, tem-se que*

$$\left(\frac{a}{(a, b)}, \frac{b}{(a, b)}\right) = 1.$$

Demonstração: Como $(a, b) \mid a$ e $(a, b) \mid b$ então $\dfrac{a}{(a, b)}$ e $\dfrac{b}{(a, b)}$ são inteiros. Portanto, fazendo $n = (a, b)$ e trocando a por $\dfrac{a}{(a, b)}$ e b por $\dfrac{b}{(a, b)}$ no corolário(1.1.2), temos

$$(a, b) = \left((a, b)\frac{a}{(a, b)}, (a, b)\frac{b}{(a, b)}\right) = (a, b)\left(\frac{a}{(a, b)}, \frac{b}{(a, b)}\right)$$

dividindo tudo por $(a, b) \neq 0$, temos

$$\left(\frac{a}{(a, b)}, \frac{b}{(a, b)}\right) = 1.$$

■

Dois números inteiros a e b serão ditos *primos entre si*, ou *coprimos*, se $(a, b) = 1$

Proposição 1.1.7 *Dois números inteiros são primos entre si se, e somente se, existem números inteiros m e n tais que $ma + nb = 1$.*

Demonstração: Suponhamos que a e b são primos entre si, ou seja, $(a, b) = 1$. Pelo teorema (1.1.2), existem números inteiros m e n tais que $ma + nb = (a, b) = 1$. Reciprocamente, suponha que existam números inteiros m e n tais que $ma + nb = 1$. Como $d = (a, b)$, temos que $d|(ma + nb)$, então $d|1$, e portanto, $d = 1$.

■

Proposição 1.1.8 *Sejam a, b e c números inteiros. Se $a|bc$ e $(a, b) = 1$, então $a|c$.*

Demonstração: Se $a|bc$, então existe $k \in \mathbb{Z}$ tal que $bc = ak$. Se $(a, b) = 1$, então, pela proposição (1.1.7), temos que existem $m, n \in \mathbb{Z}$ tais que

$$ma + nb = 1. \tag{1.4}$$

Multiplicando a equação (2.31) por c temos

$$c = mac + nbc.$$

Substituindo bc por ak temos

$$c = mac + nak = a(mc + nk)$$

portanto, $a|c$.

■

A noção de mdc pode ser generalizada como a seguir.

Definição 1.1.1 *Um número natural d será dito mdc de n números inteiros dados, $a_1, \ldots, a_n$, não todos nulos, se possuir as seguintes propriedades:*
i) d é um divisor comum de $a_1, \ldots, a_n$.
ii) Se c é um divisor comum de $a_1, \ldots, a_n$, então $c \mid d$.

Os inteiros $a_1, \ldots, a_n$ são primos entre si, ou coprimos, se $(a_1, \ldots, a_n) = 1$.

Teorema 1.1.3 *[Teorema de Bézout] Sejam $a_1, \ldots, a_n$ inteiros não nulos. Se*

$$S = \left\{ \sum_{i=1}^{n} a_i x_i;\ x_i \in \mathbb{Z},\ \forall\ 1 \leq i \leq n \right\},$$

então $S = d\mathbb{Z}$ onde $d = (a_1, \ldots, a_n)$. Em particular, existem números inteiros $u_1, \ldots, u_n$ tais que

$$(a_1, \ldots, a_n) = a_1 u_1 + \ldots + a_n u_n.$$

Demonstração: Como d divide $a_1 x_1 + \ldots + a_n x_n$ para todos $x_1, \ldots, x_n \in \mathbb{Z}$, temos que $S \subset d\mathbb{Z}$. Vamos mostrar que $d\mathbb{Z} \subset S$. Note que S contém inteiros positivos; de fato, fazendo $x_1 = \ldots = x_{n-1} = 0$ e $x_n = a_n$, por exemplo, concluímos que

$$a_n^2 = a_1 x_1 + a_2 x_2 + \ldots + a_n x_n \in S.$$

Como S contém inteiros positivos, existe um menor inteiro positivo d' em S. Basta então mostrar que $d' = d$, pois assim seguirá que $d \in S$ e como todo múltiplo de um elemento de S pertence a S teremos então que $d\mathbb{Z} \subset S$.
Inicialmente, observemos que $d' \mid a_1, \ldots, a_n$. De fato, como $d' \in S$, existem $u_1, u_2, \ldots, u_n \in \mathbb{Z}$ tais que $d' = a_1 u_1 + a_2 u_2 + \ldots + a_n u_n$. Agora, seja $a_1 = d'q + r$, com $q, r \in \mathbb{Z}$ e $0 \leq r < d'$. Então

$$\begin{aligned} r &= a_1 - d'q \\ &= a_1 - (a_1 u_1 + a_2 u_2 + \ldots + a_n u_n)q \\ &= a_1(1 - u_1 q) + a_2(-u_2 q) + \ldots + a_n(-u_n q), \end{aligned}$$

assim, $r \in S$. Se $0 < r < d'$, teríamos uma contradição ao fato de ser d' o menor inteiro positivo pertencente a S. Logo, $r = 0$ e $d' \mid a_1$. Analogamente, $d' \mid a_2, \ldots, a_n$. Por fim, como d' é um divisor comum de $a_1, a_2, \ldots, a_n$, para mostrarmos que $d' = d$ basta que seja $d' \geq d$. Mas, se $a_1 = dq_1, a_2 = dq_2, \ldots, a_n = dq_n$, com $q_1, q_2, \ldots, q_n \in \mathbb{Z}$, então

$$\begin{aligned} d' &= a_1 u_1 + a_2 u_2 + \ldots + a_n u_n \\ &= dq_1 u_1 + dq_2 u_2 + \ldots + dq_n u_n \\ &= d(q_1 u_1 + q_2 u_2 + \ldots + q_n u_n), \end{aligned}$$

ou seja, $0 < d \mid d'$. Logo, $d \leq d'$.

■

Corolário 1.1.4 *Sejam $a_1, a_2, \ldots, a_n$ inteiros não nulos dados e d seu mdc. Então, $d = 1$ se, e somente se, existirem inteiros $u_1, u_2, \ldots, u_n$ tais que $a_1u_1 + a_2u_2 + \ldots + a_nu_n = 1$.*

Demonstração: Se $d = 1$, o teorema de Bézout garante a existência de inteiros $u_1, u_2, \ldots, u_n$ como pede no enunciado. Reciprocamente, sejam $u_1, u_2, \ldots, u_n$ inteiros como no enunciado. Como $d \mid a_1, a_2, \ldots, a_n$, segue da generalização da proposição (1.1.2) que $d \mid (a_1u_1 + a_2u_2 + \ldots + a_nu_n)$, isto é, $d \mid 1$. Logo $d = 1$

■

Corolário 1.1.5 *Temos que:*

i) Se $(a, c) = 1$, então $(a, bc) = (a, b)$.

ii) Se $(a, b) = 1$, então $(a^m, b^n) = 1$, para todos $n, m \in \mathbb{N} \cup \{0\}$.

Demonstração:
i) Sejam $d = (a, b)$ e $d' = (a, bc)$. De $d \mid b$, segue que $d \mid bc$. Assim, $d \mid a$ e $d \mid bc$, portanto, $d \mid (a, bc) = d'$. Vamos mostrar agora que $d' \mid d$: Como $(a, c) = 1$ segue da proposição (1.1.7) que existem $m, n \in \mathbb{Z}$ tais que $ma + nc = 1$ e, daí, multiplicando toda a equação por b temos que $a(mb) + (bc)n = b$; mas, como $d' \mid a$ e $d' \mid bc$ segue que $d' \mid b$. Então, $d' \mid a$ e $d' \mid b$, ou seja, $d' \mid (a, b) = d$. Logo $d' = d$.
ii) Como $(a, b) = 1$, o teorema de Bézout garante a existência de $x, y \in \mathbb{Z}$ tais que $ax + by = 1$. Portanto, segue da fórmula de expansão binomial que

$$1 = (ax + by)^n = \sum_{k=0}^{n-1} \binom{n}{k} (ax)^{n-k}(by)^k + (by)^n = aq + b^n y^n,$$

onde $q = \sum_{k=0}^{n-1} \binom{n}{k} a^{n-k-1}x^{n-k}(by)^k$. Daí, pelo corolário (1.1.4), segue que $(a, b^n) = 1$. Agora, como $(a, b^n) = 1$, o teorema de Bézout garante a existência de $r, s \in \mathbb{Z}$ tais que $ar + b^n s = 1$. Assim, pela expansão binomial temos

$$1 = (ar + b^n s)^m = (ar)^m + \sum_{k=1}^{m} \binom{m}{k} (ar)^{m-k}(b^n s)^k = a^m r^m + tb^n,$$

onde $t = \sum_{k=1}^{m} \binom{m}{k} (ar)^{m-k}((b^n)^{k-1}s^k)$. Novamente, pelo corolário (1.1.4), concluímos que $(a^m, b^n) = 1$.

■

Proposição 1.1.9 *Sejam $a, b, c \in \mathbb{Z}$. A equação $ax + by = c$ admite solução em números inteiros se, e somente se, $(a, b)|c$.*

Demonstração: Ora, pelo teorema (1.1.2) temos que

$$I(a,b) = \{ma + nb;\ m, n \in \mathbb{Z}\} = (a,b)\mathbb{Z}.$$

Evidentemente a equação $ax+by = c$ possui uma solução se, e somente se $c \in I(a,b)$, o que é equivalente a $c \in (a,b)\mathbb{Z}$, ou seja, $c = (a,b)k$ para algum $k \in \mathbb{Z}$. Portanto, a equação $ax + by = c$ admite solução se, e somente se, $(a,b)|c$.

■

1.1.3 Números Primos

Um número natural maior que 1 que só possui como divisores positivos 1 e ele próprio é chamado de número primo. Um número natural maior que 1 e que não é primo será dito composto.

Proposição 1.1.10 *[Lema de Euclides] Sejam $a, b, p \in \mathbb{Z}$, com p primo. Se $p|ab$, então $p|a$ ou $p|b$.*

Demonstração: Ora, se $p \nmid a$ então $(p,a) = 1$. Portanto, pela proposição (1.1.8) segue-se que $p|b$.

■

Corolário 1.1.6 *Se $p_1, ..., p_n$ são números primos e, se $p|p_1 \dots p_n$, então $p = p_i$ para algum $i = 1, \dots, n$.*

Demonstração: Como sabemos que se $p \mid p_i$ com p e p_i primos como no enunciado, então $p = p_i$. Basta apenas aplicar o Lema de Euclides (proposição (1.1.10)) e indução sobre n.

■

Vejamos um resultado de muita importância para a matemática pois caracteriza todo número natural em termos dos números primos, ou seja, ele mostra que os números primos são suficientes para gerar todos os números naturais.

Teorema 1.1.4 *[Teorema Fundamental da Aritmética] Todo número natural maior do que 1 ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos.*

Demonstração: Pelo princípio de indução matemática temos: Se $n = 2$, nada há a fazer.
Suponhamos o resultado válido para todo número natural menor do que n e vamos provar que vale para n. Se o número n é primo, nada temos a demonstrar. Suponhamos, então, que n não é primo, ou seja, n é composto. Logo, existem números naturais n_1 e n_2 tais que $n = n_1 n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$. Pela hipótese de indução, temos que existem números primos $p_1, \dots, p_r$ e $q_1, \dots, q_r$ tais que

$n_1 = p_1 \dots p_r$ e $n_2 = q_1 \dots q_s$. Portanto, $n = p_1 \dots p_r q_1 \dots q_s$. Para a unicidade suponha que tenhamos $n = p_1 \dots p_r = q_1 \dots q_s$, onde os p_i e os q_j são números primos. Como $p_1 \mid q_1 \dots q_s$, pelo corolário (1.1.6) temos que $p_1 = q_j$ para algum j, que após reordenamento de $q_1, \dots, q_s$, podemos supor que seja q_1. Portanto,

$$p_2 \dots p_r = q_2 \dots q_s$$

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

■

1.2 Congruências

Seja m um número natural. Diremos que dois inteiros a e b são congruentes módulo m se os restos de sua divisão Euclidiana por m são iguais. Quando os inteiros a e b são congruentes módulo m, escreve-se

$$a \equiv b \bmod m$$

Quando a relação $a \equiv b \bmod m$ for falsa, diremos que a e b não são congruentes, ou que são incongruentes módulo m. Escrevemos nesse caso

$$a \not\equiv b \bmod m$$

Decorre imediatamente da definição que a congruência módulo um inteiro fixado m é uma relação de equivalência. Observe o resultado a seguir:

Proposição 1.2.1 *Seja $m \in \mathbb{N}$. Para todos $a, b, c \in \mathbb{Z}$, tem-se que*

i) $a \equiv a \bmod m$

ii) Se $a \equiv b \bmod m$, *então* $b \equiv a \bmod m$

iii) Se $a \equiv b \bmod m$ *e* $b \equiv c \bmod m$, *então* $a \equiv c \bmod m$

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

Proposição 1.2.2 *Suponha que $a, b, m \in \mathbb{Z}$, com $m > 1$. Tem-se que $a \equiv b \bmod m$ se, e somente se, $m \mid b - a$.*

Demonstração: Sejam $a = mq + r$, com $0 \leq r < m$ e $b = mq' + r'$, com $0 \leq r' < m$, as divisões euclidianas de a e b por m, respectivamente. Logo,

$$b - a = m(q' - q) + (r' - r).$$

Portanto, $a \equiv b \bmod m$ se, e somente se, $r = r'$, o que, em vista da igualdade acima, é equivalente a dizer que $m \mid b - a$, já que $|r - r'| < m$.

■

Observação 1.2.1 *Note que todo número inteiro é congruente módulo m ao seu resto pela divisão euclidiana por m e, portanto, é congruente módulo m a um dos números $0, 1, \ldots, m-1$. Além disso, dois desses números distintos não são congruentes módulo m. Portanto, para achar o resto da divisão de um número a por m, basta achar o número natural r dentre os números $0, 1, \ldots, m-1$ que seja congruente a a módulo m.*

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

Proposição 1.2.3 *Sejam $a, b, c, d, m \in \mathbb{Z}$, com $m > 1$.*

i) Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $a + c \equiv b + d \bmod m$.

ii) Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $ac \equiv bd \bmod m$.

Demonstração: Suponhamos que $a \equiv b \bmod m$ e $c \equiv d \bmod m$. Logo, temos que $m|b-a$ e $m|d-c$.
i) $m|((b-a)+(d-c)) = ((b+d)-(a+c))$. Logo, $a + c \equiv b + d \bmod m$.
ii) $m|d(b-a)+a(d-c) = (bd-ac)$. Logo, $ac \equiv bd \bmod m$.

■

Proposição 1.2.4 *Sejam $a, b, c, m \in \mathbb{Z}$, com $m > 1$. Temos que*

$$ac \equiv bc \bmod m \Leftrightarrow a \equiv b \bmod \frac{m}{(c,m)}$$

Demonstração: Como $\dfrac{m}{(c,m)}$ e $\dfrac{c}{(c,m)}$ são coprimos, temos que

$$ac \equiv bc \bmod m \Leftrightarrow m \mid (b-a)c \Leftrightarrow \frac{m}{(c,m)} \mid (b-a)\frac{c}{(c,m)}$$

$$\Leftrightarrow \frac{m}{(c,m)} \mid b-a \Leftrightarrow a \equiv b \bmod \frac{m}{(c,m)}.$$

■

Capítulo 2

Primos em Progressões Aritméticas

Neste capítulo apresentaremos alguns resultados que nos auxiliarão na demonstração da infinidade de primos em determinadas progressões aritméticas. Mostraremos inicialmente alguns resultados mais simples, e no decorrer do texto apresentaremos casos um pouco mais gerais cujas demonstrações necessitam de alguns conceitos menos elementares da matemática.

2.1 Casos particulares do Teorema de Dirichlet

Vejamos nesta seção algumas variantes mais simples do teorema de Dirichlet. Antes de mostrarmos o primeiro exemplo de progressões aritméticas satisfazendo as condições do teorema de Dirichlet iremos ver um resultado suficiente para tal demonstração.

O teorema a seguir foi provado por Euclides a mais de 2000 anos e é considerada uma obra de arte entre os matemáticos.

Teorema 2.1.1 *Existem infinitos números primos*

Demonstração: Suponha que existe apenas um número finito de primos $p_1, p_2, \cdots, p_r$. Considere o número natural

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_r + 1.$$

Pelo teorema fundamental da aritmética, o número n possui um fator primo p que, portanto, deve ser um dos $p_1, p_2, \ldots, p_r$ e, consequentemente, divide o produto $p_1 \cdot p_2 \cdot \ldots \cdot p_r$. Mas isto implica que p divide 1, o que é absurdo.

■

Podemos agora ver o nosso primeiro caso particular do teorema de Dirichlet.

A sequência dos números ímpares

Teorema 2.1.2 *Na progressão aritmética* $1, 3, 5, \ldots, 2n+1, \ldots$ *existem infinitos números primos.*

Demonstração: Ora, todo número primo maior que 2 é ímpar e como, pelo teorema (2.1.1), existem infinitos primos e na sequência $1, 3, 5, \ldots, 2n+1, \ldots$ estão todos os números ímpares, então existem infinitos primos na progressão aritmética $S = \{2n+1\}_{n\in\mathbb{N}}$.

■

Vejamos a seguir as demonstrações de três tipos de progressões aritméticas contendo infinitos números primos que já podem ser demonstradas com as ferramentas que temos.

A progressão aritmética $S = \{4n+3\}_{n\in\mathbb{N}}$

Teorema 2.1.3 *Na progressão aritmética $3, 7, 11, 15, \ldots, 4n+3, \ldots$ existem infinitos números primos.*

Demonstração: Pela observação (1.2.1) todo primo ímpar é da forma $4n+1$ ou $4n+3$. Em seguida, observemos que o conjunto $A = \{4n+1; n \in \mathbb{N}\}$ é fechado multiplicativamente. De fato,

$$(4n+1)(4n'+1) = 4(4nn' + n + n') + 1.$$

Suponhamos agora, por absurdo, que haja apenas um número finito de números primos $3 < p_1 < \ldots < p_k$ da forma $4n+3$. Portanto, o número $a = 4(p_1.p_2 \ldots p_k)+3$ não é divisível por nenhum dos números primos $3, p_1, p_2, \ldots, p_k$ e, consequentemente, sua decomposição em fatores primos só pode conter primos da forma $4n+1$. Assim, a é da forma $4n+1$, o que é uma contradição, pois é da forma $4n+3$.

■

A progressão aritmética $S = \{6n+5\}_{n\in\mathbb{N}}$

Teorema 2.1.4 *Na progressão aritmética $5, 11, 17, 23, \ldots, 6n+5, \ldots$ existem infinitos números primos.*

Demonstração: Analogamente ao caso anterior observe inicialmente que todo número ímpar é da forma $6n+1$, $6n+3$, $6n+5$ e como todos os números da forma $6n+3$ são divisíveis por 3 então todo primo ímpar, diferente de 3, é da forma $6n+1$ ou $6n+5$.
Em seguida, note que o conjunto $A = \{6n+1; n \in \mathbb{N}\}$ é fechado multiplicativamente. Agora suponha, por absurdo, que haja somente uma quantidade finita de primos da forma $6n+5$, digamos $5, p_1, p_2, \ldots, p_k$ e seja

$$\alpha = 6(p_1 p_2 \ldots p_k) + 5$$

Observe que α não é divisível por nenhum dos primos $2, 3, 5, p_1, p_2, \ldots, p_k$, então sua decomposição em fatores primos só pode conter primos da forma $6n+1$. Como $A = \{6n+1; n \in \mathbb{N}\}$ é fechado multiplicativamente, então α é da forma $6n+1$, o que é um absurdo, pois α é da forma $6n+5$.

■

A progressão aritmética $S = \{3n+2\}_{n\in\mathbb{N}}$

Teorema 2.1.5 *Na progressão aritmética* $2, 5, 8, 11, \ldots, 3n+2, \ldots$ *existem infinitos números primos.*

Demonstração: Analogamente ao caso anterior observe que todo primo, diferente de 3, é da forma $3m+1$ ou $3m+2$.
Suponhamos, por absurdo, que haja uma quantidade finita de primos da forma $3m+2$, digamos $2, p_1, p_2, \ldots, p_k$ e seja

$$\beta = 3(p_1 p_2 \ldots p_k) + 2.$$

Como β não é divisível por nenhum dos primos $2, 3, p_1, p_2, \ldots p_k$, sua decomposição em fatores primos só contém primos da forma $3m+1$. E como $B = \{3n+1; n \in \mathbb{N}\}$ é fechado multiplicativamente, então β é da forma $3n+1$, o que é um absurdo, pois β é da forma $3m+2$.

■

Vejamos agora alguns resultados que embora apareçam de forma aleatória serão úteis para a demonstração do nosso próximo exemplo.

Desde muito tempo antes de Cristo, os chineses já sabiam que $p \mid 2^p - 2$, com p primo. O grande matemático Pierre de Fermat generalizou esse resultado, enuciando o famoso *pequeno teorema de fermat*. Os chineses também acreditavam que se p fosse composto, então $p \nmid 2^p - 2$. Veremos que isto nada mais é do que uma recíproca do teorema quando $a = 2$. Muitos matemáticos acreditavam que essa recíproca era verdadeira até que em 1819, Sarrus mostrou que o número composto 341 divide $2^{341} - 2$.

Para provar o teorema necessitamos do resultado a seguir.

Lema 2.1.1 *Seja* p *um número primo. Os números* $\binom{p}{i}$, *onde* $0 < i < p$, *são todos divisíveis por* p.

Demonstração: Ora, se $i = 1$ então $p \mid \binom{p}{1} = p$. Vamos, portanto, consideram apenas $1 < i < p$. Assim, $i! \mid p(p-1)\ldots(p-i+1)$. Mas $(i!, p) = 1$ pois $(i, p) = 1$, então $i! \mid (p-1)\ldots(p-i+1)$, e como

$$\binom{p}{i} = \frac{p!}{i!(p-i)!} = p\frac{(p-1)\ldots(p-i+1)}{i!}$$

logo $p \mid \binom{p}{i}$ para todo i tal que $0 < i < p$.

■

Pequeno Teorema de Fermat

Teorema 2.1.6 *[Pequeno teorema de Fermat] Dado um número primo p, tem-se que p divide o número $a^p - a$, para todo $a \in \mathbb{Z}$.*

Demonstração: Observe que $2 \mid a(a-1)$. Considere $a \geq 0$. Vamos provar por indução sobre a. Para $a = 0$ o resultado é óbvio pois $p \mid 0$. Supondo o resultado válido para a, iremos prová-lo para $a+1$. Pelo Binômio de Newton temos

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

Pelo lema anterior (2.1.1) $p \mid \binom{p}{1}, p \mid \binom{p}{2}, \ldots, p \mid \binom{p}{p-1}$. Por hipótese de indução, $p \mid (a^p - a)$. Logo, $p \mid ((a+1)^p - (a+1))$. Além disso, se $a < 0$ então $a^p = -(-a)^p \equiv -(-a) = a \bmod p$.

■

Antes do nosso próximo resultado essencial para apresentarmos mais um caso particular do teorema da Dirichlet vejamos uma proposição que nos será útil em sua demonstração.

Proposição 2.1.1 *Seja $a \in \mathbb{Z}$. Mostre que*
a) Para cada $n \in \mathbb{N}$, existe $m \in \mathbb{Z}$ tal que $(a-1)^{2n+1} = ma - 1$.
b) Para cada $n \in \mathbb{N}$, existe $m \in \mathbb{Z}$ tal que $(a-1)^{2n} = ma + 1$.

Demonstração:
a) Pelo corolário (1.1.1) temos

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

Colocando a em evidência no segundo membro temos:

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

Basta agora fazer $m = \left(a^{2n} - \binom{2n+1}{1}a^{2n-1} + \binom{2n+1}{2}a^{2n-2} + (-1)^{2n}\binom{2n+1}{2n}\right) \in \mathbb{Z}$.
b) Análogo ao item *a)*.

■

Lema 2.1.2 *Seja $x \in \mathbb{N}$ com $x \geq 2$. Todo divisor ímpar de x^2+1 é da forma $4n+1$.*

Demonstração: Pelo fato do conjunto $A = \{4n+1 \ ; \ n \in \mathbb{N}\}$ ser fechado multiplicativamente, basta provarmos o resultado para os divisores primos ímpares de x^2+1. Suponha, então, que $p|(x^2+1)$, com $p > 2$. Então, para algum $\lambda \in \mathbb{N}$, temos que $x^2 + 1 = \lambda p$. Assim,

$$x^2 = \lambda p - 1.$$

Como $p-1$ é par, temos que $\frac{p-1}{2} \in \mathbb{N}$. Portanto, elevando à potência $\frac{p-1}{2}$ ambos os lados da igualdade acima, temos

$$x^{p-1} = (x^2)^{\frac{p-1}{2}} = (\lambda p - 1)^{\frac{p-1}{2}}$$

Logo, pela proposição (2.1.1), temos que para alguns $\mu, \mu' \in \mathbb{N}$,

$$x^{p-1} = (x^2)^{\frac{p-1}{2}} = (\lambda p - 1)^{\frac{p-1}{2}} = \begin{cases} \mu p + 1, \text{ se } \frac{p-1}{2} \text{ é par;} \\ \mu' p - 1, \text{ se } \frac{p-1}{2} \text{ é ímpar.} \end{cases}$$

Se

$$x^{p-1} = \mu' p - 1,$$

então

$$x^{p-1} - 1 = \mu' p - 2. \tag{2.1}$$

Como $p \mid x^2 + 1$, segue que p não divide x. Logo, pelo Pequeno Teorema de Fermat, temos que $p \mid x^{p-1} - 1$ e, consequentemente, por (2.32), $p \mid 2$ o que é uma contradição já que consideramos p um primo ímpar. Portanto a única alternativa possível é que $\frac{p-1}{2}$ seja par. Vamos mostrar que para $\frac{p-1}{2}$ ser par p tem que ser da forma $4n+1$. Ora, basta fazer $p = 4n+3$, ou seja, $\frac{(4n+3)-1}{2} = 2n+1$ é ímpar. Logo, p tem que ser da forma $4n+1$.

■

Teorema 2.1.7 *Na progressão aritmética* $1, 5, 9, 13, \ldots, 4n+1, \ldots$ *existem infinitos números primos.*

Demonstração: Suponha, por absurdo, que haja um número finito $p_1, \ldots, p_k$ de primos da forma $4n+1$. Considere o número

$$a = 4p_1^2 \cdot \ldots \cdot p_k^2 + 1.$$

Ora, nenhum dos primos $p_1, p_2, \ldots, p_k$ divide a, então todo divisor primo de a é da forma $4n+3$, absurdo, pois pelo lema (2.1.2) todo divisor ímpar de x^2+1 é da forma $4n+1$.

■

Iremos agora desenvolver mais instrumentos que nos auxiliarão na demonstração do nosso próximo caso particular do teorema de Dirichlet.

Inicialmente introduziremos um tipo de número especial, os números de Fermat devido a Pierre de Fermat. Os números de Fermat são os números da forma

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

Em 1640, Fermat lançou a conjectura, em uma carta escrita para Marin Mersenne, onde afirmava que esses números eram todos primos. Mais tarde, Euler demonstrou que essa conjectura era falsa ao mostrar que o quinto número de Fermat era composto. No exemplo a seguir mostramos que dois números de Fermat distintos são coprimos.

Proposição 2.1.2 *Se $n \neq m$, então*

$$(2^{2^n}+1, 2^{2^m}+1) = 1.$$

Demonstração: Para facilitar os cálculos usaremos a notação $(F_m, F_n) = 1$. Inicialmente vamos provar, por indução, que

$$\prod_{i=0}^{n-1} F_i = F_n - 2 \tag{2.2}$$

Para $n = 1$ o resultado é válido, pois $F_0 = F_1 - 2$. Suponhamos o resultado válido para todo $n \in \mathbb{N} \cup \{0\}$, assim

$$\begin{aligned}
\prod_{i=0}^{n} F_i &= \left(\prod_{i=0}^{n-1} F_i\right) F_n \\
&= (F_n - 2)F_n \\
&= (2^{2^n} - 1)(2^{2^n} + 1) \\
&= 2^{2^{n+1}} - 1 \\
&= 2^{2^{n+1}} + 1 - 2 \\
&= F_{n+1} - 2.
\end{aligned}$$

Supondo, sem perda de generalidade, $m > n$ e usando (2.2) temos:

$$\prod_{i=0}^{m-1} F_i = F_m - 2.$$

Então,

$$F_m - \prod_{i=0}^{m-1} F_i = 2.$$

Logo, se t é um divisor de F_m e F_n para todo $m, n \in \mathbb{N} \cup \{0\}$, então $t \mid 2$, mas F_m é sempre ímpar o que garante que t só pode ser 1. Portanto, $(F_m, F_n) = 1$.

■

2.1.1 Teorema de Euler

Veremos agora um importante teorema na Teoria dos números, o teorema de Euler. Para isso serão necessários alguns conceitos e resultados da aritmética dos restos. Mais a frente voltaremos a falar deste teorema que será essencial também para o estudo das propriedades que aparecerão na seção 2.2 dos polinômios ciclotômicos.

Proposição 2.1.3 *Sejam $a, m \in \mathbb{Z}$, com $m > 1$. A congruência $aX \equiv 1 \bmod m$ possui solução se, e somente se, $(a, m) = 1$. Além disso, se $x_0 \in \mathbb{Z}$ é uma solução, então x é uma solução da congruência se, e somente se, $x \equiv x_0 \bmod m$.*

Demonstração: A congruência acima tem uma solução x_0 se, e somente se, $m|ax_0 - 1$, o que equivale a dizer que a equação diofantina $aX - mY = 1$ possui solução em números inteiros. Em virtude da proposição (1.1.9), isso ocorre se, e somente se, $(a, m) = 1$.
Por outro lado, se x_0 e x são soluções da congruência $aX \equiv 1 \bmod m$, então $ax \equiv ax_0 \bmod m$ e $(a, m) = 1$, o que implica, em virtude da proposição (1.2.4), que $x \equiv x_0 \bmod m$.
Observe que, se x_0 é solução da congruência $aX \equiv 1 \bmod m$, e $x \equiv x_0 \bmod m$, então x é também solução da mesma congruência, pois

$$ax \equiv ax_0 \equiv 1 \bmod m$$

■

Um sistema reduzido de resíduos módulo m é um conjunto de números inteiros $r_1, \ldots, r_s$ tais que
a) $(r_i, m) = 1$, para todo $i = 1, \ldots, s$;
b) $r_i \not\equiv r_j \bmod m$, se $i \neq j$;

Designaremos por $\varphi(m)$ o número de elementos de um sistema reduzido de resíduos módulo $m > 1$, que corresponde a quantidade de números naturais entre 0 e $m - 1$ que são primos com m. Pondo $\varphi(1) = 1$, isso define uma importante função

$$\varphi : \mathbb{N} \to \mathbb{N}$$

chamada de função fi de Euler.
Pela definição, temos que $\varphi(m) \leq m - 1$, para todo $m \geq 2$.
Além disso, se $m \geq 2$, então $\varphi(m) = m - 1$ se, e somente se, m é um número primo.

Proposição 2.1.4 *Seja $r_1, \ldots, r_{\varphi(m)}$ um sistema reduzido de resíduos módulo m e seja $a \in \mathbb{Z}$ tal que $(a, m) = 1$. Então, $ar_1, \ldots, ar_{\varphi(m)}$ é um sistema reduzido de resíduos módulo m.*

Demonstração: Primeiramente vamos mostrar que $(ar_i, m) = 1$. Ora, sabemos que $(a, m) = 1$ e como $r_1, \ldots, r_{\varphi(m)}$ é um sistema reduzido de resíduos módulo m temos que $(r_i, m) = 1$ assim pelo corolário (1.1.5)(i), $(ar_i, m) = (r_i, m) = 1$. Para mostrar que $ar_i \not\equiv ar_j \bmod m$, se $i \neq j$ suponhamos, por absurdo, que $ar_i \equiv ar_j \bmod m$. Como $(a, m) = 1$ temos que $r_i \equiv r_j \bmod m$, o que é um absurdo já que $r_1, \ldots, r_{\varphi(m)}$ é um sistema reduzido de resíduos módulo m. Logo, $ar_i \not\equiv ar_j \bmod m$.

■

Teorema 2.1.8 (Euler) *Sejam $m, a \in \mathbb{Z}$ com $m > 1$ e $(a, m) = 1$. Então,*

$$a^{\varphi(m)} \equiv 1 \bmod m$$

Demonstração: Seja $r_1, \ldots, r_{\varphi(m)}$ um sistema reduzido de resíduos módulo m. Logo, pela proposição (2.1.4) $ar_1, \ldots, ar_{\varphi(m)}$ formam um sistema reduzido de resíduos módulo m. Então, dado ar_i existe um único r_j com $1 \leq j \leq \varphi(m)$ tal que $ar_i \equiv r_j \bmod m$. Logo,

$$a^{\varphi(m)} r_1.r_2 \ldots r_{\varphi(m)} = ar_1.ar_2 \ldots ar_{\varphi(m)} \equiv r_1.r_2 \ldots r_{\varphi(m)} \bmod m$$

Como $(r_1.r_2 \ldots r_{\varphi(m)}, m) = 1$, temos que $a^{\varphi(m)} \equiv 1 \bmod m$.

■

Dentre muitas aplicações do teorema de Euler tem-se a de calcular o resto da divisão de uma potência a^n por um número natural $m > 1$. Basta achar um expoente $h \in \mathbb{N}$ de modo que $a^h \equiv 1 \bmod m$, pois, se $n = hq + r$ é a divisão euclidiana de n por h, teremos $a^n \equiv a^{hq}a^r \equiv a^r \bmod m$. Nem sempre é possível achar tal número h. Veremos no resultado a seguir quando isso acontece.

Proposição 2.1.5 *Sejam dados $a, m \in \mathbb{Z}$, com $m \geq 2$. Existe $h \in \mathbb{N}$ tal que $a^h \equiv 1 \bmod m$ se, e somente se, $(a, m) = 1$.*

Demonstração: Começando pela volta temos que se $(a, m) = 1$, o Teorema de Euler nos garante a existência do expoente h, basta fazer $h = \varphi(m)$, pois $a^h = a^{\varphi(m)} \equiv 1 \bmod m$. Reciprocamente, suponhamos $a^h \equiv 1 \bmod m$ para algum $h \in \mathbb{N}$. Se $h = 1$, temos que $a \equiv 1 \bmod m$, assim $m \mid (a - 1)$. Então, existe $k \in \mathbb{Z}$ tal que $a - 1 = mk$ ou equivalentemente $a - mk = 1$, que, por sua vez, só tem solução se $(a, m) \mid 1$ o que implica que $(a, m) = 1$. Já para $h > 1$, temos que para $x = a^{h-1}$ a congruência $ax \equiv 1 \bmod m$ admite solução. Portanto, pela proposição (2.1.3) temos que $(a, m) = 1$.

■

Sendo $a, m \in \mathbb{Z}$, com $m > 1$ e $(a, m) = 1$. A proposição (2.1.5) garante que

$$\{i \in \mathbb{N};\ a^i \equiv 1 \bmod m\} \neq \emptyset.$$

Nesse caso, podemos definir a ordem de a com respeito a m como sendo o número natural

$$\mathrm{ord}_m(a) = min\{i \in \mathbb{N}; a^i \equiv 1 \bmod m\}.$$

Note ainda que para $(a, m) \neq 1$ o conjunto $\{i \in \mathbb{N};\ a^i \equiv 1 \bmod m\}$ é vazio. Nesse caso, a proposição (2.1.5) nos mostra que não faz sentido falar em ordem de a com respeito a m. Um dos resultados básicos mais importantes que estão relacionados ao conceito de ordem é o seguinte:

Lema 2.1.3 *Sejam $a, m \in \mathbb{Z}$, com $m > 1$ e $(a, m) = 1$. Temos que $a^t \equiv 1 \bmod m$ se, e somente se, $\mathrm{ord}_m(a) \mid t$.*

Demonstração: Como $a^{\,\mathrm{ord_m(a)}} \equiv 1 \bmod m$, se $\mathrm{ord}_m(a) \mid t$, existe $k \in \mathbb{Z}$ tal que $t = k\ \mathrm{ord}_m(a)$. Então,

$$a^t = a^{k\ \mathrm{ord}_m(a)} \equiv 1 \bmod m.$$

Por outro lado, se $a^t \equiv 1 \bmod m$, pela divisão euclidiana existem $q, r \in \mathbb{Z}$ tais que $t = q\ \mathrm{ord}_m(a) + r$, onde $0 \leq r < \mathrm{ord}_m(a)$. Então,

$$1 \equiv a^t \equiv a^{q\ \mathrm{ord}_m(a)+r} \equiv \left(a^{\,\mathrm{ord}_m(a)}\right)^q a^r \equiv a^r \bmod m.$$

Logo,

$$a^r \equiv 1 \bmod m.$$

Como $0 \leq r < \mathrm{ord}_m(a)$, pela minimalidade de $\mathrm{ord}_m(a)$ temos que $r = 0$ então, $\mathrm{ord}_m(a) \mid t$.

■

Como consequência do lema acima temos que se $a, m \in \mathbb{Z}$, com $m > 1$ e $(a, m) = 1$ então $\text{ord}_m(a) \mid \varphi(m)$.

No nosso próximo passo veremos um resultado que nos dá informações sobre os divisores dos números de Fermat.

Proposição 2.1.6 *Todo divisor natural de F_n é da forma $2^{n+1}\alpha + 1$, onde $\alpha \in \mathbb{N} \cup \{0\}$.*

Demonstração: Ora, o produto de números da forma $2^{n+1}\alpha + 1$ é também dessa forma. Assim, pelo teorema fundamental da aritmética, basta provar o resultado para os divisores primos de F_n.
Seja p um divisor primo de $F_n = 2^{2^n} + 1$. Então, $2^{2^n} \equiv -1 \mod p$, com p ímpar. Pelo lema (2.1.3) se $\text{ord}_p(2) \mid 2^n$ então $2^{2^n} \equiv 1 \mod p$ e consequentemente $-1 \equiv 1 \mod p$ o que seria um absurdo, portanto, $\text{ord}_p(2) \nmid 2^n$. Assim,

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

Novamente, pelo Lema (2.1.3), $\text{ord}_p(2) \mid 2^{n+1}$ e, como $\text{ord}_p(2) \nmid 2^n$, pela definição da ordem segue-se que $\text{ord}_p(2) = 2^{n+1}$.
Por outro lado, pelo Pequeno Teorema de Fermat temos que $2^{p-1} \equiv 1 \mod p$ assim, $\text{ord}_p(2) \mid p - 1$. Logo, $2^{n+1} \mid p - 1$ e, portanto, $p = 2^{n+1}\alpha + 1$ onde $\alpha \in \mathbb{N} \cup \{0\}$.

■

Vimos anteriormente que em uma carta escrita a Marin Mersenne, Fermat lançou uma conjectura onde afirmava que os números da forma $F_n = 2^{2^n} + 1, n = 0, 1, 2, \ldots$ eram todos números primos e só depois Euler provou que não era verdade mostrando que para $n = 5$ a afirmação dada por Fermat era falsa. Vejamos, no exemplo a seguir, uma aplicação da proposição acima onde damos uma prova de que o quinto número de fermat é de fato composto.

Exemplo 2.1.1 *O quinto número de Fermat ($F_5 = 2^{2^5} + 1$) não é primo.*

Solução: De fato, pela proposição (2.1.6) sabemos que pra ser divisor primo de F_5 o número tem que ser da forma $2^6k + 1$, com $k \in \mathbb{N} \cup \{0\}$, ou seja, para encontrar um possível divisor de F_5 basta escolher o valor de k. Vejamos os 10 primeiros candidatos a divisores de F_5: 65, 129, 193, 257, 321, 385, 449, 513, 577, 641, dos quais 193, 257, 449, 577 e 641 são primos. Faremos os testes para os números 257 e 641. Ora, para $p = 257$ temos

$$2^8 = 256 \equiv -1 \mod 257$$

então

$$(2^8)^4 = 2^{32} \equiv (-1)^4 = 1 \mod 257$$

portanto,

$$2^{32} + 1 \equiv 1 + 1 = 2 \not\equiv 0 \mod 257$$

o que significa $257 \nmid F_5$. Já para $p = 641$ temos

$$2^{16} = 65536 \equiv 154 \bmod 641$$

então,

$$(2^{16})^2 = 2^{32} \equiv 154^2 = 23716 \equiv 640 \bmod 641$$

logo,

$$2^{32} + 1 \equiv 640 + 1 \equiv 0 \bmod 641$$

portanto $641 \mid F_5$

■

Agora já temos ferramentas suficientes para provar mais um caso particular do teorema de Dirichlet como veremos a seguir.

A progressão aritmética $S = \{2^r n + 1\}_{n \in \mathbb{N}}$

Teorema 2.1.9 *Na progressão aritmética de primeiro termo* 1 *e razão* 2^r*, para* $r \in \mathbb{N}$ *fixo, existem infinitos números primos.*

Demonstração: Seja F_n o n-ésimo número de Fermat. Como, pelo teorema fundamental da aritmética, todo número natural maior do que 1 possui pelo menos um divisor primo, segue-se que cada número de Fermat tem, pelo menos, um divisor primo e, como $(F_n, F_m) = 1$ se $n \neq m$, esses divisores são dois a dois distintos. Assim, fazendo $r = n + 1$ na proposição (2.1.6) temos que existem infinitos primos divisores de F_n para n variando em $\mathbb{N}$. Portanto existem infinitos números primos na progressão aritmética $S = \{1 + 2^r n\}_{n \in \mathbb{N}}$ onde $r \in \mathbb{N}$ é fixo.

■

Veremos agora alguns resultados como o teorema de Wilson, a resolução de congruências lineares, o teorema de Thue, o teorema Chinês dos Restos, algumas propriedades das congruências quadráticas, resíduos quadráticos, o critério de Euler, o símbolo de Legendre e um teorema envolvendo somas de quadrados, que serão utilizados na demonstração da infinidade de primos na progressão aritmética $S = \{8n + 5\}_{n \in \mathbb{N}}$.

2.1.2 Teorema de Wilson

O teorema a seguir apesar de ter sido provado pela primeira vez por Lagrange, foi atribuído a Wilson. Este teorema nos fornece uma caracterização para os números primos, porém, essa caracterização não é prática pois não se conhece um algoritmo eficiente para se calcular rapidamente o fatorial de um número grande e consequentemente testar a primaridade desse número.

Teorema 2.1.10 *Se* p *é um número primo, então* $(p-1)! \equiv -1 \bmod p$.

Demonstração: Para $p = 2$ e $p = 3$ o resultado é óbvio. Consideremos então $p \geq 5$ primo. Para todo $i \in \{1, \ldots, p-1\}$, pela proposição (2.1.3), a congruência $iX \equiv 1 \bmod p$ possui única solução módulo p, pois o conjunto $\{1, 2, \ldots, p-1\}$ forma um sistema reduzido de resíduos módulo p. Portanto, dado $i \in \{1, \ldots, p-1\}$ existe um único $j \in \{1, \ldots, p-1\}$ tal que $ij \equiv 1 \bmod p$.

Se $i^2 \equiv 1 \bmod p$ onde $i \in \{1, \ldots, p-1\}$, então $p \mid i^2 - 1$, assim $p \mid i - 1$ ou $p \mid i + 1$, o que só pode ocorrer se $i = 1$ ou $i = p - 1$. Portanto,

$$2 \cdot 3 \cdot \ldots \cdot (p-2) \equiv 1 \bmod p$$

e, multiplicando ambos os lados da congruência por $p - 1$ temos,

$$1 \cdot 2 \cdot \ldots \cdot (p-2) \cdot (p-1) \equiv p - 1 \equiv 1 \bmod p$$

e como $p - 1 \equiv -1 \bmod p$, temos que $(p-1)! \equiv -1 \bmod p$.

■

A título de facilitar o entendimento das ideias apresentadas na demonstração do teorema de Wilson, analisaremos o exemplo onde $p = 11$, ou seja, vamos mostrar que $(11-1)! \equiv -1 \bmod 11$. Observe inicialmente que, $1 \equiv 1 \bmod 11$ e $10 \equiv -1 \bmod 11$. Além disso, nenhum dos números $2, 3, 4, 5, 6, 7, 8, 9, 10$ é congruente a 1 ou -1 módulo 11. Pela proposição (2.1.3), dado $i \in \{2, 3, 4, 5, 6, 7, 8, 9\}$ existe um único $j \in \{2, 3, 4, 5, 6, 7, 8, 9\}$ tal que $ij \equiv 1 \bmod 11$. Por exemplo,

$$2 \cdot 6 \equiv 1 \bmod 11$$

$$3 \cdot 4 \equiv 1 \bmod 11$$

$$5 \cdot 9 \equiv 1 \bmod 11$$

$$7 \cdot 8 \equiv 1 \bmod 11$$

Assim,

$$2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \equiv 1 \bmod 11$$

então

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \equiv 10 \equiv -1 \bmod 11$$

Portanto, $(11-1)! \equiv -1 \bmod 11$

Como aplicação do teorema de Wilson vejamos o exemplo a seguir.

Exemplo 2.1.2 *Sejam p um número primo e $m, n \in \mathbb{N} \cup \{0\}$ tais que $m+n = p-1$. Tem-se que*

$$m!n! \equiv (-1)^{n+1} \bmod p$$

Solução: Seja $0 \leq n \leq p - 1$. Temos que

$$p - 1 \equiv -1 \bmod p$$

$$p - 2 \equiv -2 \bmod p$$

$$\vdots$$

$$p - n \equiv -n \bmod p$$

Portanto,

$$(p-n)\dots(p-2)(p-1) \equiv (-1)^n n! \bmod p$$

fazendo $m = p - 1 - n$, temos

$$(p-1)! = 1 \cdot 2 \cdot \ldots \cdot (p-1-n)(p-n)\dots(p-2)(p-1) \equiv m!(-1)^n n! \bmod p \quad (2.3)$$

Pelo teorema de Wilson sabemos que $(p-1)! \equiv -1 \bmod p$, então

$$(p-1)!(-1)^n \equiv (-1)^{n+1} \bmod p \quad (2.4)$$

Logo, de (2.33) e (2.4) temos que

$$m!n! \equiv (-1)^{n+1} \bmod p.$$

■

Note que o exemplo acima é na verdade uma generalização do teorema de Wilson bastando para isso substituir $n = 0$ e $m = p - 1$.

2.1.3 Resolução de Congruências Lineares

Aqui veremos alguns resultados sobre a resolução de congruências do tipo $aX \equiv b \bmod m$ onde $a, b, m \in \mathbb{Z}, m > 1$.

Inicialmente daremos um critério para saber quais congruências lineares admitem solução.

Proposição 2.1.7 *Dados $a, b, m \in \mathbb{Z}$, com $m > 1$, a congruência*

$$aX \equiv b \bmod m$$

possui solução se, e somente se, $(a, m) \mid b$.

Demonstração: Suponhamos que a congruência $aX \equiv b \bmod m$ tenha uma solução x. Então, existe um y tal que $ax - b = my$. Portanto, a equação $aX - mY = b$ admite solução. Logo, pela proposição (1.1.9) $(a, m) \mid b$. Reciprocamente, suponha que $(a, m) \mid b$. Novamente pela proposição (1.1.9) a equação $aX - mY = b$ que equivale a $ax \equiv b \bmod m$ admite uma solução x, y. Logo, x é solução da congruência.

■

Observe que se x_0 for uma solução da congruência $aX \equiv b \bmod m$, qualquer x tal que $x \equiv x_0 \bmod m$ também é, uma vez que $ax \equiv ax_0 \equiv c \bmod m$. Note ainda que sendo $(a, m) = 1$, então a congruência $aX \equiv b \bmod m$ possui uma única solução módulo m. Assim, a congruência $aX \equiv 1 \bmod m$, com $(a, m) = 1$, admite uma única solução módulo m. Chamaremos esta solução de *inverso multiplicativo módulo m*.

Corolário 2.1.1 *Sejam $m > 1$ e R' um conjunto reduzido de resíduos módulo m. Se $b \in \mathbb{Z}$, então, para todo $r \in R'$, a congruência $rX \equiv b \bmod m$ possui uma única solução em R'.*

Demonstração: Ora, como $r \in R'$, então $(r, m) = 1$, o que equivale a dizer que a congruência $rX \equiv b \bmod m$ tem uma única solução módulo m. Além disso toda solução x em $\mathbb{Z}$ é tal que $(x, m) = 1$ e, portanto, tem um único representante módulo m em R'.

■

Proposição 2.1.8 *Toda congruência $aX \equiv b \bmod m$ que possui solução é equivalente a uma congruência da forma*

$$X \equiv c \bmod n$$

Demonstração: Ora, sabemos que se a congruência

$$aX \equiv b \bmod m$$

possui solução, então $d = (a, m)$ divide b. Portanto, fazendo

$$a' = \frac{a}{d}, \quad b' = \frac{b}{d}, \quad n = \frac{m}{d}$$

temos a seguinte congruência equivalente

$$a'X \equiv b' \bmod n, \quad com\ (a', n) = 1,$$

e sendo $c = a''b'$, onde a'' é o inverso multiplicativo de a' módulo n, temos que

$$X \equiv c \bmod n,$$

■

2.1.4 Teorema de Thue

O teorema de Thue garante a existência de soluções não triviais em algumas congruências lineares, com valores positivos e relativamente pequenos.

Teorema 2.1.11 (Thue) *Sejam $m > 1$ um número natural não quadrado e $a \in \mathbb{Z}$, com $(a, m) = 1$. A congruência $aX \equiv Y \bmod m$ possui uma solução $(x, y) \in \mathbb{Z}^2$ tal que $0 < |x| < \sqrt{m}$ e $0 < |y| < \sqrt{m}$.*

Demonstração: Considere a congruência $aX \equiv Y \bmod m$. Como m é não quadrado existe um $k \in \mathbb{Z}$ tal que $k - 1 < \sqrt{m} < k$. Consideremos o conjunto

$$S = \{(s, t) \in \mathbb{Z}^2 \ ; \ 0 \leq s < k \text{ e } 0 \leq t < k\}.$$

Sabemos que o número de inteiros não congruentes entre si módulo m é no máximo m e como S tem k^2 elementos então existem $(s_1, t_1), (s_2, t_2) \in S$, com $s_1 \neq s_2$ ou $t_1 \neq t_2$, tais que

$$as_1 \equiv t_1 \bmod m \quad e \quad as_2 \equiv t_2 \bmod m.$$

Assim,

$$a(s_1 - s_2) \equiv (t_1 - t_2) \bmod m. \tag{2.5}$$

Se $s_1 = s_2$ em (2.5), $m \mid (t_2 - t_1)$ e, como $|t_1 - t_2| < k$, teríamos $t_1 = t_2$. Analogamente, se $t_1 = t_2$, então $a(s_1 - s_2) \equiv 0 \bmod m$, e como $(a, m) = 1$ temos $(s_1 - s_2) \equiv 0 \bmod m$. Assim, teríamos $s_1 = s_2$. Dessa maneira devemos ter $s_1 \neq s_2$ e $t_1 \neq t_2$. Assim, podemos fazer $x = s_1 - s_2 \neq 0$ e $y = t_2 - t_1 \neq 0$. Logo,

$$|x| = |s_1 - s_2| \leq k - 1 < \sqrt{m}$$

e

$$|y| = |t_2 - t_1| \leq k - 1 < \sqrt{m},$$

portanto, (x, y) é uma solução da congruência $aX \equiv Y \bmod m$.

■

Estamos agora interessados em resolver sistemas de congruências da forma:

$$a_i X \equiv b_i \bmod n_i, \quad i = 1, \ldots, r$$

Para que tal sistema possua solução, é necessário que $(a_i, n_i) \mid b_i$, para todo $i = 1, \ldots, r$. Pela proposição (2.1.8), o sistema acima é equivalente a um sistema da forma

$$X \equiv c_i \bmod m_i, \quad i = 1, \ldots, r.$$

2.1.5 Teorema Chinês dos Restos

O teorema a seguir ficou conhecido como teorema Chinês dos Restos pelo fato de que matemáticos chineses já o conhecia desde a antiguidade. Neste trabalho ele tem o objetivo de mostrar como resolver sistemas de congruências lineares.

Teorema 2.1.12 *[Teorema Chinês dos Restos] Se $(m_i, m_j) = 1$ para todo par m_i, m_j com $i \neq j$, então o sistema*

$$X \equiv c_i \bmod m_i, \quad i = 1, \ldots, r \tag{2.6}$$

possui uma única solução módulo $M = m_1 m_2 \ldots m_r$. As soluções são $x = M_1 y_1 c_1 + \ldots + M_r y_r c_r + tM$, onde $t \in \mathbb{Z}$, $M_i = \frac{M}{m_i}$ e y_i é solução de $M_i Y \equiv 1 \bmod m_i$, $i = 1, \ldots, r$.

Demonstração: Vamos inicialmente provar que x é uma solução simultânea do sistema (2.6). Como $m_i \mid M_j$, quando $i \neq j$ temos que

$$x = M_1 y_1 c_1 + \ldots + M_r y_r c_r \equiv M_i y_i c_i \bmod m_i. \tag{2.7}$$

Além disso, se y_i é solução de $M_iY \equiv 1 \bmod m_i$ então

$$M_i y_i \equiv 1 \bmod m_i$$

Assim,

$$M_i y_i c_i \equiv c_i \bmod m_i \tag{2.8}$$

De (2.7) e (2.8) temos que

$$x = M_1 y_1 c_1 + \ldots + M_r y_r c_r \equiv M_i y_i c_i \equiv c_i \bmod m_i.$$

Portanto, x é solução simultânea para o nosso sistema (2.6)

Agora vamos mostrar que essa solução é única. Se x' é outra solução para o nosso sistema (2.6), então $x \equiv x' \bmod m_i$, $\forall i = 1, \ldots, r$. Como $(m_i, m_j) = 1$, para $i \neq j$, então $m_1 m_2 \ldots m_r = M \mid x - x'$, ou equivalentemente $x \equiv x' \bmod M$.

■

O exemplo a seguir é uma aplicação interessante do teorema Chinês dos restos. Ele mostra que podemos ter intervalos arbitrariamente longos entre dois primos consecutivos.

Exemplo 2.1.3 *Utilizando o teorema Chinês dos restos mostre que dado $n > 1$ inteiro, existem n naturais consecutivos, todos compostos.*

Solução: Escolha n primos distintos $p_1, p_2, \ldots, p_n$ e considere o sistema de congruências

$$\begin{cases} x \equiv -1 \bmod p_1^2 \\ x \equiv -2 \bmod p_2^2 \\ \quad\vdots \\ x \equiv -n \bmod p_n^2 \end{cases}$$

Como $p_1, p_2, \ldots, p_n$ são dois a dois primos entre si, o teorema Chinês dos Restos garante a existência de $m \in \mathbb{N}$ satisfazendo o sistema acima. Portanto, $p_j^2 \mid (m + j)$ para $1 \leq j \leq n$, de maneira que $m + 1, m + 2, \ldots, m + n$ são naturais consecutivos e compostos.

■

Iremos agora apresentar dois resultados relacionados com a resolução de congruências quadráticas que serão usados na demonstração do teorema sobre soma de quadrados.

2.1.6 Congruências Quadráticas

Estamos interessados em resolver congruências do tipo

$$AY^2 + BY + C \equiv 0 \bmod N \tag{2.9}$$

onde A, B, C são números inteiros e $N > 1$ com $N \nmid A$.
Por completamento de quadrados temos que resolver (2.11) é equivalente a resolver

$$(2AY + B)^2 \equiv B^2 - 4AC \bmod N.$$

Portanto, estamos interessados em encontrar critérios de existência de soluções da equação

$$X^2 \equiv a \bmod N.$$

Vejamos, a seguir, como tratar de congruências deste tipo.

Proposição 2.1.9 *Seja $n = p_1^{r_1} \dots p_s^{r_s}$ a decomposição de n em fatores primos, a congruência $x^2 \equiv a \bmod n$ admite solução se, e somente se, cada congruência, separadamente, da família*

$$x^2 \equiv a \bmod p_i^{r_i}, \quad i = 1, 2, \dots, s, \tag{2.10}$$

admitir solução.

Demonstração: Suponhamos que a congruência $X^2 \equiv a \bmod n$ admita uma solução x, então $p_1^{r_1} \dots p_s^{r_s} = n \mid (x^2 - a)$ e consequentemente $p_i^{r_i} \mid (x^2 - a) \ \ \forall i \in \{1, 2, \dots, s\}$, o que equivale a $X^2 \equiv a \bmod p_i^{r_i}$. Reciprocamente, se para cada i, a congruência correspondente em (2.10) tiver uma solução a_i, então

$$a_i^2 \equiv a \bmod p_i^{r_i}. \tag{2.11}$$

Por outro lado, o teorema chinês dos restos garante-nos que o sistema de congruências simultâneos $X \equiv a_i \bmod p_i^{r_i}$, possui uma solução x. Assim, $x \equiv a_i \bmod p_i^{r_i}$, então

$$x^2 \equiv a_i^2 \bmod p_i^{r_i}. \tag{2.12}$$

De (2.12) e (2.11) temos que

$$x^2 \equiv a \bmod p_i^{r_i}.$$

Ora, se $p_i^{r_i} \mid x^2 - a$, então o produto dos $p_i^{r_i}$ divide $x^2 - a$, pois $(p_i^{r_i}, p_j^{r_j}) = 1$ com $1 \leq i, j \leq s$ e $i \neq j$. Portanto,

$$x^2 \equiv a \mod n.$$

■

Vamos, a seguir, mostrar que a resolução de congruências do tipo (2.10) se reduz à resolução de congruências do tipo $X^2 \equiv a \bmod p$.

Proposição 2.1.10 *Sejam $a, p, r \in \mathbb{Z}$, onde p é um número primo ímpar e $r \geq 2$ tais que $(a, p) = 1$. A congruência $x^2 \equiv a \bmod p^r$ admite solução se, e somente se, a congruência $x^2 \equiv a \bmod p$ admite solução.*

Demonstração: Analogamente ao que foi feito na primeira parte da proposição anterior se $r \geq 2$ e x é uma solução de $X^2 \equiv a \bmod p^r$, sendo $a \equiv a' \bmod p^{r-1}$ então x também é uma solução de

$$X^2 \equiv a' \bmod p^{r-1}, \tag{2.13}$$

já que $p^{r-1} \mid p^r$.

Para a recíproca, primeiramente note que como $(a, p) = 1$, então $(a', p) = 1$. Se y é uma solução de (2.13), existe $k_1 \in \mathbb{Z}$ tal que $y^2 = a' + k_1 p^{r-1}$ e como $(a', p) = 1$ então $(y, p) = 1$. Temos também que $a = a' + k_2 p^{r-1}$, para algum $k_2 \in \mathbb{Z}$.

Fazendo $x = y + \lambda p^{r-1}$, onde $\lambda \in \mathbb{Z}$ vamos encontrar um λ que seja solução de $X^2 \equiv a \bmod p^r$, ou seja, um $\lambda \in \mathbb{Z}$ tal que $(y + \lambda p^{r-1})^2 \equiv a \bmod p^r$. Assim,

$$y^2 + 2\lambda y p^{r-1} + \lambda^2 p^{2(r-1)} \equiv a \mod p^r,$$

Substituindo y^2 por $a' + k_1 p^{r-1}$ e a por $a' + k_2 p^{r-1}$ temos

$$\begin{aligned} a' + k_1 p^{r-1} + 2\lambda y p^{r-1} + \lambda^2 p^{2(r-1)} &\equiv a' + k_2 p^{r-1} \bmod p^r \\ k_1 p^{r-1} + 2\lambda y p^{r-1} &\equiv k_2 p^{r-1} \mod p^r \\ k_1 + 2\lambda y &\equiv k_2 \mod p \\ 2\lambda y &\equiv k_2 - k_1 \mod p. \end{aligned}$$

Como $(y, p) = 1$, e p é um primo ímpar então $(2y, p) = 1$. Logo, a última congruência acima tem uma única solução $\lambda' \bmod p$. Portanto, teremos uma única solução $x = y + \lambda' p^{r-1}$ de $X^2 \equiv a \bmod p^r$. Analogamente ao que foi feito acima se $X^2 \equiv a \bmod p$ admite solução então $X^2 \equiv a \bmod p^r$ também admite.

■

2.1.7 Resíduos Quadráticos

Vimos que o problema da resolubilidade de uma congruência quadrática recai na resolubilidade ou não de congruências do tipo $X^2 \equiv a \bmod p$, onde p é primo e $p \nmid a$.

Seja a um número inteiro. Quando a congruência $X^2 \equiv a \bmod p$ possui alguma solução, diz-se que a é *resíduo quadrático módulo p*, caso contrário, diz-se que *a não é resíduo quadrático módulo p*.

Observe que a congruência $X^2 \equiv 2 \bmod 3$ não possui nenhuma solução, portanto, 2 não é resíduo quadrático módulo 3. Por outro lado, todo número natural a é resíduo quadrático módulo 2 (pequeno teorema de Fermat). O resultado a seguir nos diz que se p é um número primo ímpar e a congruência $X^2 \equiv a \bmod p$, onde $a \not\equiv 0 \bmod p$, possui uma solução, então ela possuirá uma outra solução, de modo que essas duas sejam as únicas soluções incongruentes entre si, módulo p.

Lema 2.1.4 *Sejam $p > 2$ um número primo e $a \in \mathbb{Z}$ tal que $(p, a) = 1$. Se $x_2 \in R = \{1, \ldots, p-1\}$ é solução da congruência $x^2 \equiv a \bmod p$, então $(x_2, p) = 1$ e $p - x_2$ também é solução, não congruente a x_2, e essas são as únicas soluções em R.*

Demonstração: Se $x_2 \in \mathbb{R}$ é solução da congruência então $x_2^2 \equiv a \bmod p$. Daí, temos que $(x_2, p) = (x_2^2, p) = (a, p) = 1$. Portanto, $p - x_2$ também é solução da congruência, uma vez que

$$(p - x_2)^2 \equiv x_2^2 \equiv a \bmod p.$$

Além disso, se $x_2 \equiv p - x_2 \bmod p$, teríamos que $p \mid 2x_2$ e como $(x_2, p) = 1$, teríamos $p \mid 2$, o que é um absurdo visto que p é um primo ímpar. Para mostrar que essas são as únicas soluções da congruência, consideremos $x_1 \in R$ e $x_2 \in R$ tal que $x_1^2 \equiv a \bmod p$ e $x_2^2 \equiv a \bmod p$. Logo, $x_1^2 \equiv x_2^2 \bmod p$ e, portanto, $p \mid x_1^2 - x_2^2$, o que implica $p \mid x_1 - x_2$ ou $p \mid x_1 + x_2$. Nesse caso, como $x_1, x_2 \in R^*$ só existem as possibilidades $p \mid 0$ ou $p \mid p$ o que implica $x_1 = x_2$ ou $x_1 = p - x_2$.

■

Observe que se $p > 2$ e $(a, p) = 1$, pelo pequeno teorema de Fermat temos que

$$p \mid a^{p-1} - 1 \Longrightarrow p \mid \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right).$$

Por outro lado, como $(a, p) = 1$ então p não pode dividir simultaneamente $\left(a^{\frac{p-1}{2}} - 1\right)$ e $\left(a^{\frac{p-1}{2}} + 1\right)$ pois se assim fosse p dividiria 2 já que

$$2a^{\frac{p-1}{2}} = \left(a^{\frac{p-1}{2}} - 1\right) + \left(a^{\frac{p-1}{2}} + 1\right).$$

Para determinar se $p \mid \left(a^{\frac{p-1}{2}} + 1\right)$ ou se $p \mid \left(a^{\frac{p-1}{2}} + 1\right)$ utilizaremos uma ferramenta conhecida como critério de Euler como veremos a seguir.

2.1.8 Critério de Euler

O critério de Euler é um teorema de suma importância na teoria dos resíduos quadráticos. Antes, porém, vejamos uma proposição da qual deduziremos o critério.

Proposição 2.1.11 *Sejam p um número primo ímpar e $a \in \mathbb{Z}$ tal que $(a, p) = 1$.*
i) Se $x^2 \equiv a \bmod p$ não tem solução, então

$$a^{\frac{p-1}{2}} \equiv -1 \bmod p.$$

ii) Se $x^2 \equiv a \bmod p$ tem solução, então

$$a^{\frac{p-1}{2}} \equiv 1 \bmod p.$$

Demonstração:
i) Seja $R^* = \{1, 2, \ldots, p-1\}$. Dado $r \in R^*$, o corolário (2.1.1) garante que a congruência $rX \equiv a \bmod p$ possui uma única solução $r' \in R^*$. Se a congruência $x^2 \equiv a \bmod p$ não tem solução, então $r' \neq r$. Agrupando os elementos de R^* aos pares temos

$$1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv a^{\frac{p-1}{2}} \bmod p$$

Logo, pelo teorema de Wilson

$$a^{\frac{p-1}{2}} \equiv -1 \bmod p$$

ii) Supondo que a congruência $x^2 \equiv a \bmod p$ tem solução, então existe $x_0 \in R^*$ tal que

$$x_0^2 \equiv a \bmod p$$

então

$$x_0^{p-1} = (x_0^2)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \bmod p. \tag{2.14}$$

Por outro lado, como $(a, p) = 1$, então $(x_0, p) = 1$. Portanto, o pequeno teorema de Fermat nos assegura que

$$x_0^{p-1} \equiv 1 \bmod p. \tag{2.15}$$

Assim, de (2.14) e (2.15) temos

$$a^{\frac{p-1}{2}} \equiv 1 \bmod p.$$

■

Podemos agora enunciar o critério.

Teorema 2.1.13 (Critério de Euler) *Seja p um número primo ímpar e $a \in \mathbb{Z}$ tal que $(a, p) = 1$, então*
i) $p \mid a^{\frac{p-1}{2}} - 1$ *se, e somente se, a é resíduo quadrático módulo p.*
ii) $p \mid a^{\frac{p-1}{2}} + 1$ *se, e somente se, a não é resíduo quadrático módulo p.*

Demonstração: Como, por definição, a é resíduo quadrático módulo p quando a congruência $X^2 \equiv a \bmod p$ possui alguma solução, então o critério decorre imediatamente da proposição anterior.

■

Vejamos um exemplo onde o critério de Euler se aplica eficientemente.

Exemplo 2.1.4 *Pelo pequeno teorema de fermat sabemos que $47 \mid 2^{46} - 1$ então $47 \mid (2^{23} - 1)(2^{23} + 1)$. Determine qual dos fatores é divisível por 47.*

Solução: Ora, pelo que foi discutido acima sabemos que $47 \mid (2^{23} - 1)$ ou $47 \mid (2^{23} + 1)$ não podendo dividir os dois fatores ao mesmo tempo. Observe que $7^2 \equiv 2 \bmod 47$, ou seja, 7 é solução da congruência $X^2 \equiv 2 \bmod 47$, portanto, 2 é resíduo quadrático módulo 47. Logo, pelo critério de Euler $47 \mid (2^{23} - 1)$.

■

2.1.9 Símbolo de Legendre

Introduziremos agora o símbolo de Legendre, uma notação que vai ser bastante eficiente no estudo dos resíduos quadráticos.

Se p é um número primo e a é um número inteiro tal que $p \nmid a$, define-se o símbolo de Legendre como:

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

Note que se a é ímpar, então $\left(\frac{a}{2}\right) = 1$. Se $p \nmid a$ então $\left(\frac{a^2}{p}\right) = 1$. Particularmente $\left(\frac{1}{p}\right) = 1$.

Vejamos algumas propriedades, relacionadas ao símbolo de Legendre, que nos ajudarão no desenvolvimento do conteúdo seguinte.

Proposição 2.1.12 *Sejam $a, b \in \mathbb{Z}$ e p um primo ímpar tal que $(a,p) = (b,p) = 1$. Tem-se que*

i) Se $a \equiv b \bmod p$, então $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

ii) $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \bmod p$

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

Demonstração:
(i) Como $a \equiv b \bmod p$, segue-se imediatamente que a congruência $X^2 \equiv a \bmod p$ tem solução se, e somente se, $X^2 \equiv b \bmod p$ tem solução.
(ii) Ora, pelo critério de Euler $p \mid a^{\frac{p-1}{2}} - 1$ ou $p \mid a^{\frac{p-1}{2}} + 1$, ou seja,

$$a^{\frac{p-1}{2}} \equiv (\pm 1) = \left(\frac{a}{p}\right) \bmod p$$

(iii) Pelo item (ii) temos que

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

Portanto, p divide $\left(\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) - \left(\frac{ab}{p}\right)\right)$ $(*)$. Por definição o símbolo de Legendre é 1 ou -1 então temos que $(*)$ só pode assumir um dos valores $-2, 0, 2$. Como p é um primo ímpar a única possibilidade para $(*)$ é 0. Logo,

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

■

Corolário 2.1.2 *Seja p um número primo ímpar. Temos que*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \begin{cases} 1, \text{ se } p = 4n+1 \\ -1, \text{ se } p = 4n+3 \end{cases}$$

Demonstração: Inicialmente note que a expressão $\left(\left(\frac{-1}{p}\right) - (-1)^{\frac{p-1}{2}}\right)$ só pode assumir um dos valores inteiros $-2, 0, 2$. Como p é um primo ímpar pelo item (ii) da proposição (2.1.12) temos que

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \bmod p \Rightarrow p \mid \left(\left(\frac{-1}{p}\right) - (-1)^{\frac{p-1}{2}}\right) \Rightarrow p \mid 0$$

logo,

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \begin{cases} 1, \text{ se } p = 4n+1 \\ -1, \text{ se } p = 4n+3 \end{cases}$$

pois,

$$p = 4n+1 \Rightarrow \ (-1)^{\frac{(4n+1)-1}{2}} = (-1)^{2n} = 1$$

e

$$p = 4n+3 \Rightarrow \ (-1)^{\frac{(4n+3)-1}{2}} = (-1)^{2n+1} = -1$$

■

2.1.10 Somas de quadrados

Antes de mostrarmos mais um caso particular do teorema de Dirichlet apresentaremos uma propriedade da teoria que estuda os números que podem ser escritos como soma de quadrados.

Teorema 2.1.14 *Para um número natural ímpar c, são equivalentes:*
i) Existem $m, n \in \mathbb{N}$, com $(n, m) = 1$ e de paridades distintas tais que $c = n^2 + m^2$
ii) A congruência $x^2 \equiv -1 \bmod c$ admite solução em $\mathbb{Z}$
iii) Os fatores primos de c são todos da forma $4k + 1$.

Demonstração:
$i) \Rightarrow ii)$ Seja $c = n^2 + m^2$ como no enunciado. Como $(n, m) = 1$ então $(n, c) = (m, c) = 1$. Consideremos agora a congruência $nX \equiv -m \bmod c$. Como $(n, c) = 1$, a proposição (2.1.7) nos assegura a existência de uma solução γ da congruência acima. Assim,

$$\begin{aligned} n\gamma &\equiv m \bmod c \\ n^2\gamma^2 &\equiv m^2 \bmod c \\ n^2\gamma^2 &\equiv -n^2 \bmod c \\ \gamma^2 &\equiv -1 \bmod c \end{aligned}$$

uma vez que $(n, c) = 1$ e $c = n^2 + m^2 \Rightarrow m^2 \equiv -n^2 \bmod c$. Logo, γ é uma solução da congruência $X^2 \equiv -1 \bmod c$.
$ii) \Rightarrow i)$ Primeiramente mostraremos que $c = n^2 + m^2$ onde n e m têm paridades distintas.
Seja $\alpha \in \mathbb{Z}$ uma solução da congruência $x^2 \equiv -1 \bmod c$, ou seja, $\alpha^2 + 1 \equiv 0 \bmod c$. Consequentemente,

$$\alpha^2 + 1 \equiv 0 \bmod c \tag{2.16}$$

Novamente, pela proposição (2.1.7) temos que $(\alpha, c) = 1$. Consideremos a congruência $\alpha X \equiv Y \bmod c$. Pelo teorema de Thue (2.1.11), existem $x, y \in \mathbb{Z}$ tais que

$$\alpha x \equiv y \bmod c \tag{2.17}$$

com $o < |x|, |y| \leq \sqrt{c}$.

Note que se trocarmos α por $-\alpha$ em (2.16) a congruência permanece igual. Portanto, podemos escolher $n = x$ e $m = y$ positivos, pois temos a liberdade de escolher o sinal de α com o objetivo de tornar os dois membros de (2.17) positivos.

Precisamos mostrar que $1 \leq n < \sqrt{c}$ ou $1 \leq m < \sqrt{c}$. Suponhamos, por absurdo, que $d = n = m = \sqrt{c}$, então $c = d^2$. Então, $\alpha d \equiv d \bmod c$ o que equivale a

$$(\alpha - 1)d \equiv 0 \bmod c \tag{2.18}$$

Como c é ímpar, $(\alpha, c) = 1$ e $(\alpha - 1)^2 \equiv -2\alpha \bmod c$ temos que

$$(\alpha - 1, c) = ((\alpha - 1)^2, c) = (2\alpha, c) = (\alpha, c) = 1$$

Assim, por (2.18) temos que $d \equiv 0 \bmod c$ o que é um absurdo já que $0 < d < c$. Fazendo as trocas $n = x$ e $m = y$ em (2.17) temos que $\alpha n \equiv m \bmod c$, então

$$n^2 + m^2 \equiv n^2 + \alpha^2 n^2 = (1 + \alpha^2)n^2 \equiv 0 \bmod c, \tag{2.19}$$

Como $1 \leq n < \sqrt{c}$ ou $1 \leq m < \sqrt{c}$ então

$$0 < n^2 + m^2 < 2c$$

Assim, por (2.19) temos que $n^2 + m^2 = c$, com n e m de paridades distintas, pois c ímpar. Finalmente, vamos mostrar que $(n, m) = 1$.

Sabemos que $\alpha m \equiv m \bmod c$ e $\alpha^2 \equiv -1 \bmod c$, então existem $s, t \in \mathbb{Z}$, que $m = \alpha n + sc$ e $\alpha^2 + 1 = tc$.
Portanto,

$$\begin{aligned} c = n^2 + m^2 &= n^2 + (\alpha n + sc)^2 \\ &= n^2 + \alpha^2 n^2 + 2\alpha nsc + s^2 c^2 \\ &= n^2(\alpha^2 + 1) + 2\alpha nsc + s^2 c^2 \\ &= n^2 tc + \alpha nsc + \alpha nsc + scsc \\ &= n^2 tc + \alpha nsc + (\alpha n + sc)sc \\ &= nc(nt + \alpha s) + msc \end{aligned}$$

Dividindo ambos os lados por c temos

$$1 = n(nt + \alpha s) + ms$$

Como tanto $(nt + \alpha s)$ quanto s são inteiros, pela proposição (1.1.7), $(n, m) = 1$
ii) $\Leftrightarrow$ *i)* Seja $c = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ a fatoração de c em primos. Como c é ímpar, cada primo p_i é ímpar. Pelas proposições (2.1.9) e (2.1.10), temos que a congruência $X^2 \equiv -1 \bmod c$ tem solução se, e somente se, cada congruência $X^2 \equiv -1 \bmod p_i$ tem solução, ou seja, -1 é resíduo quadrático módulo p_i o que equivale ao símbolo de legendre $\left(\frac{-1}{p_i}\right) = 1$ que, por sua vez, pelo corolário (2.1.2), equivale a dizer que cada primo p_i é da forma $4k_i + 1$

■

Teorema 2.1.15 *Existem infinitos primos da forma* $8n + 5$.

Demonstração: Sabemos que todo número pode ser escrito em uma das formas $8k, 8k+1, 8k+2, 8k+3, 8k+4, 8k+5, 8k+6, 8k+7$ então para ser ímpar ele deve ter uma das formas: $8k+1, 8k+3, 8k+5, 8k+7$.

Além disso, se m é ímpar então m^2 é da forma $8k+1$. Suponhamos, por absurdo, que haja apenas um número finito de primos $3, 5, p_1, p_2, \ldots, p_r$ da forma $8k+5$ onde p_r é o maior deles. Considere o número

$$\beta = (3.5.p_1 \ldots p_r)^2 + 4.$$

Como $(3.5.p_1 \ldots p_r)^2$ é o quadrado de um número ímpar então ele é da forma $8k+1$ e, portanto, β é da forma $8k+5$.

Pelo teorema (2.1.14) todo divisor de β é da forma $4k+1$, pois β é um número ímpar e soma dos quadrados de dois números coprimos de paridades distintas. Mas todo número da forma $4k+1$ é de uma das formas $8k+1$ ou $8k+5$. Como o conjunto $A = \{8k+1, k \in \mathbb{N}\}$ é fechado multiplicativamente, então α deve ter um fator primo $p_s \neq 3, 5, p_1, \ldots, p_r$ da forma $8k+5$ já que nenhum deles divide β. Portanto, $p_s > p_r$, o que é um absurdo, pois p_r é o maior primo da forma $8k+5$.

■

2.1.11 Lei da reciprocidade Quadrática

Vejamos agora, a *lei da reciprocidade quadrática*, um resultado muito mais forte que o critério de Euler e que torna mais fácil calcular se um determinado número n é um resíduo quadrático módulo p. Este resultado havia sido formulado como princípio, sem prova, por Euler em 1772 e em 1785 Legendre provou parte do resultado. Em 1796, ao 18 anos, Gauss deu uma prova do resultado e publicou em 1801, no seu livro *Disquisitiones Arithmeticae*, a primeira demonstração completa. Atualmente encontramos na literatura mais de 150 provas para este resultado e o próprio Gauss deu pelo menos 8 demonstrações diferentes para o mesmo. Vejamos alguns resultados necessários para a demonstração apresentada neste trabalho.

A seguir veremos o resultado, conhecido como Lema de Gauss, que nos dará um método para calcular $\left(\frac{a}{p}\right)$ com p primo ímpar e a natural tal que $(a, p) = 1$.

Proposição 2.1.13 *[Lema de Gauss] Sejam p e a dois números, com p primo ímpar e $(p, a) = 1$. Sejam $r_1, \ldots, r_{\frac{p-1}{2}}$ os restos da divisão por p dos números $a, 2a, \ldots, \frac{p-1}{2}a$, respectivamente. Se γ é o número dos r_i que são maiores do que $\frac{p-1}{2}$, então*

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

Demonstração: Inicialmente, lembre-se que se $xa \equiv ya \bmod p$, com $1 \leq x, y \leq \frac{p-1}{2}$ e $x \neq y$, então $x \equiv y \bmod p$. Assim, como $(a,p) = 1$ então $r_1, \ldots, r_{\frac{p-1}{2}} \in \{1, 2, \ldots, p-1\}$ e são distintos, já que $a, 2a, \ldots, \frac{p-1}{2}a$ são dois a dois incongruentes módulo p.

Sejam $\{b_1, \ldots, b_\gamma\}$, os elementos maiores do que $\frac{p-1}{2}$ e $\{c_1, \ldots, c_\beta\}$, dos elementos menores do que ou iguais a $\frac{p-1}{2}$ de modo que $\gamma + \beta$ contemple todos os elementos do conjunto $\{r_1, r_2, \ldots, r_{\frac{p-1}{2}}\}$, ou seja,

$$\gamma + \beta = \frac{p-1}{2} \tag{2.20}$$

Como $\{b_1, \ldots, b_\gamma\}$ são menores do que $\frac{p-1}{2}$ então os números $p - b_i$, com $i \in \{1, 2, \ldots, \gamma\}$ também o são e, além disso, são distintos entre si. Por outro lado, esses números são ainda distintos dos números $c_1, \ldots, c_\beta$, pois, se $p - b_i = c_j$, teríamos $p - b_i \equiv c_j \bmod p$ e assim $b_i \equiv c_j \bmod p$, o que seria um absurdo. Portanto,

$$\{p - b_1, \ldots, p - b_\gamma\} \cup \{c_1, \ldots, c_\beta\} = \{1, 2, \ldots, \frac{p-1}{2}\}.$$

Consequentemente,

$$c_1 \ldots c_\beta (p - b_1) \ldots (p - b_\gamma) = \left(\frac{p-1}{2}\right)! \tag{2.21}$$

Pela definição dos $r_1, \ldots, r_{\frac{p-1}{2}}$ e por sua divisão nos conjuntos $\{b_1, \ldots, b_\gamma\}$ e $\{c_1, \ldots, c_\beta\}$ conforme discutimos acima, temos que

$$\begin{aligned} b_1 \ldots b_\gamma c_1 \ldots c_\beta &\equiv a \cdot 2a \cdot \ldots \cdot \frac{p-1}{2}a \bmod p \\ b_1 \ldots b_\gamma c_1 \ldots c_\beta &\equiv a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \bmod p \end{aligned}$$

e, portanto, substituindo (2.21) temos

$$\begin{aligned} b_1 \ldots b_\gamma c_1 \ldots c_\beta &\equiv a^{\frac{p-1}{2}} (p - b_1) \ldots (p - b_\gamma) c_1 \ldots c_\beta \bmod p \\ b_1 \ldots b_\gamma &\equiv a^{\frac{p-1}{2}} (p - b_1) \ldots (p - b_\gamma) \bmod p \end{aligned} \tag{2.22}$$

Como $(p, p - b_i) = 1$,para todo i, a proposição (2.1.7) nos garante a existência de uma solução x_i da congruência $X(p - b_i) \equiv 1 \bmod p$, ou seja, $\forall i$, existe x_i tal que $x_i(p - b_i) \equiv 1 \bmod p$. Logo,

$$x_1(p - b_1) \ldots x_\gamma(p - b_\gamma) \equiv 1 \bmod p$$

e, assim, por (2.22)

$$\begin{aligned} x_1(p - b_1) \cdot \ldots \cdot x_\gamma(p - b_\gamma) b_1 \ldots b_\gamma &\equiv a^{\frac{p-1}{2}} (p - b_1) \ldots (p - b_\gamma) \bmod p \\ x_1 \ldots x_\gamma b_1 \ldots b_\gamma &\equiv a^{\frac{p-1}{2}} \bmod p \end{aligned} \tag{2.23}$$

Observe ainda que $p - b_i \equiv -b_i \bmod p$ e como $x_i(p - b_i) \equiv 1 \bmod p$, então

$$x_i b_i \equiv -1 \bmod p$$

Assim, $x_1 \dots x_\gamma b_1 \dots b_\gamma \equiv 1 \bmod p$, se γ é par, e $x_1 \dots x_\gamma b_1 \dots b_\gamma \equiv -1 \bmod p$, se γ é ímpar. Portanto, por (2.23), obtemos

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

Finalmente, pelo item (ii) da proposição (2.1.12)

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

■

Nosso próximo resultado irá nos fornecer uma fórmula para o cálculo do símbolo de Legendre.

Proposição 2.1.14 *Sejam p e a dois números naturais ímpares, com p primo e $(a,p) = 1$. Pondo $p' = \frac{p-1}{2}$ e $\kappa = \left[\frac{a}{p}\right] + \left[\frac{2a}{p}\right] + \ldots + \left[\frac{p'a}{p}\right]$, temos*

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

Demonstração: Sejam $r_1, \dots, r_{\frac{p-1}{2}}$ o conjunto dos restos da divisão por p dos números $a, 2a, \dots, \frac{p-1}{2}a$. O dividamos em dois conjuntos $\{b_1, \dots, b_\gamma\}$, dos elementos maiores do que $\frac{p-1}{2}$; e $\{c_1, \dots, c_\beta\}$, dos elementos menores do que ou iguais a $\frac{p-1}{2}$ como foi feito na demonstração da proposição anterior. Então, fazendo $B = b_1 + \ldots + b_\gamma$ e $C = c_1 + \ldots + c_\beta$ temos que

$$r_1 + r_2 \ldots + r_{\frac{p-1}{2}} = B + C \tag{2.24}$$

Note que

$$\begin{aligned} a &= p\left[\frac{a}{p}\right] + r_1 \\ 2a &= p\left[\frac{2a}{p}\right] + r_2 \vdots \\ p'a &= p\left[\frac{(\frac{p-1}{2})a}{p}\right] + r_{\frac{p-1}{2}} \end{aligned}$$

Somando, membro a membro, as igualdades acima temos que

$$a + 2a + \ldots + \frac{p-1}{2}a = p\left(\left[\frac{a}{p}\right] + \left[\frac{2a}{p}\right] + \ldots + \left[\frac{(\frac{p-1}{2})a}{p}\right]\right) + r_1 + r_2 + \ldots + r_{\frac{p-1}{2}}$$

Somando os termos da PA $1, 2, \ldots, \frac{p-1}{2}$ e substituindo (2.24) temos que

$$\frac{p^2-1}{8}a = p\kappa + B + C \tag{2.25}$$

Por outro lado,

$$\{c_1, \ldots, c_\beta, p-b_1, \ldots, p-b_\gamma\} = \{1, \ldots, \frac{p-1}{2}\},$$

então $p - b_1 + p - b_2 + \ldots + p - b_\gamma = p\gamma - (b_1 + b_2 + \ldots + b_\gamma) = p\gamma - B$. Assim,

$$1 + 2 + \ldots + \frac{p-1}{2} = \frac{p^2-1}{8} = p\gamma - B + C. \tag{2.26}$$

Subtraindo (2.26) de (2.25), temos que

$$\frac{p^2-1}{8}(a-1) = p(\kappa - \gamma) + 2B.$$

Como $(a-1)$ é par e p é ímpar, decorre das desigualdades acima que κ e γ têm a mesma paridade. Logo, pelo Lema de Gauss (2.1.13)

$$\left(\frac{a}{p}\right) = (-1)^\gamma = (-1)^\kappa$$

■

As ferramentas apresentadas até aqui para calcular o símbolo de Legendre podem se tornar muito trabalhosas quando os números forem muito grandes. A Lei da Reciprocidade Quadrática, nos ajudará nesse sentido, pois ele permite fazer esse cálculo de uma forma muito mais eficiente. Para demonstrar a lei da reciprocidade quadrática, necessitamos do resultado a seguir. Apresentaremos a demonstração, usando argumentos geométricos, que foi dada, originalmente, pelo matemático alemão ferdinand Gotthold Max Eisenstein, contemporâneo de Gauss.

Lema 2.1.5 *Sejam p e q dois números primos ímpares distintos. Tem-se que*

$$\left[\frac{q}{p}\right] + \left[\frac{2q}{p}\right] + \ldots + \left[\frac{\frac{p-1}{2}q}{p}\right] + \left[\frac{p}{q}\right] + \left[\frac{2p}{q}\right] + \ldots + \left[\frac{\frac{q-1}{2}p}{q}\right] = \frac{p-1}{2}\frac{q-1}{2}$$

Demonstração: Vamos utilizar o seguinte artifício geométrico: Contar os pontos de coordenadas naturais no interior do retângulo de dois modos diferentes. Ora, o segundo membro da igualdade acima é igual ao número de ponto no interior do retângulo S (figura(2.1)). Note que

$$S = \left\{(x,y) \in \mathbb{R}^2;\ 0 \leq x \leq \frac{p-1}{2} \ \ e \ \ 0 \leq y \leq \frac{q-1}{2}\right\}$$

É fácil ver que a quantidade de pontos de coordenadas naturais no interior de S é $\frac{p-1}{2} \cdot \frac{q-1}{2}$

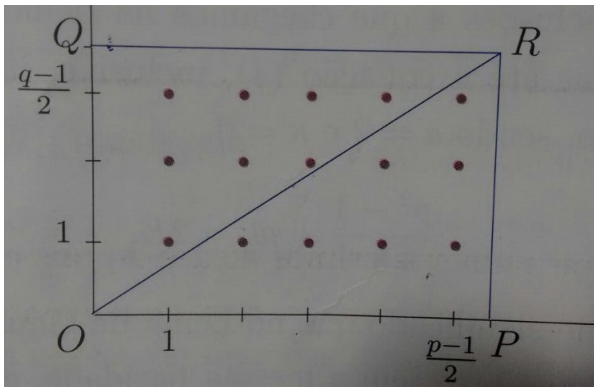

Figura 2.1: Retângulo S

Considere a reta que passa pelos pontos O e R dada pela equação $y = \frac{qx}{p}$. Suponha, sem perda de generalidade $p > q$. Observe que para cada $j > 0$ o número de inteiros positivos menores ou iguais a $\frac{jq}{p}$ é $\left[\frac{jq}{p}\right]$ e como $\frac{jq}{p} \notin \mathbb{Z}$, o número de coordenadas naturais acima do eixo OP e abaixo da reta OR é dado por $\left[\frac{jq}{p}\right]$. Portanto, o número de pontos de coordenadas naturais no interior do triângulo OPR é

$$\kappa = \left[\frac{q}{p}\right] + \left[\frac{2q}{p}\right] + \ldots + \left[\frac{\frac{p-1}{2}q}{p}\right]$$

Analogamente, o número de pontos de coordenadas naturais no interior do triângulo OQR é

$$\kappa' = \left[\frac{p}{q}\right] + \left[\frac{2p}{q}\right] + \ldots + \left[\frac{\frac{q-1}{2}p}{q}\right]$$

Portanto, $\kappa + \kappa'$ é igual ao número total de pontos de coordenadas naturais no interior do retângulo S.

■

Teorema 2.1.16 *[Lei da reciprocidade quadrática] sejam p e q dois números primos ímpares distintos. Tem-se que*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Demonstração: Ora, pela proposição (2.1.14) $\left(\frac{q}{p}\right) = (-1)^{\kappa}$ e $\left(\frac{p}{q}\right) = (-1)^{\kappa'}$ onde

$$\kappa = \left[\frac{q}{p}\right] + \left[\frac{2q}{p}\right] + \ldots + \left[\frac{\frac{p-1}{2}q}{p}\right]$$

$$\kappa' = \left[\frac{p}{q}\right] + \left[\frac{2p}{q}\right] + \ldots + \left[\frac{\frac{q-1}{2}p}{q}\right]$$

e como, pelo lema (2.1.5) $\kappa + \kappa' = \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$ segue que

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

■

Para encerrar essa seção vejamos agora, como aplicação da lei da reciprocidade quadrática, o caso $3n+1$ e, em seguida, mais dois casos particulares do teorema de Dirichlet.

Teorema 2.1.17 *Existem infinitos primos da forma* $3n+1$.

Demonstração: Suponhamos, por absurdo, que haja somente uma quantidade finita de primos da forma $3n+1$, digamos $p_1, p_2, \ldots p_k$, e seja $x = (2p_1 \ldots p_k)^2 + 3$. Se p é um divisor primo de x, então $p \neq 2, 3, p_1, \ldots, p_k$, de modo que $p \equiv -1 \bmod 3$. Além disso, como

$$(2p_1 \ldots p_k)^2 \equiv -3 \bmod p$$

temos que -3 é resíduo quadrático módulo p. Devemos, então, ter $\left(\frac{-3}{p}\right) = 1$.

Por outro lado, como $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, temos

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{3}{p}\right). \tag{2.27}$$

Pela lei da reciprocidade quadrática,

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{(\frac{p-1}{2})(\frac{3-1}{2})} = (-1)^{\frac{p-1}{2}}.$$

Assim,

$$\left(\frac{3}{p}\right) = \frac{(-1)^{\frac{p-1}{2}}}{\left(\frac{p}{3}\right)} = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)^{-1} = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right) \tag{2.28}$$

Substituindo (2.28) em (2.27) temos que

$$\left(\frac{-3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}} = \left(\frac{p}{3}\right)$$

Pelo item (i) da proposição (2.1.12) se $p \equiv -1 \bmod 3$ então

$$\left(\frac{p}{3}\right) = \left(\frac{-1}{3}\right) = -1$$

o que é uma contradição, pois -3 é resíduo quadrático módulo p.

■

Teorema 2.1.18 *Existem infinitos primos da forma* $6n+1$.

Demonstração: Na demonstração da infinidade de primos da forma $3n+1$ vimos que

$$\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) \tag{2.29}$$

(i) Se p for da forma $6n+1$ então é da forma $3n+1$. Assim, $p \equiv 1 \bmod 3$. Logo,

$$\left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1$$

Substituindo em (2.29) temos

$$\left(\frac{-3}{p}\right) = 1$$

(ii) Se p for da forma $6n+5$ então é da forma $3n+2$. Assim, $p \equiv -1 \bmod 3$. Logo,

$$\left(\frac{p}{3}\right) = \left(\frac{-1}{3}\right) = -1$$

Substituindo em (2.29) temos

$$\left(\frac{-3}{p}\right) = -1$$

Vamos mostrar que todo divisor primo de um número maior do que 4 e da forma x^2+3 é igual a 2 ou a 3, ou é da forma $6n+1$. De fato, considere $\alpha = x^2+3$, $\alpha > 4$. Evidentemente todo divisor primo de α é igual a 2 ou a 3 ou é da forma $6n+1$ ou é da forma $6n+5$.

Se $p \mid \alpha$ isso significa dizer que a congruência $x^2 \equiv -3 \bmod p$ tem solução. Portanto, $\left(\frac{-3}{p}\right) = 1$ e pelo que vimos acima, no item (i), p só pode ser da forma $6n+1$ pois para p da forma $6n+5$, $\left(\frac{-3}{p}\right) = -1$ (item (ii))

Finalmente, suponhamos, por absurdo, que haja apenas uma quantidade finita de primos da forma $6n+1$. Sejam eles $p_1, p_2, \ldots, p_r$. Considere agora $\beta = (2 \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_r)^2 + 3$. Seja p um divisor primo de β, então $p \neq 2, 3, p_1, \ldots, p_r$. Portanto, p tem que ser da forma $6n+5$. Assim,

$$\left(\frac{-3}{p}\right) = -1$$

Por outro lado p ser um divisor primo de β significa que a congruência $x^2 \equiv -3 \bmod p$ tem solução. Assim,

$$\left(\frac{-3}{p}\right) = 1$$

o que é uma contradição.

■

Teorema 2.1.19 *Existem infinitos primos da forma* $8n+3$.

Demonstração: Pela proposição (2.1.12)(*iii*) temos que

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{2}{p}\right)$$

Primeiramente vamos calcular $\left(\frac{-1}{p}\right)$. Note que se p é da forma $8n+1$ ou $8n+5$ então é da forma $4n+1$. Assim, pelo corolário (2.1.2) temos

$$\left(\frac{-1}{p}\right) = 1 \tag{2.30}$$

Se p é da forma $8n+3$ ou $8n+7$ então é da forma $4n+3$. Assim, pelo corolário (2.1.2) temos

$$\left(\frac{-1}{p}\right) = -1 \tag{2.31}$$

Vamos agora calcular $\left(\frac{2}{p}\right)$. Note que independentemente da paridade de a todas as conclusões na demonstração da proposição (2.1.14) são verdadeiras até a equação

$$\frac{p^2-1}{8}(a-1) = p(\kappa - \gamma) + 2B. \tag{2.32}$$

Além disso,

$$\left[\frac{2}{p}\right] = \left[\frac{2\cdot 2}{p}\right] = \ldots = \left[\frac{\frac{p-1}{2}\cdot 2}{p}\right] = 0$$

Portanto, seguindo as notações da proposição (2.1.14) temos

$$\kappa = \left[\frac{2}{p}\right] + \left[\frac{2\cdot 2}{p}\right] + \ldots + \left[\frac{\frac{p-1}{2}\cdot 2}{p}\right] = 0$$

Assim, fazendo $a = 2$ e $\kappa = 0$ e substituindo em (2.32) temos

$$\frac{p^2-1}{8} + p\gamma = 2B \tag{2.33}$$

Como p é ímpar a equação (2.33) nos diz que $\frac{p^2-1}{8}$ e γ tem a mesma paridade. O resultado segue do lema de Gauss, pois o fato de p ser ímpar equivale a dizer que ele assume uma das formas $8n+1, 8n+3, 8n+5, 8n+7$ e assim,

Se p é da forma $8n+1$ então $\frac{p^2-1}{8}$ é par;

Se p é da forma $8n+3$ então $\frac{p^2-1}{8}$ é ímpar;

Se p é da forma $8n+5$ então $\frac{p^2-1}{8}$ é ímpar;

Se p é da forma $8n+7$ então $\frac{p^2-1}{8}$ é par;

Portanto, essas informações juntas com (2.30) e (2.31) nos assegura que

$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{2}{p}\right) = 1$ se p assumir umas das formas $8n+1$ ou $8n+3$
$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{2}{p}\right) = -1$ se p assumir umas das formas $8n+5$ ou $8n+7$

Agora, suponhamos que haja apenas uma quantidade finita de primos da forma $8n+3$ e sejam $p_1, p_2, \ldots, p_s$ todos esses primos. Considere o número

$$\beta = (p_1 \cdot p_2 \cdot \ldots \cdot p_s)^2 + 2$$

Assim, β é da forma $8n+3$, já que o quadrado de todo número de uma das formas $8n+1, 8n+3, 8n+5, 8n+7$ é da forma $8n+1$

Por outro lado, se p é um divisor primo de β então $p \neq p_1, p_2, \ldots, p_s$ e além disso,

$$(p_1 \cdot p_2 \cdot \ldots \cdot p_s)^2 \equiv -2 \bmod p$$

Logo, $\left(\frac{-2}{p}\right) = 1$. Então, pelo que foi discutido acima p é da forma $8n+1$ ou é da forma $8n+3$, mas p não pode ser da forma $8n+3$ já que $p \neq p_1, p_2, \ldots, p_s$. Portanto é da forma $8n+1$, e como o conjunto $A = 8n+1; n \in \mathbb{N}$ é fechado multiplicativamente temos que β é da forma $8n+1$, o que é uma contradição, pois β é da forma $8n+3$.

■

2.2 Primos em progressões aritméticas mais gerais

Vejamos um exemplo onde o primeiro termo é 1 e a razão da progressão aritmética é uma potência de primos.

2.2.1 Primeiro termo 1 e razão q^s

Teorema 2.2.1 *Na progressão aritmética de primeiro termo 1 e razão q^s, para $s \in \mathbb{N}$ e q primo, existem infinitos números primos.*

Demonstração: Suponhamos que haja apenas uma quantidade finita de primos $p_1 < p_2 < \ldots < p_r$ na progressão aritmética $1, 1+q^s, 1+2q^s, 1+3q^s, \ldots$ Então eles são os únicos primos tais que $q^s \mid p_i - 1$ para $i = 1, 2, \ldots, r$. Sejam $N = qp_1p_2 \ldots p_r$ e $M = N^{q^{s-1}}$. Vamos mostrar que existe um primo p tal que $q^s \mid p-1$ onde $p \neq p_1, p_2, \ldots, p_r$. Pela fórmula do binômio de Newton temos que

$$M^q - 1 = [(M-1)+1]^q - 1 = (M-1)^q + \binom{q}{1}(M-1)^{q-1} + \binom{q}{2}(M-1)^{q-2} + \ldots + \binom{q}{q-1}(M-1).$$

Logo, $M-1 \mid M^q - 1$ e como $M-1 < M^q - 1$, existe um primo p tal que

$$p \mid \frac{M^q - 1}{M-1} = \frac{N^{q^s} - 1}{N^{q^{s-1}} - 1}$$

Note que se p divide $M-1$, então, p divide $\binom{q}{q-1} = q$, logo, $p = q$; mas q divide M, assim p divide 1, que é um absurdo. Portanto,

$$p \nmid M - 1 = N^{q^{s-1}} - 1 \tag{2.34}$$

Mas, por outro lado

$$p \mid M^q - 1 = N^{q^s} - 1 \tag{2.35}$$

Como $(p, N) = 1$, pelo pequeno teorema de Fermat temos que

$$p \mid N^{p-1} - 1 \tag{2.36}$$

Seja $t \geq 1$ o menor inteiro positivo tal que $p \mid N^t - 1$.Pelas equações (2.35) e (2.36) sabemos que t divide q^s e que t divide $p-1$, respectivamente. Mas pela equação (2.34) t não divide q^{s-1}, assim, $t = q^s$. Portanto, $q^s \mid p-1$. Contradição. Logo existem infinitos primos na progressão aritmética $S = \{q^s n + 1\}_{n \in \mathbb{N}}$.

■

2.2.2 Polinômios ciclotômicos

Para o nosso próximo exemplo apresentaremos algumas propriedades de uma classe especial de polinômios, os chamados polinômios ciclotômicos. Para um estudo mais completo dos polinômios ciclotômicos indicamos [1].

Para tanto, lembremos que um número complexo z é uma raiz $n-$ésima da unidade se existir $n \in \mathbb{N}$ tal que $z^n = 1$. Essas raízes são dadas por

$$z_k = cos\left(\frac{2k\pi}{n}\right) + isen\left(\frac{2k\pi}{n}\right); \quad 0 \leq k < n, \quad k \in \mathbb{Z}.$$

Assim, temos que existem n raízes n-ésimas da unidade. Dado $n \in \mathbb{N}$, fazendo $\omega_n = cos\left(\frac{2\pi}{n}\right) + isen\left(\frac{2\pi}{n}\right)$ essas raízes são os números complexos

$$1, \omega_n, \omega_n^2, \ldots, \omega_n^{n-1}.$$

Chamaremos de raízes primitivas as raízes n-ésimas da unidade da forma ω_n^k, onde $1 \leq k \leq n$ e $\text{mdc}(k, n) = 1$. Para o que segue denotaremos o grau do polinômio Φ_n por $\partial\Phi_n$.

Definição 2.2.1 *Para $n \in \mathbb{N}$, o n-ésimo polinômio ciclotômico é o polinômio*

$$\Phi_n(X) \quad = \prod_{\substack{1 \leq k \leq n \\ (k,n)=1}} (X - \omega_n^k)$$

Proposição 2.2.1 *Para $n \in \mathbb{N}$, temos:*

i) $X^n - 1 = \prod_{\substack{0<d \\ d \mid n}} \Phi_d(X)$;

ii) Φ_n *é mônico de coeficientes inteiros;*

iii) $\partial\Phi_n = \varphi(n)$;

iv) $\Phi_n(0) = 1$, *para* $n > 1$.

Demonstração:
i) Observe que

$$\prod_{\substack{0<d \\ d \mid n}} \Phi_d(X) = \prod_{\substack{0<d \\ d \mid n}} \Phi_{n/d}(X) = \prod_{\substack{0<d \\ d \mid n}} \prod_{\substack{1 \le k \le \frac{n}{d} \\ (k, \frac{n}{d})=1}} (X - \omega_{n/d}^k) = \prod_{\substack{0<d \\ d \mid n}} \prod_{\substack{1 \le k \le \frac{n}{d} \\ (k, \frac{n}{d})=1}} (X - \omega_n^{dk})$$

Como cada inteiro $1 \le m \le n$ pode ser escrito de modo único como $m = dk$, com $0 < d \mid n$ e $\left(k, \frac{n}{d}\right) = 1$ onde $d = (m, n)$, a última soma acima é claramente igual a

$$\prod_{j=1}^{n} (X - \omega_n^j) = X^n - 1$$

ii) Vamos provar, por indução, que Φ_n é mônico de coeficientes inteiros. Para $n = 1$ temos
$\Phi_1 = X - 1$ que é obviamente mônico de coeficientes inteiros. Suponhamos, por hipótese de indução, que Φ_k seja mônico de coeficientes inteiros para todo inteiro $1 \le k < n$. Então

$$\Phi(X) = \prod_{\substack{1 \le d < n \\ d \mid n}} \Phi_d(X) \tag{2.37}$$

é mônico de coeficientes inteiros. Como pelo item *i)*

$$X^n - 1 = \Phi_n(X)\Phi(X) \tag{2.38}$$

e $\Phi(X)$ é mônico de coeficientes inteiros por hipótese de indução, pelo algoritmo da divisão de polinômios concluímos que Φ_n é mônico de coeficientes inteiros.
iii) Ora, por definição o grau de Φ_n é igual ao número de inteiros k tais que $1 \le k \le n$ tais que $(k, n) = 1$. Por outro lado, $\varphi(n)$ é o número de elementos de um sistema reduzido de resíduos módulo n, ou seja é a quantidade de números naturais entre 0 e $n - 1$ que são primos com n. Portanto $\partial\Phi_n = \varphi(n)$.
iv) Vamos provar por indução. Para $n = 2$ temos

$$X^2 - 1 = \prod_{0<d|2} \Phi_d(X) = \Phi_1(X)\Phi_2(X) = (X - 1)\Phi_2(X)$$

Então $\Phi_2(X) = X + 1$ e $\Phi_2(0) = 1$.
Suponhamos, por hipótese de indução, que $\Phi_m(0) = 1$ para todo inteiro $2 < m < n$. Por (2.37) temos que

$$\Phi(0) = \Phi_1(0) \prod_{\substack{1<d<n \\ d \mid n}} \Phi_d(0) = (-1) \prod_{\substack{1<d<n \\ d \mid n}} \Phi_d(0) = -1,$$

Por (2.38) temos que

$$0^n - 1 = \Phi_n(0)\Phi(0) =$$

então

$$\Phi_n(0) = 1$$

■

2.2.3 Primeiro termo 1 e razão d

Teorema 2.2.2 *Se $n \in \mathbb{N}$, então a progressão aritmética $1, 1+n, 1+2n, 1+3n, \ldots$ contém infinitos números primos.*

Demonstração: Sejam $p_1, p_2, \ldots, p_k$ números primos quaisquer e $\Phi_n(a)$ o n-ésimo polinômio ciclotômico. Como $\Phi_n(a)$ é mônico, podemos escolher um $y \in \mathbb{Z}$ suficientemente grande tal que $\Phi_n(ynp_1p_2 \ldots p_k) > 1$. Agora, fazendo $a = ynp_1p_2 \ldots p_k$ temos que

$$\Phi_n(a) \equiv \Phi_n(0) \bmod a$$

Como $\Phi_n(0) = 1$ temos

$$\Phi_n(a) \equiv 1 \bmod a$$

Então existe $q \in \mathbb{Z}$ tal que $\Phi_n(a) = aq + 1 = ynp_1p_2 \ldots p_kq + 1$. Se p é um fator primo de $\Phi_n(a)$ então $p \neq p_1, p_2, \ldots, p_k$ e $(p, n) = (p, y) = (p, a) = 1$. Vamos mostrar que $n \mid p - 1$ o que equivale a $p = ns + 1$ para algum $s \in \mathbb{N}$, ou seja, p é um primo na progressão aritmética $1, 1+n, 1+2n, 1+3n, \ldots$ diferente de todos os primos $p_1, p_2, \ldots, p_k$ o que mostra que a PA contém infinitos primos. Como $(a, p) = 1$ podemos denotar $t := ord_p(a)$. Como p é um fator primo de $\Phi_n(a)$ e $\Phi_n(a) \mid (a^n - 1)$, temos que $a^n \equiv 1 \bmod p$ e, portanto, $t \mid n$. Se $c \in \{a, a + p\}$, como $a^t \equiv 1 \bmod p$ então $c^t \equiv 1 \bmod p$. Observe também que como $t \mid n$ então $t \leq n$. Vamos mostrar que $t = n$. Suponha por contradição que $t < n$. Pela proposição (2.2.1) e pelo fato de que $t \mid n$ temos

$$c^n - 1 = \prod_{0<d|n} \Phi_d(c) = \Phi_n(c) \prod_{\substack{0<d<n \\ d \mid n}} \Phi_d(c) = \Phi_n(c) \prod_{0<d|t} \Phi_d(c)H(c) =$$

$$= \Phi_n(c)(c^t - 1)H(c)$$

Para algum polinômio $H(c)$ apropriado. Por outro lado, $c \equiv a \bmod p$, portanto

$$\Phi_n(c) \equiv \Phi_n(a) \equiv 0 \bmod p$$

Logo

$$c^n - 1 = \Phi_n(c)(c^t - 1)H(c) \equiv 0 \bmod p^2$$

Mas pelo Binômio de Newton sabemos que

$$(a+p)^n - 1 = a^n - 1 + \sum_{j=1}^{n-1} \binom{n}{j} a^{n-j}p^j$$

Como $c \in \{a, a+p\}$ temos que $p^2 \mid ((a+p)^n - 1)$ e que $p^2 \mid a^n - 1$. Então, temos que $p^2 \mid \binom{n}{1}a^{n-1}p$. Logo, $p \mid na^{n-1}$ o que é um absurdo já que $(p,n) = (p,a) = 1$. Portanto, $t = n$. Pelo teorema de Euler (ou Fermat) sabemos que $a^{p-1} \equiv 1 \bmod p$ e como $ord_p(a) \mid \varphi(p)$ segue que $n \mid (p-1)$

■

2.3 Distribuição de primos em progressões aritméticas

Nessa seção iremos mostrar outros fatos sobre os números primos em progressões aritméticas. Apresentaremos alguns problemas em aberto, algumas estimativas, alguns recordes e outras curiosidades sobre os primos em progressões aritméticas, por fim apresentaremos umas notas sobre Dirichlet

2.3.1 PA's formadas por primos

Começamos com a questão da existência de k números primos $p_1 < p_2 < \ldots < p_k$ tais que aconteçam a igualdade entre as diferenças $p_{n+1} - p_n$, ou seja, $p_2 - p_1 = p_3 - p_2 = \ldots = p_k - p_{k-1}$. Vejamos um pouco dessa história em ordem cronológica até se chegar ao teorema principal sobre a questão.

Em 1939, Van Der Corput mostrou que existem uma infinidade de sucessões de três números primos em progressão aritmética. Por exemplo $3, 7, 11$. Em 1981, Heath-Brown demonstraram a existência de uma infinidade de progressões aritméticas constituídas por 4 números, dos quais 3 são primos e o quarto, ou é primo, ou é produto de dois primos (não necessariamente distintos). Recentemente, ou melhor, apenas em 2004, B. Green e T. Tao demonstraram, mas só foi publicado em 2008, o seguinte teorema:

Para todo $k \geq 3$ existe pelo menos uma progressão aritmética de k inteiros positivos que são números primos.

Este trabalho ajudou a T. Tao ganhar uma medalha Fields no Congresso Internacional de Matemática de 2006. A demonstração de Green e Tao não permite encontrar um exemplo concreto de uma progressão aritmética formada por k números primos e por isso muitos trabalhos têm sido desenvolvidos na área de computação em busca de resultados mais construtivos. Porém, essa pesquisa requer cálculos muito longos. Para alguns valores pequenos de k podemos encontrar progressões sem precisar recorrer a muitos cálculos como por exemplo, com cinco primos $5, 11, 17, 23, 29$

, com seis primos $7, 37, 67, 97, 127, 157$, com sete primos $157, 307, 457, 607, 751, 907$, com 10 primos $199, 409, 619, 829, 1039, 1249, 1459, 1669, 1879, 2089$. Já para valores um pouco maiores que esses, foram necessários numerosos cálculos, muitos com auxílio de computadores.

O maior valor encontrado para k é 26. Atualmente existem várias progressões para $k = 26$, mas os primeiros a descobrirem um exemplo foram P. Perichon, J. Wróblewski, G. Reynolds e o Projeto PrimeGrid em abril de 2010 onde o menor dos primos é $p = 43142746595714191$ e a razão da PA é $d = 5283234035979900$. Já a mais recente foi descoberta por Bryan Little em fevereiro de 2015. A PA é a seguinte:

$$161004359399459161 + 47715109 \cdot \left(\prod_{p=2}^{23} p \right) \cdot n$$

com p primo e $0 \leq n \leq 25$ onde $\prod_{p=2}^{23} p = 223092870$.

Alguns outros recordes foram:
1977:17 termos, por S. Weintraub,
1982:18 termos, por P. Pritchard,
1985:19 termos, por P. Pritchard,
1987:20 termos, por J. Young e J. Fry,
1993:22 termos, pelo Projeto Pritchard,
2004:23 termos, por M. Frind, P.Jobling e P. Underwood,
2006:24 termos, por J. Wróblewski,
2008:25 termos, por R. Chermoni e J. Wróblewski.

O Projeto Pritchard foi um esforço coletivo que contou com mais de 60 participantes, administrado por P. Pritchard da Griffith University na Austrália, com o objetivo de descobrir sucessões longas de números primos em progressão aritmética.

O teorema que rendeu a medalha Fields a T. Tao sugere procurarmos progressões aritméticas que sejam formadas apenas por números primos, já que ele afirma que para qualquer $k \geq 3$ existe pelo menos uma progressão aritmética de k inteiros positivos, todos primos. O teorema a seguir nos mostra que não existe tal possibilidade.

Teorema 2.3.1 *Não existe progressão aritmética infinita formada apenas por números primos.*

Demonstração: Sejam $p_i's$ os números primos, com $i = 1, 2, 3, \ldots$ e $a, b \in \mathbb{N}$. Suponhamos, por absurdo, que exista uma progressão aritmética $a, a+b, a+2b, a+3b, \ldots$ formada apenas por números primos. Então existe $n_1 \in \mathbb{N}$ tal que $a + n_1 b = p_i$ para algum $i = 1, 2, 3, \ldots$ fixo. Pondo $n_k = n_1 + kp_i,\ k = 1, 2, 3, \ldots$ temos:

$$a + n_k b = a + (n_1 + kp_i)b = a + n_1 b + bkp_i = p_i + bkp_i = p_i(1 + bk).$$

Logo, $a + n_k b$ é divisível por p_i, absurdo. Portanto, não pode existir tal progressão aritmética.

■

Vimos acima que não pode existir uma progressão aritmética formada por infinitos termos onde esses termos são todos primos. Por outro lado o Teorema de Terence Tao garante que sempre existe uma progressão aritmética, finita de $k > 2$ termos, cujos termos são todos números primos.Assim, uma outra pergunta que podemos fazer é: Será que fixado um primo p qualquer, existe um natural k tal que $p, p+k, p+2k, \ldots, p+(p-1)k$ são números primos?

Para primos pequenos a resposta a essa pergunta tem sido sim. Acredita-se que para outro primo qualquer ela também seja positiva. Porém, esse ainda seja um problema em aberto. Vejamos alguns exemplos encontrados para primos pequenos.
p=3 e k=2: 3 5 7
p=5 e k=6: 5 11 17 23 29
p=7 e k=150: 7 157 307 457 607 751 907
p=11 e k=1536160080821194590
p=13 e k=918821194590
p=17 e k=341976204789992332560
Até o momento não há exemplos numéricos conhecidos para p maior que 17.

Uma outra pergunta que o teorema de Terence Tao nos levar a fazer é a seguinte: Será que existem progressões aritméticas cujos termos são todos números primos consecutivos? Uma conjectura ligada a essa questão é a seguinte:

Existem progressões aritméticas, de número de termos arbitrariamente grande, composta apenas por números primos consecutivos.

Note que $3, 5, 7$ são três primos consecutivos em PA; $251, 257, 263, 269$ são quatro primos consecutivos em PA; Apesar de não existir uma resposta concreta a essa pergunta, para primos pequenos ela também é positiva. A sequência mais longa de primos consecutivos em progressão aritmética conhecida contém dez termos. O menor deles é o primo:

$$p = 1009969724697142476377866555879698403295093246-$$

$$8919004180360341775890434170334888215906722971 9.$$

A razão da progressão aritmética é 210. Essa sucessão de números primos consecutivos foi descoberta em março de 1998 por M. Toplic. Anteriormente, em janeiro de 1998, M. Toplic tinha encontrado uma progressão aritmética constituída de 9 números primos consecutivos. O primeiro deles é:

$p = 9967943206670108648449065369585356163898236408099161839577404858552907147546111479960$

A razão também é 210.

2.3.2 O menor primo de uma PA

Dado uma progressão aritmética com primeiro termo e razão primos entre si já sabemos que ela contém infinitos números primos. Uma pergunta que podemos fazer aqui é: Quando é esperado que o primeiro número primo apareça na progressão. Introduziremos a seguir a seguinte notação.

Se $1 \leq a < d$ com $\text{mdc}(a, d) = 1$. Seja $p(d, a)$ o menor primo da progressão aritmética $\{a + kd \mid k \geq 0\}$. Seja $p(d) = max\{p(d, a)\ 1 \leq a < d\ e\ mdc(a, d) = 1\}$.

1	2	3	$\ldots$	d
$d+1$	$d+2$	$d+3$	$\ldots$	$2d$
$2d+1$	$2d+2$	$2d+3$	$\ldots$	$3d$
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
$(d-1)d+1$	$(d-1)d+2$	$(d-1)d+3$	$\ldots$	d^2

Figura 2.2: Matriz quadrada de ordem d

Sabemos que esse número existe, mas será que ele não pode ser maior que uma determinada quantidade que depende apenas de d ? Antes de vermos algumas estimativas a respeito, vamos mostrar um resultado profundo da teoria analítica dos números e que foi provado por Linnik em 1944.

Teorema 2.3.2 *[Linnik] Existe $L > 1$, tal que $p(d) < d^L$, para d suficientemente grande.*

A prova deste teorema envolve conceitos profundos da teoria analítica dos números e não será exposta aqui. Essa constante L é chamada de constante de Linnik. Linnik mostrou que L é efetivamente calculável e o primeiro a calculá-la foi Cheng Dong Pan em 1957. Ele mostrou que $L \leq 5448$. Alguns outros valores melhores para k foram:

1965: $L \leq 777$, por Chen,
1970: $L \leq 550$, por Jutila,
1977: $L \leq 36$, por Graham,
1979: $L \leq 17$, por Chen,
1981: $L \leq 20$, por Graham,
1986: $L \leq 16$, por Wang,
1989: $L \leq 13,5$, por Chen e Liu,
1990: $L \leq 8$, por Heath-Brown

Vejamos duas estimativas que estão relacionadas ao estudo de $p(d)$ as quais analisaremos suas veracidades.

Estimativa 2.3.1 *Existe um inteiro $M \geq 1$ tal que $p(d) < d + M$ para cada $d > 1$.*

Estimativa 2.3.2 *$p(d) < d^2$ para cada d suficientemente grande.*

Vamos ver que a estimativa 2.3.1 é falsa. De fato, dado M, seja d tal que $d \geq M$ e $1 + d$ é composto. Então,

$$1 + d + d > d + M$$

logo, $p(d) > d + M$ e, portanto, a estimativa 2.3.1 é falsa.

Sobre a estimativa 2.3.2 observe a matriz quadrada (figura(2.2)) com d linhas e d colunas acima onde estão escritos os número de 1 a d^2

A estimativa 2.3.3 pode ser reescrita assim: Se $1 \leq a \leq d$ e $(a, d) = 1$ a primeira coluna contém um número primo. O que significa que $p(d, a) < d^2$ para todo a, logo

$p(d) < d^2$. É claro que não se pode provar uma estimativa com esse tipo de argumento, mas muitas pessoas têm analisado matrizes quadradas de d^2 números, com d muito grandes e todas têm verificado a estimativa. Por isso Schinzel e Sierpinski e Kanold conjecturaram que a estimativa 2.3.3 é verdadeira. Isto significa que se d é suficientemente grande, e se $1 \leq a < d$ e $(a, d) = 1$, então existe um número primo entre os números $a, a + d, a + 2d, \ldots, a + (d - 1)d$.

2.3.3 Versão fraca do Teorema de Dirichlet

Devido a complexidade da demonstração do teorema de Dirichlet alguns matemáticos tentaram encontrar outras versões mais simples para a sua demonstração. Mostraremos a seguir uma versão mais fraca equivalente ao teorema.

Teorema 2.3.3 *Sejam a e b números naturais primos entre si. Existe pelo menos um número primo da forma $an + b$ onde n é um número natural.*

Vamos mostrar que para provar a existência de uma infinidade de números primos na progressão aritmética de primeiro termo e razão primos entre si é suficiente mostrarmos a existência de pelo menos um primo na PA, ou seja, o Teorema de Dirichlet e o teorema (2.3.3) são equivalentes.

De fato, o teorema de Dirichlet implica no teorema acima, pois se existem infinitos primos é óbvio que existe pelo menos um. Para a recíproca, suponhamos que o teorema acima seja verdadeiro. Se $a = 1$ nada há à fazer. Portanto, suponhamos $a \geq 2$. Seja m um número natural qualquer. Vamos mostrar que existe um número primo p da forma $an+b$ maior que m. Como $(a, b) = 1$ então, pelo item (ii) do corolário 1.1.5 temos que $(a^m, b) = 1$. Nesse caso, o teorema (2.3.3) garante a existência de um primo p da forma $a^m n + b$ para algum $n \in \mathbb{N}$. Como $a \geq 2$, então:

$$a^m \geq 2^m.$$

Por outro lado, $2^m > m$ para todo $m \in \mathbb{N}$ (Indução sobre m). Logo, para todo m natural qualquer existe um número primo $p = a^m n + b > m$.

Considerações Finais

Neste trabalho apresentamos alguns resultados da Teoria dos Números e dos polinômios ciclotômicos que nos deram o alicerce necessário para o entendimento de alguns casos de alguns casos particulares do Teorema de Dirichlet. Apesar de não apresentarmos a demonstração do teorema por necessitar de ferramentas que fogem ao escopo do texto, ele é o tema central do nosso trabalho. Trazemos outros teoremas, também apresentados sem demonstração, com finalidade de enriquecer o texto e mostrar que o tema em questão tem sido um campo fértil que tem produzido resultados bastante sofisticados e importantes para a Matemática, como foi o caso do teorema que contribuiu com o prêmio da medalha Fields ao Terence Tao.

Vimos que muitos matemáticos têm tentado encontrar progressões aritméticas formadas apenas por números primos, mas os resultados obtidos até esta data não passam de 26 termos para PA's formadas por primos quaisquer e de apenas 10 termos para PA's formadas só por primos consecutivos. Este fato, além de curioso, nos mostra que ainda estamos iniciando uma caminhada pelo fantástico mundo dos primos em PA's e que ainda temos muito por desenvolver.

Além disso, vimos que existe um limite para se encontrar o primeiro primo de uma PA cujo primeiro termo é um número natural menor que a razão e ambos primos entre si. Por outro lado, vimos que para mostrar a infinidade de termos primos numa PA, basta mostrar a existência de pelo menos um primo, ou seja, o Teorema de Linnik implica no clássico Teorema de Dirichlet. Por tudo isso, acreditamos ter alcançado o nosso objetivo que era explorar um pouco sobre os primos em PA's e em especial sobre o Teorema de Dirichlet.

Referências Bibliográficas

[1] Neto, A.C.M. *Tópicos de matemática elementar: Polinômios*. vol 6. 2 ed. Rio de Janeiro: SBM, (2016).

[2] Muniz Neto, A.C. *Tópicos de matemática elementar: Teoria dos números*. vol 3. 2 ed. Rio de Janeiro: SBM, (2013).

[3] Santos, J.P.O. *Introdução à teoria dos números*. Coleção matemática universitária. 3 ed. Rio de Janeiro: IMPA, (2015).

[4] Martines, F.B.,et al. *Teoria dos números: Um passeio com primos e outros números familiares pelo mundo inteiro*. 4 ed. Rio de Janeiro: IMPA, (2015).

[5] Ribenboim, P. *Números primos. Velhos mistérios e novos recordes*. Coleção matemática universitária. 1 ed. Rio de Janeiro: IMPA, (2014).

[6] Ribenboim, P. *Números primos, amigos que causam problemas*. Rio de Janeiro: SBM, (2015).

[7] Moreira, C.G.T. de A. *Tópicos de teoria dos números*. Coleção PROFMAT. 1 ed. Rio de Janeiro: SBM, (2012).

Apêndice

Notas sobre Dirichlet

Figura 2.3: Dirichlet

Johann Peter Gustav Lejeune Dirichlet(1805-1859) foi um matemático alemão. Casado como Rebecca Mendelssohn. Sua família originou-se em Richelet, uma pequena cidade na Bélgica daí o nome Lejeune Dirichlet que significa "le jeune de Richelet", o jovem de Richelet. Nascido em Düren, na Alemanha, local onde sua família foi morar, Gustav Lejeune Dirichlet, viveu numa época em que Düren estava em território do império francês. Sua genialidade sempre foi reconhecida em todas as disciplinas durante o tempo que estudou no ginásio de Bonn e depois no Colégio dos Jesuítas, em Köln, onde Dirichlet teve a oportunidade de aprender Matemática com George Simon Ohm. Ele entrou na Universidade de Paris em 1832, e teve a honra de assistir aulas no Collège de France e na Faculté des Sciences ministradas por grandes matemáticos, como Poisson, Fourier, Lacroix, Legendre e Laplace. Após sua formatura, Dirichlet continuou por alguns anos em Paris até que voltou para a Alemanha onde ocupou uma posição de curta duração em Wroclaw (então chamada de Breslau, na Alemanha), e depois em Berlim onde compartilhava um programa de ensino entre a Universidade de Berlim e a Academia Militar. Em 1855, ele se tornou o sucessor de Gauss em Göttingen onde ficou até sua morte. Sua produção, apesar de não ser tão volumosa, contribuiu bastante para a teoria dos números criando o ramo da teoria analítica dos números, devido as suas ideias originais. Em seu

primeiro artigo, publicado em 1828, Dirichlet mostrou que a equação $x^5 + y^5 = z^5$ não tem solução em números inteiros diferentes de zero x, y e z. Em 1832, Dirichlet provou o último teorema de Fermat para o expoente 14. Dirichlet também publicou um artigo sobre a lei da reciprocidade biquadrática. Estes resultados e outros artigos publicados posteriormente chamaram a atenção dos matemáticos para o jovem matemático que estava se destacando. Segundo Ribenboim:

> Dirichlet usou métodos analíticos muito originais e poderosos para provar o seu famoso teorema sobre os números primos em progressão aritmética... (Ribenboim, 2015, p. 314). [6]

Para isso, estudou uma categoria de séries, agora chamadas de séries de Dirichlet, da qual a série zeta de Riemann é o principal exemplo. Além de suas contribuições para a Teoria dos Números, ele contribuiu para o estudo da convergência de séries trigonométricas, a Teoria das Séries de Fourier, ao estudo das funções harmônicas com condição de contorno que dão origem ao hoje conhecido Problema de Dirichlet e também contribuiu com uma solução da equação diferencial em um importante problema de hidrodinâmica. Ele estudou a estabilidade do sistema solar e também contribuiu em outras áreas. Por todo seu brilho ele foi homenageado por academias e instituições científicas durante sua vida e é claro tornou-se um grande matemático.