UNIVERSIDADE FEDERAL DO CEARÁ

CENTRO DE CIÊNCIAS

DEPARTAMENTO DE MATEMÁTICA

PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA EM REDE NACIONAL

THEDY BARBOSA BEZERRA

REPRESENTAÇÃO DE INTEIROS POR FORMAS QUADRÁTICAS BINÁRIAS

FORTALEZA

2019

THEDY BARBOSA BEZERRA

REPRESENTAÇÃO DE INTEIROS POR FORMAS QUADRÁTICAS BINÁRIAS

Dissertação apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional do Departamento de Matemática da Universidade Federal do Ceará, como parte dos requisitos necessários para a obtenção do título de Mestre em Matemática. Área de Concentração: Ensino de Matemática.

Orientador: Prof. Dr. Antonio Caminha Muniz Neto

FORTALEZA

2019

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Universitária
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

B469r Bezerra, Thedy Barbosa.
Representação de inteiros por formas quadráticas binárias / Thedy Barbosa Bezerra. – 2019.
60 f.

Dissertação (mestrado) – Universidade Federal do Ceará, Centro de Ciências, Departamento de Matemática, Programa de Pós-Graduação em Matemática em Rede Nacional, Fortaleza, 2019.
Orientação: Prof. Dr. Antonio Caminha Muniz Neto.

1. Formas quadráticas binárias. 2. Teoria dos Números. 3. Álgebra Abstrata. I. Título.

CDD 510

THEDY BARBOSA BEZERRA

REPRESENTAÇÃO DE INTEIROS POR FORMAS QUADRÁTICAS BINÁRIAS

Dissertação apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional do Departamento de Matemática da Universidade Federal do Ceará, como parte dos requisitos necessários para a obtenção do título de Mestre em Matemática. Área de Concentração: Ensino de Matemática.

Aprovada em:

BANCA EXAMINADORA

Prof. Dr. Antonio Caminha Muniz Neto (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. Angelo Papa Neto
Instituto Federal de Educação, Ciência e Tecnologia do Ceará (IFCE)

Prof. Dr. Ulisses Lima Parente
Universidade Estadual do Ceará (UECE)

A Deus.

À minha família e aos meus amigos.

AGRADECIMENTOS

A Deus, por me proporcionar esta conquista.

Aos meus pais, Marta Maria Barbosa Bezerra (*in memorian*) e Espedito Edilson Bezerra (*in memorian*), por todo amor que tiveram por mim.

Aos meus tios, Maria Holanda Barbosa Bié e Carlos de Sousa Bié, por todo carinho, acolhimento e incentivo a prosseguir nos estudos.

Ao meu irmão, Anthony Barbosa Bezerra (*in memorian*), por ter sido o meu melhor amigo e um grande entusiasta do meu crescimento pessoal.

Às minhas irmãs, Richele Barbosa Bezerra e Ruth Barbosa Rocha, pelo encorajamento frente aos obstáculos e por me instigarem a buscar meus objetivos.

Ao meu irmão, Carlos Alberto Bezerra, por suas palavras sábias de apoio nessa empreitada profissional.

Ao meu amigo, Felipe Anderson da Silva, pelas conversas de estímulo e pela amizade genuína, iniciada há muitos anos e que se prolonga até hoje.

À minha amiga, Edvania Ferreira Bandeira, pela amizade verdadeira, dialógos de ânimo e pelos momentos de atenção no processo de escrita.

A todos os professores do Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, da Universidade Federal do Ceará - UFC, pelo aprendizado adquirido e pelas valiosas contribuições no âmbito acadêmico.

Ao meu orientador, Prof. Dr. Antonio Caminha Muniz Neto, pela competência, confiança, empenho, excelente orientação e pelas preciosas colaborações referentes ao tema dissertado.

Ao integrante da banca examinadora de Defesa, Prof. Dr. Angelo Papa Neto, pela simplicidade, competência e por ter me iniciado no Latex.

Ao integrante da banca examinadora de Defesa, Prof. Dr. Ulisses Lima Parente, pelo tempo dedicado à leitura deste texto e pelas contribuições.

À Universidade Federal do Ceará - UFC.

A todos os colegas da turma iniciada em 2017 do PROFMAT - UFC, em especial, Francisco Erilson Freire de Oliveira e Antônio Erivan Bezerra Ferreira, pelo companheirismo, apoio, incentivo e pela parceria nos estudos, que nos proporcionou profunda aprendizagem no decorrer do curso.

A toda minha família e amigos que torceram por mim.

"LOUVAI ao Senhor. Louvai ao Senhor, porque ele é bom; porque a sua benignidade é para sempre."

(SALMO 106:1)

RESUMO

Este trabalho consiste em apresentar respostas às seguintes indagações: seja a forma quadrática binária $ax^2 + bxy + cy^2$, de discriminante $\Delta = b^2 - 4ac$, em duas variáveis x e y, com a, b, c números inteiros dados, nem todos 0; para quais inteiros n existem inteiros x e y tais que $n = ax^2 + bxy + cy^2$? Qual a caracterização dos inteiros positivos que podem ser escritos como soma de dois quadrados? Quais são os primos $p > 3$ que podem ser representados pela forma $2x^2 + 3y^2$ ou pela forma $x^2 + 6y^2$? Nesta dissertação, estudamos as teorias matemáticas que possibilitam a resolução dos questionamentos expostos acima. Nesse sentido, exibimos boa parte dos pré-requisitos imprescindíveis à apreciação dos resultados centrais que discutimos. Em seguida, discorremos sobre a representação de inteiros por formas quadráticas binárias, estabelecendo um critério útil, a partir do qual podemos determinar se um inteiro n é ou não representável por alguma forma quadrática, dado seu discriminante. Por fim, apresentamos respostas às duas últimas questões e tecemos nossas considerações relativas ao trabalho produzido, apontando para o que vai além da teoria desenvolvida aqui e reconhecendo a relevância das inter-relações entre áreas diferentes da Matemática.

Palavras-chave: Formas quadráticas binárias. Teoria dos Números. Álgebra Abstrata.

ABSTRACT

This works aims at giving answers to the following questions: let be given the binary quadratic form $ax^2+bxy+cy^2$, of discriminant $\Delta = b^2-4ac$, in the two variables x and y, with a, b ,c given integers, not all 0; for which integers n do exist integers x and y such that $n = ax^2+bxy+cy^2$? How can one characterize the positive integers which can be written as the sum of two squares? Which primes $p > 3$ can be represented by the form $2x^2+3y^2$ and by the form x^2+6y^2? In this report, we present the mathematical theories that allow us to elucidate the aforementioned questions. In this sense, we exhibit essentially all of the most important prerequisites needed for a full appreciation of the central results. We then present the elementary theory of presentation of integers by quadratic binary forms, establishing a useful criterion for deciding whether an integer n is or is not presentable by a quadratic binary form of given discriminant. Finally, we answer the posed questions, as well as some remarks related to the work in a broader sense, namely, pointing to further developments and to the relevance of assembling together different areas of Mathematics.

Keywords: Binary quadratic forms. Number Theory. Abstract Algebra.

SUMÁRIO

1 INTRODUÇÃO

Este trabalho fornece respostas às seguintes indagações: seja a forma quadrática binária $ax^2 + bxy + cy^2$, de discriminante $\Delta = b^2 - 4ac$, em duas variáveis x e y, com a, b, c números inteiros dados, nem todos 0; para quais inteiros n existem inteiros x e y tais que $n = ax^2 + bxy + cy^2$? Qual a caracterização dos inteiros positivos que podem ser escritos como soma de dois quadrados? Quais são os primos $p > 3$ que podem ser representados pela forma $2x^2 + 3y^2$ ou pela forma $x^2 + 6y^2$?

O estudo das teorias matemáticas que permitem a solução dos problemas mencionados acima teve início nos trabalhos de Pierre de Fermat (1601 - 1665), Leonhard Euler (1707 - 1783), Joseph-Louis Lagrange (1736 - 1813) e Adrien-Marie Legendre (1752 - 1833). Mas, coube a Carl Friedrich Gauss (1777 - 1855), no seu livro Disquisitiones Arithmeticae, publicado em 1801, ser o primeiro a expor uma teoria mais completa das formas quadráticas binárias.

Embora a matemática empregada para dar soluções a esses questionamentos demande conhecimentos mais profundos, o problema em si é de fácil compreensão. Desse modo, essas questões podem ser enunciadas a alunos da Educação Básica, devido aos seus caracteres familiares e à facilidade de entendimento de tais problemas.

O desdobramento realizado, nesta dissertação, das teorias referentes às formas quadráticas binárias e das aplicações dessas teorias tem por base o livro Number Theory, escrito por John Hunter e publicado, em 1964, pela editora americana Oliver and Boyd (HUNTER, 1964).

Após o capítulo inicial de introdução, esta dissertação se estrutura em quatro capítulos, descritos a seguir:

No segundo capítulo, intitulado "Preliminares", discorremos sobre alguns fundamentos relativos à Teoria dos Números e à Teoria de Grupos, que são imprescindíveis à assimilação dos conteúdos centrais deste trabalho, a serem expostos posteriormente. De início, apresentamos alguns pontos referentes a grupos e, logo após, expomos noções de relações e classes de equivalência, finalizando com o estudo de resíduos quadrádicos, os quais nos permitem reverenciar a elegante Lei da Reciprocidade Quadrática de Gauss.

No próximo capítulo, nomeado "Teoria Elementar de Formas Quadráticas Binárias", discutimos formas equivalentes, em que a noção de equivalêcia é crucial para o desenvolvimento da teoria, bem como a representação de inteiros por formas quadráticas binárias, relacionando duas áreas da Matemática, Teoria dos Números e Álgebra Abstrata, e produzindo um método

útil, firmado em resíduos quadráticos, para reconhecer se um inteiro n é ou não representável por alguma forma, dado seu discriminante.

O capítulo seguinte consiste em dar duas aplicações à teoria desenvolvida no capítulo anterior. A primeira delas, devida a Fermat, ainda no século XVII, caracteriza o conjunto de inteiros positivos representados pela forma $x^2 + y^2$, enquanto a segunda, problema presente no livro Number Theory (HUNTER, 1964), fornece uma caraterização dos primos $p > 3$ que podem ser representados por alguma forma quadrática binária de discriminante -24.

No último capítulo, tecemos nossas conclusões e considerações a respeito do trabalho elaborado, sinalizando para o que vai além da teoria desenvolvida nesta dissertação e reconhecendo a relevância das inter-relações entre campos distintos da Matemática.

2 PRELIMINARES

Neste capítulo, nossa intenção é apresentar alguns dos resultados indispensáveis para a leitura e a compreensão deste trabalho, iniciando com alguns fatos sobre grupos e, em seguida, definindo relações e classes de equivalência. Estudaremos, também, a resolubilidade ou não de congruências algébricas da forma $x^2 \equiv a \pmod{p}$, em que a é um inteiro e p é um primo tal que $(a,p) = 1$, coroando o capítulo com um famoso Teorema de Gauss, a Lei da Reciprocidade Quadrática.

Embora não tenhamos o propósito de exibir todos os pré-requisitos necessários à abordagem do objeto desta dissertação, este capítulo contém boa parte dos conteúdos necessários para a apreciação dos resultados centrais que discutiremos. Nesse sentido, assumimos que o leitor tenha familiaridade com os tópicos básicos referentes à Teoria dos Números, como divisibilidade e congruências, por exemplo. Boas referências nesse sentido são (ANDREWS, 1994), (NETO, 2013), (MOREIRA; MARTÍNEZ; SALDANHA, 2012), (MOREIRA; MARTÍNEZ; SALDANHA, 2018) ou (SANTOS, 2017).

2.1 Grupos

Um conjunto não vazio G, em que está definida uma operação binária

$$\begin{array}{rccc} * : & G \times G & \longrightarrow & G \\ & (a,b) & \longmapsto & a*b \end{array},$$

é denominado um **grupo** se são satisfeitas as seguintes condições:

1. $*$ é uma operação **associativa**, isto é, quaisquer que sejam $a,b,c \in G$, tem-se

$$(a*b)*c = a*(b*c);$$

2. $*$ tem **elemento identidade**, isto é, existe $e \in G$ tal que

$$e*a = a = a*e,$$

   para todo $a \in G$;

3. para cada $a \in G$, existe $a^{-1} \in G$ (chamado **inverso** de a em relação à operação $*$) tal que

$$a*a^{-1} = e = a^{-1}*a.$$

Se, além das condições anteriores, vale a condição

$$a*b = b*a,$$

para todos $a, b \in G$, dizemos que G é um grupo **comutativo** ou **abeliano**.

Doravante, dados $a, b \in G$, sempre que não houver perigo de confusão, denotaremos $a * b$ simplesmente por ab.

Exemplo: seja $G = M_{n\times m}(\mathbb{R})$ o conjunto de todas as matrizes sobre $\mathbb{R}$ de tipo $n \times m$. Então, munido com a operação usual de adição de matrizes, $M_{n\times m}(\mathbb{R})$ é um grupo abeliano.

Demonstração: se $A = [a_{ij}]$ e $B = [b_{ij}]$ são matrizes de tipo $n \times m$, então a operação usual de matrizes é definida por:

$A + B = C$, em que $C = [c_{ij}]$ é uma matriz de tipo $n \times m$ tal que $c_{ij} = a_{ij} + b_{ij}$, para todo $1 \leqslant i \leqslant n$ e para todo $1 \leqslant j \leqslant m$.

Agora, percebamos que para quaisquer que sejam as matrizes $A = [a_{ij}], B = [b_{ij}], C = [c_{ij}]$ de tipo $n \times m$, tem-se

$$\begin{aligned} A + (B + C) &= [a_{ij}] + [b_{ij} + c_{ij}] \\ &= [a_{ij} + (b_{ij} + c_{ij})] \\ &= [(a_{ij} + b_{ij}) + c_{ij}] \\ &= [a_{ij} + b_{ij}] + [c_{ij}] \\ &= (A + B) + C, \end{aligned}$$

mostrando, assim, que a operação é associativa.

Ademais, existe

$$O = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix} \in G$$

tal que

$$A + O = O + A = A,$$

para todo $A \in G$, e, sendo assim, O é o elemento neutro da adição de matrizes.

Por último, dada a matriz

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nm} \end{bmatrix} \in G,$$

existe

$$-A = \begin{bmatrix} -a_{11} & -a_{12} & \cdots & -a_{1m} \\ -a_{21} & -a_{22} & \cdots & -a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & -a_{nm} \end{bmatrix} \in G$$

tal que

$$A + (-A) = (-A) + A = O,$$

e, em vista disso, $-A$ é o inverso aditivo (nesse caso denominado o *simétrico*) de A. Além de tudo, é notório que

$$A + B = B + A,$$

para todos $A, B \in G$. Portanto, G é um grupo abeliano com a operação adição usual de matrizes.

□

Se G é um grupo, $g \in G$ e $k \in \mathbb{Z}$, definimos

$$g^k = \underbrace{g \cdot \ldots \cdot g}_{k \text{ vezes}}, \text{ se } k > 0; \;\; g^k = e, \text{ se } k = 0; \;\; g^k = \underbrace{g^{-1} \cdot \ldots \cdot g^{-1}}_{k \text{ vezes}} \text{ se } k < 0.$$

É possível mostrar que, com essa definição, ainda valem as propriedades

$$(g^k)^l = g^{kl} \text{ e } g^{k+l} = g^k \cdot g^l, \; \forall \, k, l \in \mathbb{Z}.$$

Dados um grupo G e um elemento $g \in G$, definimos a **ordem** de g, denotada $\mathscr{O}(g)$, da seguinte forma:

$$\mathscr{O}(g) = \begin{cases} k, \text{ se } k \text{ é o menor natural tal que } g^k = e \\ +\infty, \text{ se não existe } k \text{ natural tal que } g^k = e \end{cases}.$$

Os resultados a seguir apresentam as propriedades mais importantes do conceito de ordem em grupos abelianos.

Lema 2.1.1 *Sejam G um grupo dado e $g,h \in G$ elementos de ordens $\mathcal{O}(g) = k$ e $\mathcal{O}(h) = l$, ambas finitas.*

(a) Se $0 \leqslant u, v < k$ são distintos, então $g^u \neq g^v$.

(b) $g^n = e \Longleftrightarrow k \mid n$.

(c) Se $t \mid k$, então $\mathcal{O}(g^t) = \frac{k}{t}$.

(d) Se $gh = hg$ e $(k,l) = 1$, então $\mathcal{O}(gh) = kl$.

Demonstração:

(a) Suponhamos, sem perda de generalidade, que $u > v$. Se fosse $g^u = g^v$, teríamos $g^{u-v} = g^u \cdot g^{-v} = g^u \cdot (g^v)^{-1} = e$. Mas, como $0 < u - v < k$, isso seria uma contradição à definição de k.

(b) Se $n = kq$, então $g^n = (g^k)^q = e^q = e$. Reciprocamente, suponhamos que $g^n = e$ e divida n por k, obtendo $n = kq + r$, com $0 \leqslant r < k$. Temos

$$e = g^n = g^{kq+r} = (q^k)^q \cdot g^r = e^q \cdot g^r = g^r.$$

Como $g^r = e$ e k é o menor natural tal que $g^k = e$ e $0 \leqslant r < k$, a única possibilidade é termos $r = 0$. Logo, $n = kq$ e, daí, $k \mid n$.

(c) Seja $\mathcal{O}(g^t) = s$. Por um lado, é claro que $(g^t)^{\frac{k}{t}} = g^k = e$, de forma que $s \leqslant \frac{k}{t}$. Por outro lado,

$$(g^t)^s = e \Longrightarrow g^{ts} = e \Longrightarrow ts \geqslant k \Longrightarrow s \geqslant \frac{k}{t}.$$

Logo, $s = \frac{k}{t}$.

(d) Como $gh = hg$, temos $(gh)^n = g^n h^n$, para todo $n \in \mathbb{N}$. Então,

$$(gh)^{kl} = g^{kl} h^{kl} = (g^k)^l (h^l)^k = e^l e^k = e,$$

e a definição de ordem garante que $\mathcal{O}(gh) \mid (kl)$.

Seja $\mathcal{O}(gh) = uv$, com $u \mid k$ e $v \mid l$. Como $(k,l) = 1$, temos $(u,v) = 1$. Então,

$$(gh)^{uv} = e \Longrightarrow g^u h^v = e \Longrightarrow (g^u h^v)^{\frac{k}{u}} = e^{\frac{k}{u}} \Longrightarrow g^k h^{\frac{vk}{u}} = e$$
$$\Longrightarrow e h^{\frac{vk}{u}} = e \Longrightarrow h^{\frac{vk}{u}} = e \Longrightarrow l \mid \left(\frac{vk}{u}\right),$$

onde utilizamos o item (b) na última implicação. Mas, como $(k,l)=1$, temos também $\left(l,\frac{k}{u}\right)=1$. Logo, $l \mid \left(v\cdot\frac{k}{u}\right) \Longrightarrow l \mid v$. Como já tínhamos que $v \mid l$, segue que $v=l$. Analogamente, $u=k$, de sorte que $\mathscr{O}(gh)=uv=kl$.

□

Para o próximo resultado, se G é um grupo abeliano tal que $\mathscr{O}(g)<+\infty$ para todo $g\in G$, definimos o **expoente** de G, denotado $\exp(G)$, pondo

$$\exp(G) := \text{mmc}\{\mathscr{O}(g);\ g\in G\},$$

com a convenção de que pode ser $\exp(G)=+\infty$.

Proposição 2.1.1 *Seja G um grupo abeliano tal que $\mathscr{O}(g)<+\infty$ para todo $g\in G$. Se $\exp(G)$ é finito, então existe $g\in G$ tal que $\mathscr{O}(g)=\exp(G)$.*

Demonstração: se $\exp(G)=1$, não há nada a fazer. Senão, seja $\exp(G)=p_1^{\alpha_1}\ldots p_k^{\alpha_k}$, com $p_1<\ldots<p_k$ primos e $\alpha_1,\ldots,\alpha_k\geqslant 1$.

Uma vez que $\exp(G)$ é o mmc das ordens dos elementos de G, existem $g_1,\ldots,g_k\in G$ tais que $\mathscr{O}(g_i)=p_i^{\alpha_i}m_i$ para algum $m_i\in\mathbb{N}$. Então, segue do item (c) do lema anterior que $\mathscr{O}(g_i^{m_i})=p_i^{\alpha_i}$.

Aplicando o item (d) do lema anterior várias vezes, obtemos

$$\mathscr{O}(g_1^{m_1}\ldots g_k^{m_k})=p_1^{\alpha_1}\ldots p_k^{\alpha_k}=\exp(G),$$

de sorte que basta fazer $g=g_1^{m_1}\ldots g_k^{m_k}$.

□

Definição 2.1.1 *Um grupo G é **cíclico** se existir $a\in G$ tal que*

$$G=\{a^k;\ k\in\mathbb{Z}\}.$$

Um exemplo de grupo cíclico é $\mathbb{Z}$, munido com a operação de adição de inteiros. Posteriormente, veremos outro exemplo relevante.

2.2 Relações de equivalência

Esta seção é destinada à apresentação da definição de uma relação de equivalência em um conjunto A qualquer, a qual classifica os elementos desse conjunto em classes de equivalência.

Seja A um conjunto não vazio. Uma **relação de equivalência** $\sim$ em A é uma relação que satisfaz as seguintes propriedades:

1. $a \sim a$, para todo $a \in A$ (reflexividade);
2. Se $a \sim b$, então $b \sim a$, para todos $a, b \in A$ (simetria);
3. Se $a \sim b$ e $b \sim c$, então $a \sim c$, para todos $a, b, c \in A$ (transitividade).

Exemplo: seja m um número natural fixado. A relação de congruência módulo m, em $\mathbb{Z}$, definida por

$$a \equiv b \pmod{m} \Longleftrightarrow a - b = km, \text{ para algum } k \in \mathbb{Z},$$

é uma relação de equivalência em $\mathbb{Z}$.

Demonstração: para todo $a \in \mathbb{Z}$, tem-se que $a - a = 0 \cdot m$ e, consequentemente,

$$a \equiv a \pmod{m},$$

o que mostra que a relação $\equiv \pmod{m}$ é reflexiva.

Agora, se $a \equiv b \pmod{m}$, segue-se da definição que $a - b = km$, com $k \in \mathbb{Z}$. Daí,

$$b - a = (-k)m, \text{ com } -k \in \mathbb{Z},$$

ou, equivalentemente, $b \equiv a \pmod{m}$. Assim, a relação $\equiv \pmod{m}$ é simétrica.

Enfim, se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então

$$a - b = k'm \text{ e } b - c = k''m, \text{ com } k', k'' \in \mathbb{Z},$$

o que implica que

$$a - c = (k' + k'')m, \text{ com } k' + k'' \in \mathbb{Z},$$

ou seja, $a \equiv c \pmod{m}$. Logo, a relação $\equiv \pmod{m}$ é transitiva. Portanto, com base no que foi apresentado acima, temos que $\equiv$ é uma relação de equivalência em $\mathbb{Z}$.

□

A seguir, apresentaremos a definição de classe de equivalência, que representa a consequência mais importante da existência de uma relação de equivalência em um conjunto, pois o particiona em subconjuntos disjuntos, cada um dos quais composto por elementos dois a dois relacionados.

Sejam A um conjunto não vazio e $\sim$ uma relação de equivalência em A. Para cada $a \in A$, definimos o conjunto

$$[a] = \{b \in A : b \sim a\},$$

o qual é denominado a **classe de equivalência** de a relativa a $\sim$. Vale observar que o símbolo $\overline{a}$ também é comumente utilizado para representar $[a]$.

O resultado seguinte nos diz que uma relação de equivalência em um conjunto não vazio A gera uma partição desse conjunto em classes de equivalência.

Proposição 2.2.1 *Seja $\sim$ uma relação de equivalência em um conjunto $A \neq \emptyset$. Então:*

(a) Para todos $a, b \in A$, $[a] = [b]$ se, e somente se, $a \sim b$;

(b) Para todos $a, b \in A$, se $[a] \neq [b]$, então $[a] \cap [b] = \emptyset$;

(c) O conjunto $\bigcup_{a \in A} [a] = A$ é uma partição de A.

Demonstração:

(a) Sabendo-se que $a \in [a]$ e, por hipótese, $[a] = [b]$, temos que $a \in [b]$, o implica que $a \sim b$.

Reciprocamente, se $c \in [a]$, então $c \sim a$. Como, por hipótese, $a \sim b$, temos que $c \sim b$ (transitividade) e, portanto, $c \in [b]$. Assim, $[a] \subset [b]$. Similarmente, é possível mostrar facilmente que $[b] \subset [a]$. Logo, $[a] = [b]$.

(b) Suponhamos, por absurdo, que $[a] \neq [b]$ mas $[a] \cap [b] \neq \emptyset$. Então, existe $c \in [a] \cap [b]$, de sorte que $c \sim a$ e $c \sim b$. Agora, usando a simetria, temos que $a \sim c$, e, pela transitividade, $a \sim b$. Por fim, pela parte (a) desta proposição, segue que $[a] = [b]$, o que é uma contradição.

(c) De fato, para cada $a \in A$, temos que $[a] \subset A$. Logo,

$$\bigcup_{a \in A} [a] \subset A.$$

Por outro lado, para cada $a \in A$, temos que $a \in [a]$, uma vez que $a \sim a$. Então, $a \in \bigcup_{a \in A} [a]$ e, portanto,

$$A \subset \bigcup_{a \in A} [a].$$

Assim, podemos concluir que

$$\bigcup_{a \in A} [a] = A.$$

□

Exemplo: seja m um inteiro positivo dado. A relação de congruência módulo m, em $\mathbb{Z}$, possui as seguintes propriedades:

i) $\overline{a} = \overline{b}$ se, e somente se, $a \equiv b \pmod{m}$;

ii) Se $\overline{a} \neq \overline{b}$, então $\overline{a} \cap \overline{b} = \emptyset$;

iii) $\mathbb{Z} = \overline{0} \cup \overline{1} \cdots \cup \overline{m-1}$, em que $\overline{i} \cap \overline{j} = \emptyset$, se $i \neq j$, com $0 \leqslant i, j \leqslant m-1$.

Denotando

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\},$$

defina as operações $\oplus$ e $\odot$ em $\mathbb{Z}_m$ pondo

$$\overline{a} \oplus \overline{b} = \overline{a+b} \text{ e } \overline{a} \odot \overline{b} = \overline{a \cdot b}.$$

Utilizando as propriedades de congruências, não é difícil mostrar que tais operações estão bem definidas, no sentido de que os resultados de $\overline{a} \oplus \overline{b}$ e $\overline{a} \odot \overline{b}$ não dependem dos representantes das classes $\overline{a}$ e $\overline{b}$.

As propriedades de congruência também permitem mostrar que $\left(\mathbb{Z}_m, \oplus\right)$ é um grupo abeliano.

Por outro lado, veja que $(mq + r, m) = (r, m)$, em que $q, r \in \mathbb{Z}$ e $0 \leqslant r < m$. Desse modo, podemos definir o mdc entre uma classe de congruência módulo m e m, pondo

$$(\overline{r}, m) = (a, m), \text{ para algum } a \in \overline{r}.$$

Observemos que as classes de congruência $\overline{r}$, módulo m, com $(\overline{r}, m) = 1$, são formadas pelos inteiros invertíveis módulo m. Assim, um **sistema completo de invertíveis** módulo m

(**SCI**) é um conjunto I de inteiros tal que

$$|I \cap \overline{r}| = \begin{cases} 1, \text{ se } (\overline{r}, m) = 1 \\ 0, \text{ se } (\overline{r}, m) \neq 1 \end{cases},$$

para cada classe de congruência $\overline{r}$, módulo m. Em particular, fixando um inteiro $m > 1$, o conjunto

$$\mathbb{Z}_m^{\times} = \{a \in \mathbb{Z};\ (a,m) = 1 \text{ e } 1 \leqslant a \leqslant m\}$$

é um SCI módulo m.

Exemplo: $\left(\mathbb{Z}_m^{\times}, \odot\right)$ é um grupo abeliano.

Demonstração: deixando a verificação da associatividade a cargo do leitor, observamos que o elemento neutro é $\overline{1}$. Para mostrar que toda classe $\overline{a} \in \mathbb{Z}_m^{\times}$ tem um inverso, digamos $\overline{b}$, em relação à operação $\odot$, veja que

$$\overline{a} \odot \overline{b} = \overline{1} \Longleftrightarrow ab \equiv 1 \,(\mathrm{mod}\, m).$$

Mas, como $\overline{a} \in \mathbb{Z}_m^{\times} \Longrightarrow (a,m) = 1$, o Teorema de Bézout (para uma demonstração, sugerimos ao leitor a seção 1.2 de (NETO, 2013)) garante a existência de $b, c \in \mathbb{Z}$ tais que $ab + cm = 1$. Então, $ab \equiv 1 (\mathrm{mod}\, m)$, como queríamos.

□

Daqui em diante, denotaremos $\oplus$ e $\odot$ simplesmente por $+$ e $\cdot$, sempre que não houver perigo de confusão.

Para continuar, precisamos da seguinte

Definição 2.2.1 *Sejam $a, m \in \mathbb{Z}$, com $m > 1$ e $(a,m) = 1$. A **ordem** de a, módulo m, é o natural*

$$ord_m(a) = min\{h \in \mathbb{N};\ a^h \equiv 1\ (mod\ m)\}.$$

Assim, se $(a,m) = 1$, a ordem de a módulo m é precisamente a ordem de $\overline{a}$ no grupo $\mathbb{Z}_m^{\times}$. Denotando o número de elementos de $\mathbb{Z}_m^{\times}$ por $\varphi(m)$, Euler provou que

$$a^{\varphi(m)} \equiv 1 \ (\mathrm{mod}\ m),$$

de sorte que, pelo Lema 2.1.1, tem-se

$$\mathrm{ord}_m(a) \mid \varphi(m).$$

Também por aquele resultado, temos que:

i) $a^k \equiv 1 \pmod{m} \iff \text{ord}_m(a) \mid k$.

ii) Se $\text{ord}_m(a) = h$, então os inteiros $1, a, a^2, \ldots, a^{h-1}$ são dois a dois incongruentes, módulo m. Especialmente, se $\text{ord}_m(a) = \varphi(m)$, então o conjunto de inteiros $\{1, a, a^2, \ldots, a^{\varphi(m)-1}\}$ é um SCI, módulo m.

2.3 Resíduos quadráticos

Nesta última seção, estudaremos as congruências algébricas do tipo $x^2 \equiv a \pmod{p}$, em que $a \in \mathbb{Z}$, p é um número primo e $(a, p) = 1$. O ponto alto é o teorema denominado na literatura como a **lei da reciprocidade quadrática** de Gauss. Assim, inicialmente, precisamos da seguinte definição.

Definição 2.3.1 *Sejam p um número primo e $a \in \mathbb{Z}$, com $(a, p) = 1$. Diremos que a é **resíduo quadrático**, módulo p, quando a congruência $x^2 \equiv a \pmod{p}$ possuir alguma solução inteira; caso contrário, diremos que a **não é resíduo quadrático**, módulo p.*

O teorema a seguir, devido a Fermat e conhecido na literatura como o **pequeno teorema de Fermat**, será imprescindível na prova de alguns resultados relevantes contidos neste trabalho. Antes de demonstrá-lo, precisamos do lema auxiliar a seguir.

Lema 2.3.1 *Seja p um número primo. Então, p divide todos os números $\binom{p}{j}$, com $0 < j < p$.*

Demonstração: para $j = 1$, o resultado segue claramente. A partir de agora, podemos, então, supor $1 < j < p$. Como

$$\binom{p}{j} = p \cdot \frac{(p-1)\ldots(p-j+1)}{j!},$$

temos que $j! \mid p(p-1)\ldots(p-j+1)$. Mas, de $(j!, p) = 1$, vem que

$$j! \mid (p-1)\ldots(p-j+1).$$

Consequentemente, o resultado segue.

□

Teorema 2.3.1 *Dados $a, p \in \mathbb{Z}$, em que p é primo, tem-se que $a^p \equiv a \pmod{p}$. Em particular, se $(a,p) = 1$, então $a^{p-1} \equiv 1 \pmod{p}$.*

Demonstração: inicialmente, supondo que $a^p \equiv a \pmod{p}$, temos que p divide $a^p - a = a(a^{p-1} - 1)$. Daí, se $(a,p) = 1$, então $a^{p-1} \equiv 1 \pmod{p}$. Agora, nos resta mostrar que $a^p \equiv a \pmod{p}$, para todo $a \in \mathbb{Z}$.

Se $p = 2$, o resultado é trivial, pois $a^2 - a = a(a-1)$, um produto de dois inteiros consecutivos, logo, par. Suponhamos $p > 2$ e provemos o resultado por indução sobre a, para $a > 0$. (Note que basta provarmos o resultado nesse caso.)

Para $a = 1$, o resultado segue claramente.

Suponhamos, por indução, o teorema verificado para algum natural a e provemos que ele também é verdadeiro para $a+1$. Pela fórmula do Binômio de Newton, temos que

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

Assim, pelo lema 2.3.1 e pela hipótese de indução, temos que $p \mid \binom{p}{j}$, com $0 < j < p$, e $p \mid (a^p - a)$, respectivamente. Isso prova que p divide $(a+1)^p - (a+1)$, concluindo a demonstração do teorema.

□

O resultado a seguir nos fornece uma lista completa dos resíduos quadráticos módulo p, determinando quantos são esses resíduos.

Proposição 2.3.2 *Seja p um primo ímpar. Dentre os números $1, 2, \ldots, p-1$, há exatamente $\frac{p-1}{2}$ resíduos quadráticos módulo p, dois a dois incongruentes, a saber: $1^2, 2^2, \ldots, (\frac{p-1}{2})^2$.*

Demonstração: inicialmente, notemos que se a é resíduo quadrático módulo p, então a é congruente, módulo p, a um dos seguintes números: $1^2, 2^2, \ldots, (p-1)^2$. Observemos, ainda, que dentre esses números há repetições, módulo p, já que

$$a^2 \equiv (p-a)^2 \pmod{p}, \text{ para } 1 \leqslant a \leqslant \frac{p-1}{2}.$$

Assim, a lista de números $1^2, 2^2, \ldots, (\frac{p-1}{2})^2$ representa todos os resíduos quadráticos módulo p, faltando mostrar que são dois a dois incongruentes.

Para tanto, se $i, j \in \{1, 2, \ldots, \frac{p-1}{2}\}$, com $i < j$, então

$$i^2 \not\equiv j^2 \pmod{p},$$

visto que $j^2 - i^2 = (j-i)(j+i)$ e, além disso, $0 < j-i < j+i < p$.

Portanto, de modo preciso, há $\frac{p-1}{2}$ resíduos quadráticos módulo p e, consequentemente, $(p-1) - (\frac{p-1}{2}) = \frac{p-1}{2}$ não resíduos quadráticos módulo p, como queríamos provar.

□

Para completar os pré-requisitos necessários ao entendimento do resultado a seguir, atentemos para a seguinte

Definição 2.3.2 *Sejam $a, m \in \mathbb{Z}$, com $m > 1$ e $(a,m) = 1$. Quando $ord_m(a) = \varphi(m)$, dizemos que a é uma **raiz primitiva**, módulo m.*

Dado um primo p, para mostrarmos que existem raízes primitivas módulo p, seja $G = \mathbb{Z}_p^{\times} = \mathbb{Z}_p \setminus \{\overline{0}\}$. Claramente, G é um grupo abeliano, quando munido com a multiplicação de classes de congruência módulo p; além disso, $|G| = p-1$.

Se mostrarmos que G é cíclico, existirá $a \in \mathbb{Z}$ tal que $(a,p) = 1$ e $\mathcal{O}(\overline{a}) = p-1$. Então, $p-1$ será o menor natural k tal que $\overline{a}^k = \overline{1}$ ou, o que é o mesmo, $a^k \equiv 1 \pmod{p}$. Em outras palavras, a será uma raiz primitiva módulo p.

Lema 2.3.2 *Um polinômio com coeficientes em $\mathbb{Z}_p$ de grau k tem no máximo k raízes distintas em $\mathbb{Z}_p$.*

Demonstração: façamos indução sobre o grau n de $f(X) = \overline{a}_n X^n + \cdots + \overline{a}_1 X + \overline{a}_0$. Aqui, $\overline{a}_0, \ldots, \overline{a}_n \in \mathbb{Z}_p$, com $\overline{a}_n \neq \overline{0}$.

Se $n = 1$, então $f(X) = \overline{a}_1 X + \overline{a}_0$, de forma que

$$f(\overline{x}) = \overline{0} \Longleftrightarrow \overline{a}_1\overline{x} + \overline{a}_0 = \overline{0} \Longleftrightarrow \overline{x} = -\overline{a}_0 \cdot \overline{a}_1^{-1}.$$

Portanto, nesse caso, $\partial f = 1$ e f tem exatamente uma raiz em $\mathbb{Z}_p$.

Suponhamos, por hipótese de indução, que o resultado vale sempre que $\partial f = k < n$. Para f de grau n, dado como acima, há duas possibilidades:

i) f não tem raízes em $\mathbb{Z}_p$: nesse caso, nada há a fazer.

ii) f tem uma raiz $\overline{a}$ em $\mathbb{Z}_p$. Como $f(\overline{a}) = \overline{0}$ e

$$X^j - \overline{a}^j = (X - \overline{a})(X^{j-1} + \overline{a}X^{j-2} + \cdots + \overline{a}^{j-2}X + \overline{a}^{j-1})$$

para todo $m \in \mathbb{N}$, podemos escrever

$$f(X) = f(X) - f(\overline{a}) = \sum_{j=0}^{n} \overline{a}_j (X^j - \overline{a}^j) = (X - \overline{a}) g(X),$$

com $\partial g = n - 1$. Por hipótese de indução, g tem no máximo $n-1$ raízes em $\mathbb{Z}_p$. Como as raízes de f são $\overline{a}$ e as raízes de g, concluímos que f tem no máximo $(n-1)+1 = n$ raízes em $\mathbb{Z}_p$.

□

Teorema 2.3.3 *Se p é primo e $G = (\mathbb{Z}_p^{\times}, \cdot)$, então G é cíclico.*

Demonstração: seja $k := \exp(G)$. Como G é abeliano e finito, temos $k < +\infty$ e, pela proposição 2.1.1, podemos tomar $\overline{a} \in G$ (isto é, $a \in \mathbb{Z}$ com $(a,p) = 1$) tal que $\mathscr{O}(\overline{a}) = k$. Como $e, \overline{a}, \overline{a}^2, \ldots, \overline{a}^{k-1}$ são dois a dois distintos, temos que $p - 1 = |G| \geqslant k$.

Por outro lado, a definição de $\exp(G)$ garante que $\mathscr{O}(g) \mid k$ para todo $g \in G$, de sorte que $g^k = \overline{1}$, para todo $g \in G$. Portanto,

$$G \subset \mathscr{R}_{X^k - \overline{1}},$$

em que $\mathscr{R}_{X^k - \overline{1}}$ denota o conjunto das raízes, em $\mathbb{Z}_p$, do polinômio $X^k - \overline{1}$.

Pelo lema anterior, segue que $p - 1 = |G| \leqslant k$. Então, $p - 1 = |G| = k$, e $G = \{\overline{a}^l ; l \in \mathbb{Z}\}$. Logo, G é cíclico.

□

A proposição a seguir é atribuída a Euler e denominada na literatura como o **critério de Euler**. Ela nos dará uma condição necessária e suficiente para determinar se um inteiro a é ou não resíduo quadrático módulo p, em que p é um primo ímpar.

Proposição 2.3.4 (Euler) *Se p é um primo ímpar, então um inteiro a é resíduo quadrático módulo p se, e somente se, $a^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$.*

Demonstração: inicialmente, suponhamos que a é resíduo quadrático módulo p. Então, $(a,p) = 1$ e existe $\alpha \in \mathbb{Z}$ tal que $\alpha^2 \equiv a \pmod{p}$. Veja que α e p são coprimos, pois, como $(a,p) = 1$ e $a = \alpha^2 + kp$, para algum $k \in \mathbb{Z}$, segue-se facilmente que $(\alpha, p) = (a,p) = 1$. Logo, pelo pequeno teorema de Fermat, temos que

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

Reciprocamente, suponhamos que $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Consequentemente, $(a,p) = 1$. Sendo β uma raiz primitiva módulo p, seque que $\{1, \beta, \beta^2, \ldots, \beta^{p-1}\}$ é um SCI, módulo p. Daí, existe um inteiro j, com $1 \leqslant j \leqslant p-1$, tal que $\beta^j \equiv a \pmod{p}$. Assim,

$$(\beta^j)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

pelo pequeno teorema de Fermat.

Como $\text{ord}_p(\beta) = p-1$, temos que $(p-1) \mid j(\frac{p-1}{2})$, o que implica que j é divisível por 2, isto é, $j = 2k$, com $k \in \mathbb{Z}$. Por fim, observando que

$$(\beta^k)^2 = \beta^j \equiv a \pmod{p},$$

concluímos que a é um resíduo quadrático módulo p.

□

Corolário 2.3.1 *Se p é um primo ímpar, então um inteiro a coprimo com p não é resíduo quadrático módulo p se, e somente se, $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.*

Demonstração: temos do pequeno teorema de Fermat que

$$(a^{\frac{p-1}{2}} + 1)(a^{\frac{p-1}{2}} - 1) = a^{p-1} - 1 \equiv 0 \pmod{p};$$

assim,

$$p \mid (a^{\frac{p-1}{2}} + 1) \text{ ou } p \mid (a^{\frac{p-1}{2}} - 1). \tag{2.1}$$

Mas, como $p > 2$, as afirmações em (2.1) não podem ocorrer de modo simultâneo, uma vez que, se ocorressem, p dividiria

$$(a^{\frac{p-1}{2}} + 1) - (a^{\frac{p-1}{2}} - 1) = 2,$$

o que é claramente uma contradição.

Portanto, pelo critério de Euler, a não é resíduo quadrático módulo p se, e somente se, a segunda afirmação em (2.1) não ocorre, ou seja, se, e somente se, $p \mid (a^{\frac{p-1}{2}} + 1)$.

□

Para lidar mais facilmente com resíduos e não resíduos quadráticos, lançaremos mão de uma notação conveniente, que será posta a seguir.

Sejam $a, p \in \mathbb{Z}$, com p primo. Definimos o **símbolo de Legendre** $\left(\frac{a}{p}\right)$ como

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

A proposição a seguir nos revela a razão pela qual é vantajosa a notação do símbolo de Legendre, apresentando suas propriedades.

Proposição 2.3.5 *Sejam p um primo ímpar e $a, b \in \mathbb{Z}$.*

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

(b) Se $p \nmid a$, então $\left(\frac{a^2}{p}\right) = 1$.

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

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

Demonstração:

(a) Inicialmente, vejamos que $a \equiv b \pmod{p}$ implica $(a, p) = (b, p)$. Por outro lado, como $a \equiv b \pmod{p}$, a congruência $x^2 \equiv a \pmod{p}$ tem solução se, e somente se, a congruência $x^2 \equiv b \pmod{p}$ tem solução.

(b) Se $p \nmid a$, então $\left(\frac{a^2}{p}\right) = 1$, já que a é solução da congruência $x^2 \equiv a^2 \pmod{p}$. Particularmente, $\left(\frac{1}{p}\right) = 1$.

(c) A demonstração deste item é imediata do critério de Euler e da definição do símbolo de Legendre.

(d) Primeiro, se $p \mid ab$, então $p \mid a$ ou $p \mid b$. Assim,

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = 0 = \left(\frac{ab}{p}\right).$$

Por outro lado, se $p \nmid ab$, então $p \nmid a$ e $p \nmid b$, e, aplicando o critério de Euler, temos que

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

Da congruência acima, temos que p divide $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) - \left(\frac{ab}{p}\right)$, isto é, p divide um inteiro do intervalo $[-2,2]$. Agora, como p é ímpar, podemos deduzir que essa diferença dá 0, concluindo que

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

□

Corolário 2.3.2 *Se p é um primo ímpar, então*

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

Demonstração: pela proposição (2.3.5), temos

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

Mas, como $p > 2$ e ambos os membros da congruência acima são iguais a ± 1, concluímos que

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

conforme desejado.

□

O próximo resultado, também atribuído a Gauss e conhecido como o **lema de Gauss**, nos fornece um método mais simples do que o critério de Euler para calcular o símbolo de Legendre $\left(\frac{a}{p}\right)$, em que p é um primo ímpar e a é um inteiro coprimo com p.

Proposição 2.3.6 (Gauss) *Sejam p um primo ímpar e a um inteiro coprimo com p. Seja m o número de elementos do conjunto*

$$\left\{a, 2a, \ldots, \left(\frac{p-1}{2}\right)a\right\}$$

que, na divisão por p, deixam resto maior do que $\frac{p-1}{2}$. Então

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

Demonstração: primeiramente, como $(a,p)=1$, os elementos do conjunto $\{a,2a,\ldots,(\frac{p-1}{2})a\}$ são dois a dois incongruentes, módulo p. Realmente, caso contrário teríamos $ia \equiv ja \pmod{p}$, com $i \neq j$ e $1 \leqslant i,j \leqslant \frac{p-1}{2}$; mas isto implicaria $i \equiv j \pmod{p}$, o que é impossível. Sejam $r_1, r_2, \ldots, r_{\frac{p-1}{2}}$ os restos da divisão dos números $a, 2a, \ldots, (\frac{p-1}{2})a$ por p, respectivamente, de sorte que $r_1, r_2, \ldots, r_{\frac{p-1}{2}} \in \{1,2,\ldots,p-1\}$ são todos distintos.

Vamos dividir o conjunto $\{r_1, r_2, \ldots, r_{\frac{p-1}{2}}\}$ em outros dois, a saber: $X = \{x_1, x_2, \ldots, x_m\}$, formado pelos elementos maiores do que $\frac{p-1}{2}$, e $Y = \{y_1, y_2, \ldots, y_n\}$, formado pelos elementos menores ou iguais a $\frac{p-1}{2}$.

Claramente, podemos observar que os números $p-x_1, p-x_2, \ldots, p-x_m$ são menores do que $\frac{p-1}{2}$ e distintos uns dos outros. Ademais, tais números são diferentes dos números $y_1, y_2, \ldots, y_n$, uma vez que, caso $p-x_l = y_s$, com $1 \leqslant l \leqslant m$ e $1 \leqslant s \leqslant n$, teríamos $x_l + y_s \equiv 0 \pmod{p}$, isto é, $r_i + r_j \equiv 0 \pmod{p}$, para certos $1 \leqslant i,j \leqslant \frac{p-1}{2}$ distintos; mas aí, viria que $ia + ja \equiv 0 \pmod{p}$, com $2 < i+j < p$, um absurdo. Assim, $m+n = \frac{p-1}{2}$ e, consequentemente,

$$\{p-x_1, p-x_2, \ldots, p-x_m\} \cup \{y_1, y_2, \ldots, y_n\} = \left\{1, 2, \ldots, \frac{p-1}{2}\right\}.$$

Por sua vez, a igualdade acima fornece

$$(p-x_1)(p-x_2)\ldots(p-x_m)y_1y_2\ldots y_n = \left(\frac{p-1}{2}\right)!. \tag{2.2}$$

Por outro lado, observando que $r_k \equiv ia \pmod{p}$, com $1 \leqslant k,i \leqslant \frac{p-1}{2}$, segue que

$$x_1x_2\ldots x_my_1y_2\ldots y_n \equiv a^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!. \tag{2.3}$$

De (2.2) e (2.3), temos que

$$x_1x_2\ldots x_my_1y_2\ldots y_n \equiv a^{\frac{p-1}{2}}(p-x_1)(p-x_2)\ldots(p-x_m)y_1y_2\ldots y_n \pmod{p},$$

o que acarreta

$$x_1x_2\ldots x_m \equiv a^{\frac{p-1}{2}}(p-x_1)(p-x_2)\ldots(p-x_m) \pmod{p}.$$

Então, módulo p, temos

$$x_1x_2\ldots x_m \equiv a^{\frac{p-1}{2}}(-x_1)(-x_2)\ldots(-x_m) = a^{\frac{p-1}{2}}(-1)^m x_1x_2\ldots x_m \pmod{p},$$

de sorte que

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

Por sua vez, isso implica, imediatamente,

$$a^{\frac{p-1}{2}} \equiv (-1)^m \pmod{p};$$

consequentemente, pela terceira parte da proposição 2.3.5, temos

$$\left(\frac{a}{p}\right) \equiv (-1)^m \pmod{p}.$$

□

A partir do lema de Gauss, a proposição a seguir nos fornece uma outra regra para calcular o símbolo de Legendre.

Proposição 2.3.7 *Sejam um primo $p > 2$ e a um natural ímpar, com $(a, p) = 1$. Se*

$$t = \left\lfloor \frac{a}{p} \right\rfloor + \left\lfloor \frac{2a}{p} \right\rfloor + \cdots + \left\lfloor \frac{\frac{p-1}{2}a}{p} \right\rfloor,$$

então

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

Demonstração: utilizando as mesmas notações aplicadas na prova do lema de Gauss, temos que

$$\begin{aligned} a &= p\left\lfloor \frac{a}{p} \right\rfloor + r_1 \\ 2a &= p\left\lfloor \frac{2a}{p} \right\rfloor + r_2 \\ &\vdots \\ \tfrac{p-1}{2}a &= p\left\lfloor \frac{\frac{p-1}{2}a}{p} \right\rfloor + r_{\frac{p-1}{2}} \end{aligned} \quad .$$

Das igualdades acima, somando-as membro a membro, obtemos

$$\frac{p^2-1}{8}a = pt + (r_1 + r_2 + \cdots + r_{\frac{p-1}{2}}).$$

Essa relação, por sua vez, pode ser escrita como

$$\frac{p^2-1}{8}a = pt + S_X + S_Y, \tag{2.4}$$

em que S_X e S_Y denotam as somas dos elementos dos conjuntos X e Y definidos na prova do Lema de Gauss.

Por outro lado, $\{p-x_1, p-x_2, \ldots, p-x_m, y_1, y_2, \ldots, y_n\} = \{1, 2, \ldots, \frac{p-1}{2}\}$, o que resulta (também somando elementos) na igualdade

$$\frac{p^2-1}{8} = pm - S_X + S_Y. \tag{2.5}$$

Agora, subtraindo, membro a membro, as igualdades (2.5) e (2.4), obtemos

$$\frac{p^2-1}{8}(a-1) = p(t-m) + 2S_X. \tag{2.6}$$

Por fim, como p é ímpar e $(a-1)$ é par (pois a é ímpar, por hipótese), a igualdade (2.6) garante que t e m têm a mesma paridade. Logo, do lema de Gauss, alcança-se imediatamente o resultado esperado.

□

Corolário 2.3.3 *Se p é um primo ímpar, então*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, \textit{ se } p \equiv 1 \textit{ ou } p \equiv 7 \ (\textit{mod } 8) \\ -1, \textit{ se } p \equiv 3 \textit{ ou } p \equiv 5 \ (\textit{mod } 8) \end{cases}.$$

Demonstração: a princípio, valendo-se da mesma notação empregada nas provas do lema de Gauss e da proposição 2.3.7, temos que

$$t = \left\lfloor \frac{2}{p} \right\rfloor + \left\lfloor \frac{2\cdot 2}{p} \right\rfloor + \cdots + \left\lfloor \frac{\frac{p-1}{2}\cdot 2}{p} \right\rfloor = 0,$$

visto que $\left\lfloor \frac{k\cdot 2}{p} \right\rfloor = 0$, para todo $1 \leqslant k \leqslant \frac{p-1}{2}$.

Vejamos, ainda, que, na prova deste corolário, podemos seguir a mesma sequência de resultados inferidos na demonstração da proposição 2.3.7 até a equação (2.6), que pode ser reescrita, para $a = 2$ e $t = 0$, como

$$\frac{p^2-1}{8} = -pm + 2S_X.$$

Finalmente, decorre da igualdade acima e do fato de p ser um primo ímpar que m e $\frac{p^2-1}{8}$ têm a mesma paridade. Daí, o lema de Gauss dá o resultado almejado.

□

Vamos, agora, provar o resultado central desta seção (a lei da reciprocidade quadrática de Gauss), que relaciona, de maneira simples, os símbolos de Legendre $\left(\frac{p}{q}\right)$ e $\left(\frac{q}{p}\right)$, em que p e q são primos ímpares distintos. A prova que apresentaremos desse teorema é devida ao matemático alemão do século XIX Ferdinand Gotthold Max Eisenstein.

Teorema 2.3.8 (Gauss) *Se p e q são primos ímpares distintos, então*

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

Demonstração: pela proposição 2.3.7, temos que

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{t}(-1)^{t'},$$

em que

$$t = \left\lfloor \frac{p}{q} \right\rfloor + \left\lfloor \frac{2p}{q} \right\rfloor + \cdots + \left\lfloor \frac{\frac{q-1}{2}p}{q} \right\rfloor \text{ e } t' = \left\lfloor \frac{q}{p} \right\rfloor + \left\lfloor \frac{2q}{p} \right\rfloor + \cdots + \left\lfloor \frac{\frac{p-1}{2}q}{p} \right\rfloor.$$

Assim, para provarmos o teorema, basta mostrarmos que

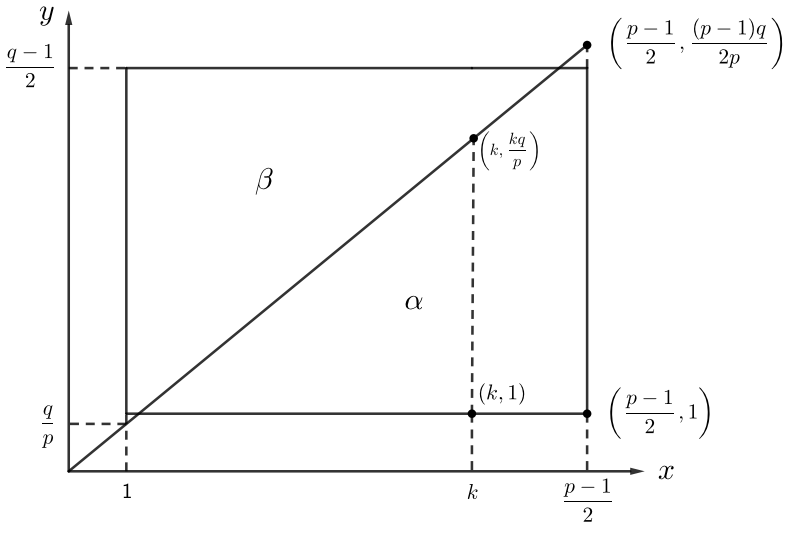
$$\left\lfloor \frac{p}{q} \right\rfloor + \left\lfloor \frac{2p}{q} \right\rfloor + \cdots + \left\lfloor \frac{\frac{q-1}{2}p}{q} \right\rfloor + \left\lfloor \frac{q}{p} \right\rfloor + \left\lfloor \frac{2q}{p} \right\rfloor + \cdots + \left\lfloor \frac{\frac{p-1}{2}q}{p} \right\rfloor = \frac{p-1}{2}\cdot\frac{q-1}{2}. \tag{2.7}$$

Para tanto, recorreremos a uma interpretação geométrica, contabilizando o número de pontos de coordenadas naturais no retângulo fechado

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

Inicialmente, notemos que tal número de pontos é $\frac{p-1}{2}\cdot\frac{q-1}{2}$. Vejamos, então, como contar o número de tais pontos de modo a obtermos a expressão do primeiro membro de (2.7) como resposta.

Podemos supor, sem perda de generalidade, que $p > q$. Além disso, consideremos a reta $y = \frac{q}{p}x$, conforme a figura abaixo, da região R.



Como $k\frac{q}{p} \notin \mathbb{N}$, para todo $1 \leqslant k \leqslant \frac{p-1}{2}$, temos que $\left\lfloor \frac{kq}{p} \right\rfloor$ conta o número de pontos de coordenadas naturais sobre a reta $x = k$, acima da reta $y = 0$ e abaixo da reta $y = \frac{q}{p}x$. Para garantir que todos esses pontos pertecem à região R, basta observarmos que

$$\left\lfloor \frac{kp}{q} \right\rfloor \leqslant \left\lfloor \frac{(p-1)q}{2p} \right\rfloor = \left\lfloor \frac{q}{2} - \frac{q}{2p} \right\rfloor \leqslant \left\lfloor \frac{q}{2} \right\rfloor = \frac{q-1}{2}.$$

Portanto, o número de pontos de coordenadas naturais na região α de R é

$$\left\lfloor \frac{q}{p} \right\rfloor + \left\lfloor \frac{2q}{p} \right\rfloor + \cdots + \left\lfloor \frac{\frac{p-1}{2}q}{p} \right\rfloor.$$

Analogamente, o número de pontos de coordenadas naturais na região β de R é

$$\left\lfloor \frac{p}{q} \right\rfloor + \left\lfloor \frac{2p}{q} \right\rfloor + \cdots + \left\lfloor \frac{\frac{q-1}{2}p}{q} \right\rfloor,$$

finalizando, assim, a demonstração deste sofisticado teorema.

□

3 TEORIA ELEMENTAR DE FORMAS QUADRÁTICAS BINÁRIAS

Neste capítulo, estudaremos as formas quadráticas binárias, isto é, expressões do tipo $ax^2+bxy+cy^2$, com a,b,c números inteiros dados, nem todos 0, e x,y, variáveis. O problema a ser averiguado é o da determinação dos inteiros n para os quais existam inteiros x e y tais que $n=ax^2+bxy+cy^2$. No final do capítulo, daremos uma resposta a essa indagação por meio de um critério vantajoso, estabelecendo uma relação com resíduos quadráticos, a partir do qual podemos determinar se um inteiro n é ou não representável por alguma forma quadrática binária, dado seu discriminante (que definiremos na seção a seguir).

A partir daqui, a palavra forma significará forma quadrática binária, salvo menção explícita em contrário.

3.1 Definições e notações

O problema referido na parte introdutória do capítulo não é fácil de ser estudado, mas é melhor respondido dividindo, por meio de uma relação de equivalência apropriada, o conjunto de todas as formas de um dado tipo em classes e encontrando uma forma de representação a mais simples possível para cada uma dessas classes. Desenvolveremos este traballho em termos de matrizes de tipo 2×2.

Por praticidade, a forma $ax^2+bxy+cy^2$ será indicada por $[a,b,c]$. Se σ é o máximo divisor comum (a,b,c) dos coeficientes a,b,c, então σ é denominado o **divisor** da forma $[a,b,c]$. Se $\sigma=1$, então a forma é denominada **primitiva**.

Se $n=ax^2+bxy+cy^2$, com $x,y\in\mathbb{Z}$, então o par de inteiros x,y é denominado uma **representação** de n pela forma $[a,b,c]$, e n é dito **representável** pela forma. O inteiro $\tau=(x,y)$ é denominado o **divisor da representação**. Se $\tau=1$, então a representação será denominada **primitiva**. Desse modo, basta considerarmos representações primitivas, uma vez que se o par de inteiros x,y é uma representação do inteiro n pela forma $[a,b,c]$ e $\tau=(x,y)$, então o par de inteiros $\frac{x}{\tau}$, $\frac{y}{\tau}$ é uma representação primitiva do inteiro $\frac{n}{\tau^2}$ pela mesma forma.

O inteiro b^2-4ac é denominado o **discriminante** da forma $[a,b,c]$ e será designado por Δ. A partir da definição, segue claramente que

$$\Delta\equiv\begin{cases}0\pmod 4, \text{ se } b \text{ for par}\\ 1\pmod 4, \text{ se } b \text{ for ímpar}\end{cases}. \tag{3.1}$$

Notemos que o comportamento da forma depende do valor de Δ. Isso pode ser

percebido através da seguinte identidade.

$$4a(ax^2+bxy+cy^2) = (2ax+by)^2 - \Delta y^2. \tag{3.2}$$

Inicialmente, suponhamos que $\Delta = 0$. Desse modo, temos dois casos a considerar:

i) Se $a = 0$, então $b = 0$ e, assim, a forma é cy^2.

ii) Se $a \neq 0$, então, de (3.2), podemos mostrar que a forma é $q(a_1x+c_1y)^2$, em que $q = (a,c)$, $a = qa_1^2$, $c = qc_1^2$ e $b^2 = 4(qa_1c_1)^2$.

Em ambos os casos, o problema de saber se um inteiro n pode ser representado ou não pela forma é respondido facilmente, razão pela qual omitiremos esse caso a partir de agora.

Suponhamos, agora, que $\Delta < 0$. A partir de $\Delta = b^2 - 4ac$, temos $ac > 0$, ou seja, a e c são ambos positivos ou ambos negativos. Se $a > 0$, a identidade (3.2) nos diz que a forma $[a,b,c]$ pode representar somente 0 ou inteiros positivos, representando 0 se, e somente se, $x = y = 0$. Analogamente, se $a < 0$, a forma $[a,b,c]$ pode representar somente 0 ou inteiros negativos, representando 0 se, e somente se, $x = y = 0$.

A forma $[a,b,c]$ é denominada **positiva definida**, se $\Delta < 0$ e $a > 0$. Se $\Delta < 0$ e $a < 0$, então a forma é denominada **negativa definida**. Como a forma $[a,b,c]$ é negativa definida se, e somente se, a forma $[-a,-b,-c]$ é positiva definida, as propriedades das formas negativas definidas podem ser deduzidas a partir daquelas das formas positivas definidas.

Por fim, suponhamos que $\Delta > 0$. Se $a = 0$, então $b \neq 0$ e, portanto, a forma é $y(bx+cy)$. Tomando $y = 1$, podemos claramente escolher x para mostrar que a forma pode assumir valores positivos ou negativos. Se $a \neq 0$, então, para $x = 1$ e $y = 0$, a forma assume o valor a, e, para $x = b$ e $y = -2a$, a forma assume o valor $-a\Delta$, mostrando que a forma pode, novamente, assumir valores positivos ou negativos. Sendo assim, uma forma com $\Delta > 0$ é chamada **indefinida**.

Observemos que, se Δ se escreve como o quadrado de um inteiro, a forma pode ser fatorada em um produto de dois fatores lineares com coeficientes inteiros. Esse caso será omitido no decorrer do capítulo, uma vez que o problema de representação de inteiros também pode ser tratado, nesse caso, por métodos elementares. Assim, doravante, assumiremos que $a \neq 0$ e $b \neq 0$.

3.2 Matrizes e transformações unimodulares

O método padrão no estudo inicial de formas quadráticas envolve o uso de homogeneização linear de variáveis, ou seja, transformações lineares. No caso de duas variáveis, tal

mudança de variáveis de x, y para x', y' é, como sabemos, da forma

$$\begin{array}{rcl} x &=& \alpha x' + \beta y' \\ y &=& \gamma x' + \delta y' \end{array}, \tag{3.3}$$

em que α, β, γ e δ pertencem domínio em que os coeficientes das formas quadráticas se encontram e $\alpha\delta - \beta\gamma \neq 0$.

Em nosso contexto, os coeficientes a,b,c nas formas $[a,b,c]$ são inteiros. Assim, consideraremos a transformação (3.3) tal que α, β, γ e δ são inteiros.

Resolvendo as relações (3.3), para x',y', obtemos as seguintes igualdades:

$$\begin{array}{rcl} x' &=& \frac{\delta}{d}x - \frac{\beta}{d}y \\ y' &=& -\frac{\gamma}{d}x + \frac{\alpha}{d}y \end{array}, \tag{3.4}$$

em que $d = \alpha\delta - \beta\gamma$.

Os sistemas (3.3) e (3.4) podem ser escritos, respectivamente, na forma matricial da seguinte maneira:

$$X = TY \text{ e } Y = T^{-1}X,$$

em que $X = \begin{bmatrix} x \\ y \end{bmatrix}$, $Y = \begin{bmatrix} x' \\ y' \end{bmatrix}$, $T = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$ e T^{-1} é a inversa de T.

Além disso, $d = |T|$ é o determinante de T. Sabendo-se que $|T^{-1}| = \frac{1}{d}$, é fácil verificar que as equações (3.4) também têm coeficientes inteiros se, e somente se, $\frac{1}{d}$ é um inteiro, o que ocorre se, e somente se, $d = |T| = \pm 1$. De fato, se $d = \pm 1$, então os coeficientes são inteiros; reciprocamente, para que as relações (3.4) tenham coeficientes inteiros, deve-se ter $\frac{\alpha}{d}, \frac{\beta}{d}, \frac{\gamma}{d}, \frac{\delta}{d} \in \mathbb{Z}$. Então, também deve ser inteiro o número

$$\frac{\alpha}{d}\cdot\frac{\delta}{d} - \frac{\beta}{d}\cdot\frac{\gamma}{d} = \frac{\alpha\delta - \beta\gamma}{d^2} = \frac{d}{d^2} = \frac{1}{d},$$

de sorte que $d \mid 1$. Visando uma maior facilitação, vamos considerar apenas o caso $d = |T| = 1$.

Se $d = |T| = 1$, então a matriz T é denominada uma **matriz unimodular inteira**, e a transformação associada $X = TY$ é denominada uma **transformação unimodular inteira**.

Teorema 3.2.1 *Seja G o conjunto de todas as matrizes unimodulares inteiras 2×2. Então, G é um grupo não abeliano com a operação de multiplicação usual de matrizes, denominado o* ***grupo unimodular inteiro***.

Demonstração: G é um conjunto não vazio, pois $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in G$.

Agora, afirmamos que a multiplicação é uma operação binária sobre G. Com efeito, se $T_1, T_2 \in G$, então T_1T_2 tem entradas inteiras e, pelo Teorema de Binet, $|T_1||T_2| = |T_1||T_2| = 1$. Logo, $T_1T_2 \in G$.

Notemos que, para quaisquer matrizes A, B, C de tipo 2×2, tem-se

$$(AB)C = A(BC).$$

Em particular, se $T_1, T_2, T_3 \in G$, então $(T_1T_2)T_3 = T_1(T_2T_3)$. Desse modo, a operação de G é associativa.

Além disso, a matriz I é tal que $TI = IT = T$, para toda $T \in G$; portando, I é o elemento identidade de G.

Agora, pelo que foi discutido no começo da seção, se $T \in G$, então T é invertível e sua inversa T^{-1} também está em G. Portanto, G é um grupo com a operação multiplicação usual de matrizes.

Por fim, tomando as matrizes

$$P = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \text{ e } Q = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix},$$

que estão em G, podemos verificar que

$$PQ = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \text{ e } QP = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix},$$

mostrando que o grupo G não é abeliano.

□

3.3 Classes de equivalência de formas quadráticas binárias

Diremos que a forma $ax^2 + bxy + cy^2$ é **equivalente** à forma $a'(x')^2 + b'x'y' + c'(y')^2$ e escrevemos

$$[a,b,c] \sim [a',b',c']$$

se existir uma transformação unimodular inteira

$$X = TY, \tag{3.5}$$

tal que

$$ax^2+bxy+cy^2=a'(x')^2+b'x'y'+c'(y')^2.$$

Percebamos que as formas quadráticas podem ser escritas na forma matricial como segue:

$$ax^2+bxy+cy^2=X^\top AX \text{ e } a'(x')^2+b'x'y'+c'(y')^2=Y^\top BY,$$

em que

$$A=\begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{bmatrix},\ B=\begin{bmatrix} a' & \frac{b'}{2} \\ \frac{b'}{2} & c' \end{bmatrix},\ X=\begin{bmatrix} x \\ y \end{bmatrix},\ Y=\begin{bmatrix} x' \\ y' \end{bmatrix},$$

e $X^\top$, $Y^\top$ denotam as transpostas de X, Y, respectivamente.

Assim, $[a,b,c]\sim[a',b',c']$ se, e somente se, existe uma matriz unimodular T tal que

$$(TY)^\top A(TY)=Y^\top BY,$$

ou, equivalentemente,

$$Y^\top(T^\top AT)Y=Y^\top BY.$$

Como consequência, temos que

$$T^\top AT=B, \tag{3.6}$$

em que $T^\top$ é a transposta de T. Se $T=\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$, então $T^\top=\begin{bmatrix} \alpha & \gamma \\ \beta & \delta \end{bmatrix}$, e $|T^\top|=\alpha\delta-\beta\gamma=1$. Portanto, $(T^\top)^{-1}$ (que é igual a $(T^{-1})^\top$) também pertence a G.

Reciprocamente, se existe $T\in G$ para a qual (3.6) vale, podemos facilmente reverter os passos acima para concluir que vale (3.5).

Agora, provemos que se S é o conjunto de todas as formas quadráticas binárias inteiras, então a relação $\sim$ que acabamos de definir é uma relação de equivalência em S. Temos que provar as três afirmações abaixo:

1. $[a,b,c]\sim[a,b,c]$.
2. $[a,b,c]\sim[a',b',c']$ implica $[a',b',c']\sim[a,b,c]$.
3. $[a,b,c]\sim[a',b',c']$ e $[a',b',c']\sim[a'',b'',c'']$ implica $[a,b,c]\sim[a'',b'',c'']$.

Demonstração: sejam

$$A = \begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{bmatrix}, B = \begin{bmatrix} a' & \frac{b'}{2} \\ \frac{b'}{2} & c' \end{bmatrix}, C = \begin{bmatrix} a'' & \frac{b''}{2} \\ \frac{b''}{2} & c'' \end{bmatrix},$$

1. Sendo $I^\top AI = A$, o resultado segue a partir de (3.6), com $B = A$ e $T = I$.
2. Se $[a,b,c] \sim [a',b',c']$, então existe uma matriz T em G tal que $T^\top AT = B$. Portanto, $A = (T^{-1})^\top BT^{-1} = (T^{-1})^\top BT^{-1}$. Como já observamos, $T^{-1} \in G$; consequentemente, $[a',b',c'] \sim [a,b,c]$.
3. Nesse caso, existem matrizes T_1 e T_2 em G tais que $T_1^\top AT_1 = B$ e $T_2^\top BT_2 = C$. Então, $T_2^\top (T_1^\top AT_1)T_2 = C$ e, assim, $(T_1T_2)^\top A(T_1T_2) = C$. Como T_1T_2 pertence a G, segue que $[a,b,c] \sim [a'',b'',c'']$.

□

De (3.6), segue que a classe de equivalência determinada pela forma $[a,b,c]$ consiste de todas as formas com matrizes $T^\top AT$, em que T varia no grupo G e $A = \begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{bmatrix}$. Desse modo, se

$$T = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \text{ e } T^\top AT = \begin{bmatrix} a' & \frac{b'}{2} \\ \frac{b'}{2} & c' \end{bmatrix},$$

então

$$\begin{aligned} \begin{bmatrix} a' & \frac{b'}{2} \\ \frac{b'}{2} & c' \end{bmatrix} &= \begin{bmatrix} \alpha & \gamma \\ \beta & \delta \end{bmatrix} \begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{bmatrix} \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \\ &= \begin{bmatrix} \alpha & \gamma \\ \beta & \delta \end{bmatrix} \begin{bmatrix} a\alpha + \frac{b\gamma}{2} & a\beta + \frac{b\delta}{2} \\ \frac{b\alpha}{2} + c\gamma & \frac{b\beta}{2} + c\delta \end{bmatrix} \\ &= \begin{bmatrix} a\alpha^2 + b\alpha\gamma + c\gamma^2 & a\alpha\beta + \frac{b(\alpha\delta+\beta\gamma)}{2} + c\gamma\delta \\ a\alpha\beta + \frac{b(\alpha\delta+\beta\gamma)}{2} + c\gamma\delta & a\beta^2 + b\beta\delta + c\delta^2 \end{bmatrix}, \end{aligned}$$

e, consequentemente,

$$\begin{aligned} a' &= a\alpha^2 + b\alpha\gamma + c\gamma^2, \\ b' &= 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta, \\ c' &= a\beta^2 + b\beta\delta + c\delta^2. \end{aligned} \tag{3.7}$$

O teorema a seguir mostra que as formas em uma dada classe de equivalência têm certas propriedades em comum.

Teorema 3.3.1 *Formas equivalentes:*

(a) Têm o mesmo divisor e discriminante,

(b) Representam os mesmos inteiros.

Além das propriedades acima, representações equivalentes de um inteiro n, ou seja, representações relacionadas por uma transformação unimodular inteira, têm o mesmo divisor.

Demonstração: inicialmente, consideremos as formas equivalentes $[a,b,c]$ e $[a',b',c']$. Assim, existe uma tranformação unimodular inteira $T = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$ tal que

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} x' \\ y' \end{bmatrix}, \text{ ou seja, } X = TY,$$

de modo que

$$ax^2 + bxy + cy^2 = a'(x')^2 + b'x'y' + c'(y')^2.$$

(a) De (3.7), os coeficientes a',b',c' são combinações lineares dos coeficientes a,b,c. Consequentemente, $(a,b,c) \mid a',b',c'$, e, portanto, $(a,b,c) \mid (a',b',c')$. Por simetria, $(a',b',c') \mid (a,b,c)$. Então, as formas têm o mesmo divisor.

Além disso, calculando determinantes na identidade

$$\begin{bmatrix} a' & \frac{b'}{2} \\ \frac{b'}{2} & c' \end{bmatrix} = T^\top \begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{bmatrix} T,$$

obtemos

$$a'c' - \frac{b'^2}{4} = |T^\top| \left(ac - \frac{b^2}{4} \right) |T| = ac - \frac{b^2}{4},$$

o que mostra que

$$b'^2 - 4a'c' = b^2 - 4ac.$$

Portando, as formas têm o mesmo discriminante.

(b) Suponhamos que

$$n = a'(x_1')^2 + b'x_1'y_1' + c'(y_1')^2,$$

em que x_1', y_1' são inteiros. Assim, se

$$\begin{bmatrix} x_1 \\ y_1 \end{bmatrix} = T \begin{bmatrix} x_1' \\ y_1' \end{bmatrix}, \tag{3.8}$$

então x_1, y_1 são inteiros e $n = ax_1^2 + bx_1y_1 + cy_1^2$. Logo, se n é representado pela forma $[a', b', c']$, ele também é representado pela forma $[a, b, c]$.

Como T^{-1} também é uma matriz unimodular inteira, o contrário é verdade por simetria. Daí, formas equivalentes representam os mesmos inteiros.

Nas notações da discussão acima, suponhamos que

$$n = ax_1^2 + bx_1y_1 + cy_1^2 = a'(x_1')^2 + b'x_1'y_1' + c'(y_1')^2,$$

com x_1, y_1, x_1', y_1' como em (3.8), com $T = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$. Então,

$$\begin{bmatrix} x_1 \\ y_1 \end{bmatrix} = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} x_1' \\ y_1' \end{bmatrix} = \begin{bmatrix} \alpha x_1' + \beta y_1' \\ \gamma x_1' + \delta y_1' \end{bmatrix}.$$

Como $x_1 = \alpha x_1' + \beta y_1'$ e $y_1 = \gamma x_1' + \delta y_1'$, segue que $(x_1', y_1') \mid x_1, y_1$; consequentemente, $(x_1', y_1') \mid (x_1, y_1)$. De modo análogo, como $T^{-1} \in G$, temos $(x_1, y_1) \mid (x_1', y_1')$. Portanto, $(x_1, y_1) = (x_1', y_1')$.

□

Observações:

i) A partir dos itens (a) e (b) do teorema, segue que as formas em uma determinada classe de equivalência são todas positivas definidas, todas negativas definidas ou todas indefinidas.

ii) Em particular, também do teorema, se um inteiro é primitivamente representável por uma dada forma, então o mesmo é primitivamente representável por qualquer forma equivalente. De fato, nas notações da prova, temos que $(x_1, y_1) = 1$ implica $(x_1', y_1') = 1$.

iii) Apesar de formas equivalentes terem o mesmo discriminante, o contrário não é verdade, ou seja, formas com um mesmo discriminante podem não ser equivalentes. Por exemplo, as formas $x^2 + 6y^2$ (isto é, $[1,0,6]$) e $2x^2 + 3y^2$ (isto é, $[2,0,3]$) têm discriminante -24, mas não são equivalentes, uma vez que, claramente, $x^2 + 6y^2$ representa o inteiro 1 mas $2x^2 + 3y^2$ não.

3.4 Formas quadráticas binárias de discriminante Δ dado

Nesta seção, será mostrado que, fixado o discriminante Δ, existe apenas um número finito de classes de equivalência de formas com discriminante Δ. Também, no caso de formas positivas definidas, será dado um método para a obtenção de formas representantes de cada uma dessas classes.

Em primeiro lugar, notemos que há sempre uma forma de um caractere bastante simples de discriminante Δ. Ela é denominada a **forma principal** de discriminante Δ e é definida como a forma

$$[1, k, \frac{k^2 - \Delta}{4}],$$

em que, $k = 0$ se $\Delta \equiv 0 \pmod 4$, e $k = 1$ se $\Delta \equiv 1 \pmod 4$. A forma é claramente inteira e tem discriminante $k^2 - (k^2 - \Delta) = \Delta$. Além disso, essa forma é primitiva e positiva definida quando $\Delta < 0$.

Por exemplo, a forma principal de discriminante -4 é $[1,0,1]$ (isto é, a forma $x^2 + y^2$) e a forma principal de discriminante 5 é $[1,1,-1]$ (isto é, a forma $x^2 + xy - y^2$).

A classe de equivalência de discriminante Δ correspondente à forma principal é denominada a **classe principal da forma de discriminante** Δ.

Uma forma quadrática binária $[a,b,c]$ será denominada uma **forma reduzida** se ela satisfizer

$$\begin{cases} -|a| < b \leqslant |a| < |c| \\ \qquad \text{ou} \qquad \\ 0 \leqslant b \leqslant |a| = |c| \end{cases}. \tag{3.9}$$

Uma forma reduzida sempre satisfaz a condição

$$b^2 \leqslant |ac| \leqslant \frac{|\Delta|}{3}, \tag{3.10}$$

em que Δ é o discriminante da forma. De fato, de (3.9), é claro que $b^2 \leqslant |ac|$. Além disso, pela desigualdade triangular, temos

$$|\Delta| = |4ac - b^2| \geqslant 4|ac| - b^2.$$

Consequentemente,

$$|\Delta| \geqslant 4b^2 - b^2 = 3b^2,$$

que dá o resultado desejado.

A forma principal de discriminante Δ é uma forma reduzida. Realmente, se $\Delta = 4N$, a forma é $[1,0,-N]$, e, se $\Delta = 4N+1$, a forma é $[1,1,-N]$, e, como $|N| \geqslant 1$ (veja a observação a seguir), cada uma dessas formas satisfaz claramente a condição (3.9).

Observação: notemos que $|N| \geqslant 1$ na discussão do parágrafo anterior, uma vez que as formas dos tipos acima e de discriminantes 0 ou 1 estão dentre as formas especiais omitidas no início da discussão.

No teorema a seguir, as propriedades das formas reduzidas são usadas para provar o principal resultado desta seção, devido a J. L. Lagrange.

Teorema 3.4.1 *Em relação às formas quadráticas binárias, temos que:*

(a) Cada classe de equivalência contém pelo menos uma forma reduzida.

(b) O número de classes de equivalência de formas com um discriminante Δ dado é finito.

Demonstração:

(a) Seja C uma classe de equivalência de formas e $[a_0,b_0,a_1]$ uma forma qualquer em C (a notação aparentemente estranha encontrará justificativa logo mais).

Se $[a_0,b_0,a_1]$ é uma forma reduzida, não há nada para provar. Consequentemente, podemos supor que $[a_0,b_0,a_1]$ não é uma forma reduzida. Seja T_1 a matriz unimodular inteira

$$\begin{bmatrix} 0 & 1 \\ -1 & \delta_1 \end{bmatrix},$$

na qual o inteiro δ_1 será escolhido depois. Aplicando a transformação $X = T_1 Y$ à forma $[a_0, b_0, a_1]$, obtemos, por (3.7), a forma equivalente

$$[a_1, -b_0 - 2a_1\delta_1, a_0 + b_0\delta_1 + a_1\delta_1^2] \,. \tag{3.11}$$

Na divisão do inteiro $-b_0$ por $2|a_1|$, existem inteiros q e r satisfazendo as condições

$$-b_0 = 2|a_1|q + r \;\text{ e }\; -|a_1| < r \leqslant |a_1|. \tag{3.12}$$

Então,

$$-b_0 - 2a_1\delta_1 = 2\left(\frac{|a_1|}{a_1}q - \delta_1\right)a_1 + r.$$

Se tomarmos $\delta_1 = \frac{|a_1|}{a_1}q$, então $-b_0 - 2a_1\delta_1 = r$ e, daí,

$$[a_0, b_0, a_1] \sim [a_1, b_1, a_2], \text{ com } -|a_1| < b_1 \leqslant |a_1|.$$

Aplicando o mesmo procedimento para a forma $[a_1, b_1, a_2]$, obtemos um resultado similar, a saber:

$$[a_1, b_1, a_2] \sim [a_2, b_2, a_3], \text{ com } -|a_2| < b_2 \leqslant |a_2|.$$

Procedendo deste modo, obtém-se uma cadeia de formas equivalentes, satisfazendo o seguinte esquema:

$$\begin{gathered}
[a_0, b_0, a_1] \sim [a_1, b_1, a_2], \text{ com } -|a_1| < b_1 \leqslant |a_1|, \\
[a_1, b_1, a_2] \sim [a_2, b_2, a_3], \text{ com } -|a_2| < b_2 \leqslant |a_2|, \\
\cdots \\
[a_{n-1}, b_{n-1}, a_n] \sim [a_n, b_n, a_{n+1}], \text{ com } -|a_n| < b_n \leqslant |a_n|, \\
\cdots
\end{gathered}$$

Suponhamos que $|a_n| > |a_{n+1}|$, para todo $n \geqslant 1$. Então, teríamos uma sequência decrescente infinita

$$|a_1| > |a_2| > |a_3| > \cdots$$

de inteiros não negativos, o que é impossível. Assim, para algum inteiro $n \geqslant 1$, temos $|a_n| \leqslant |a_{n+1}|$, de forma que

$$[a_0, b_0, a_1] \sim [a_n, b_n, a_{n+1}], \text{ com } -|a_n| < b_n \leqslant |a_n| \leqslant |a_{n+1}|.$$

Se $|a_n| < |a_{n+1}|$, a forma $[a_n, b_n, a_{n+1}]$ é reduzida, e nada mais há a fazer. Se $|a_n| = |a_{n+1}|$ e $b_n \geqslant 0$, novamente a forma é reduzida. Suponhamos, pois, que $|a_n| = |a_{n+1}|$ e $b_n < 0$. Então, aplicando a transformação unimodular com matriz $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ à forma $[a_n, b_n, a_{n+1}]$, obtemos a forma equivalente $[a_{n+1}, -b_n, a_n]$. Como $0 \leqslant -b_n \leqslant |a_n| = |a_{n+1}|$, esta última forma é reduzida e a primeira parte do teorema está provada.

(b) Para provar que o número de classes de equivalência de formas com discriminante Δ é finito, é claramente suficiente, pelo item (a), provar que o número de formas reduzidas de discriminante Δ é finito.

Dado Δ, existe apenas um número finito de inteiros a, b e c satisfazendo as condições (3.10). De fato, (3.9) implica $a, c \neq 0$, logo, $|a|, |c| \geqslant 1$; portanto, (3.10) implica

$$|b| \leqslant \sqrt{\frac{|\Delta|}{3}},\ |a| \leqslant \frac{|\Delta|}{3} \text{ e } |c| \leqslant \frac{|\Delta|}{3}.$$

Assim, existe apenas um número finito de formas $[a, b, c]$ satisfazendo (3.9). Já que as formas reduzidas estão dentre estas, o resultado segue.

□

O número de classes de equivalência de formas de discriminante Δ é chamado o **número de classe** do discriminante Δ.

Exemplo 1: Encontre as formas reduzidas de discriminante -15.

Solução: como $\Delta = -15$, temos que, de (3.10), $b^2 \leqslant 5$. Como $\Delta \equiv 1 \pmod 4$, temos b ímpar, logo, $|b| = 1$. Então, $\Delta = b^2 - 4ac$ implica $ac = 4$. Portanto, por (3.9), as possíveis escolhas para o par de inteiros (a, c) são $(1,4), (2,2), (-1,-4), (-2,-2)$. Finalmente, de novo usando (3.9) para a seleção do valor de b a partir dos possíveis valores ± 1, obtemos quatro formas reduzidas distintas de discriminante -15, que são $[1,1,4], [2,1,2], [-1,1-4], [-2,1,-2]$. As duas primeiras são positivas definidas, e as duas últimas, negativas definidas.

□

No caso das formas quadráticas binárias positivas definidas (e, também, das formas negativas definidas), o item (a) do Teorema 3.4.1 pode ser melhorado para um resultado mais forte, que diz que toda classe de equivalência de tais formas contém exatamente uma forma reduzida.

No caso de formas indefinidas, a situação não é simples e será omitida. De fato, a definição dada nesse caso não é inteiramente satisfatória para trabalhos futuros sobre esse

assunto.

Teorema 3.4.2 *Toda classe de equivalência de formas quadráticas binárias e positivas definidas contém exatamente uma forma reduzida.*

Demonstração: suponhamos que $[a,b,c]$ e $[a',b',c']$ sejam formas quadráticas binárias positivas definidas e reduzidas. Queremos mostrar que $a=a', b=b'$ e $c=c'$.

Da condição (3.9), juntamente com o fato das formas serem positivas definidas, temos que

$$-a < b \leqslant a < c \text{ ou } 0 \leqslant b \leqslant a = c \tag{3.13}$$

e

$$-a' < b' \leqslant a' < c' \text{ ou } 0 \leqslant b' \leqslant a' = c'. \tag{3.14}$$

Primeiro, mostraremos que os três menores números representados primitivamente por uma forma positiva definida e reduzida $[a,b,c]$ são a,c e $a+c-|b|$. Estes inteiros podem, claro, não serem distintos.

Se $f(x,y)$ denota $ax^2+bxy+cy^2$, então

$$f(x,y) = a\left(x+\frac{b}{2a}y\right)^2 + \frac{4ac-b^2}{4a}y^2.$$

Usando (3.10), deduzimos que, se $|y| \geqslant 2$, então

$$f(x,y) \geqslant \frac{3ac}{4a}4 = 3c > a+c,$$

em que utilizamos (3.13) na última passagem.

Para $y = \pm 1$, temos, em vista de (3.13), que

$$f(x,\pm 1) = ax^2 \pm bx + c \geqslant ax^2 - a|x| + c.$$

Consequentemente, se $|x| \geqslant 2$, então

$$f(x,\pm 1) \geqslant 2a + c \geqslant a + c.$$

Os únicos casos restantes são $y=0$ ou $|x| \leqslant 1$, $y = \pm 1$. Esses casos dão origem a exatamente quatro inteiros representados primitivamente pela forma, a saber: $a, c, a+b+c$ e $a-b+c$, dados pelos pares $(x,y) = (1,0),(0,1),(1,1)$ e $(1,-1)$, respectivamente. Uma vez

que todos esses números são menores ou iguais a $a+c$, segue que os três menores inteiros representados primitivamente pela forma são a, c e $a+c-|b|$. Eles satisfazem as inequações:

$$a \leqslant c \leqslant a+c-|b|.$$

Analogamente, os três menores inteiros representados primitivamente pela forma $[a',b',c']$ são a', c' e $a'+c'-|b'|$, satisfazendo as inequações:

$$a' \leqslant c' \leqslant a'+c'-|b'|.$$

Agora, se $\begin{bmatrix} x \\ y \end{bmatrix} = T \begin{bmatrix} x' \\ y' \end{bmatrix}$ é a transformação que conecta as duas formas equivalentes $[a,b,c]$ e $[a',b',c']$, então cada par de inteiros relativamente primos x, y dá origem a um único par de inteiros relativamente primos x', y', e vice-versa. Assim, como as duas formas representam os mesmos inteiros, temos $a' = a$, $c' = c$ e $|b'| = |b|$ (ou seja, $b' = \pm b$).

Quando $a = c$, as condições (3.13) e (3.14) implicam $b' = b$ e, portanto, $[a',b',c'] = [a,b,c]$.

Agora, temos finalmente a considerar o caso $c > a$. Se $b' = b$, o resultado segue. Supondo que $b' = -b$, temos $[a,b,c] \sim [a,-b,c]$; logo, existem inteiros α, β, γ e δ para os quais

$$\alpha\delta - \beta\gamma = 1, \tag{3.15}$$

e, de acordo com (3.7),

$$a = a\alpha^2 + b\alpha\gamma + c\gamma^2 \tag{3.16}$$

e

$$-b = 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta. \tag{3.17}$$

De (3.16), da inequação $c > a$ e do fato de que $\alpha^2 + \gamma^2 - 2|\alpha\gamma| \geqslant 0$, temos

$$a > a\alpha^2 - a|\alpha\gamma| + a\gamma^2 \geqslant 2a|\alpha\gamma| - a|\alpha\gamma| = a|\alpha\gamma|,$$

o que implica que $\alpha\gamma = 0$. Se $\alpha = 0$, então (3.15) dá $\gamma \neq 0$; logo, (3.16) mostra que $a \geqslant c$, um absurdo. Segue que $\gamma = 0$ e, de (3.15), $\alpha\delta = 1$. Inserindo esses valores em (3.17), obtemos a igualdade $|b| = a|\alpha\beta|$, que mostra que $b = 0$ ou $|b| \geqslant a$. Se $b = 0$, então $b' = -b = 0$ e as formas são idênticas. Se $|b| \geqslant a$, então (3.13) garante que $b = a$, logo, $[a',b',c'] = [a,-a,c]$; mas essa última forma não é reduzida, de sorte que a possibilidade $|b| \geqslant a$ não ocorre.

□

O teorema supracitado e o exemplo 1 desta seção mostram que existem exatamente duas classes de formas quadráticas binárias positivas definidas de discriminannte -15, as quais têm como representantes as formas reduzidas $[1,1,4]$ e $[2,1,2]$.

Para determinar se um inteiro n é representável por uma dada forma $[a,b,c]$ positiva definida e de discriminante -15, é suficiente considerar uma tal representação pelas formas $[1,1,4]$ ou $[2,1,2]$, já que qualquer outra forma positiva definida é equivalente a uma dessas.

Discutiremos o problema da representação na próxima seção.

3.5 Representação de inteiros por formas quadráticas binárias

Na seção 3.1, um inteiro n foi definido como primitivamente representável pela forma $[a,b,c]$, quando existem inteiros x,y, com $(x,y)=1$, tais que $n=ax^2+bxy+cy^2$, sendo o par de inteiros x,y denominado uma representação primitiva de n pela forma $[a,b,c]$. Nesta seção, obteremos condições para tal representação.

Teorema 3.5.1 *Um inteiro n é primitivamente representável por uma dada forma quadrática binária* $[a,b,c]$ *se, e somente se, existe uma forma* $[n,b',c']$ *equivalente a* $[a,b,c]$.

Demonstração: suponhamos que o par de inteiros α, γ seja uma representação primitiva de n pela forma $[a,b,c]$. Assim, $n=a\alpha^2+b\alpha\gamma+cy^2$ e $(\alpha,\gamma)=1$. Agora, como $(\alpha,\gamma)=1$, o Teorema de Bézout garante que existem inteiros β e δ tais que $\alpha\delta-\beta\gamma=1$. Desse modo, a transformação $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$ é inteira, unimodular e transforma $[a,b,c]$ em $[a',b',c']$, em que $a'=a\alpha^2+b\alpha\gamma+c\gamma^2$; portanto, $a'=n$.

Reciprocamente, suponhamos que $[a,b,c]\sim[n,b',c']$. Como o par de inteiros 1, 0 é uma representação primitiva de n pela forma $[n,b',c']$, temos, do Teorema 3.3.1, que n é primitivamente representável pela forma $[a,b,c]$.

□

Tomando $n=0$, podemos facilmente deduzir, a partir do teorema 3.5.1, que uma forma $[a,b,c]$ representa primitivamente zero se, e somente se, seu discriminante é o quadrado

de um número inteiro. Como temos excluído formas desse tipo, iremos supor, daqui pra frente, que $n \neq 0$.

A seguir, obteremos um critério útil para a representação de um inteiro n por uma forma de discriminante Δ dado.

Teorema 3.5.2 *Um dado inteiro n, diferente de zero, é primitivamente representável por alguma forma de um dado discriminante* Δ *se, e somente se,* Δ *é um resíduo quadrático de* $4|n|$*, isto é, a congruência algébrica a seguir possui alguma solução:*

$$x^2 \equiv \Delta \pmod{4|n|}. \tag{3.18}$$

Demonstração: suponhamos que n é primitivamente representável por uma forma de discriminante Δ. Então, pelo teorema 3.5.1, temos que n é primitivamente representável por uma forma $[n, b', c']$ de discriminante Δ. Como $\Delta = (b')^2 - 4nc'$, segue que $(b')^2 \equiv \Delta \pmod{4|n|}$. Portanto, a congruência (3.18) possui alguma solução.

Reciprocamente, suponhamos que (3.18) possua alguma solução. Então, existem inteiros b' e c' tais que $(b')^2 - 4nc' = \Delta$. Assim, a forma $[n, b', c']$ tem discriminante Δ e o par de inteiros 1, 0 é uma representação primitiva de n por esssa forma, completando, assim, a demonstração do teorema.

□

No caso das formas quadráticas binárias positivas definidas, desenvolvemos um método para atacar o problema de saber se uma dada forma $[a, b, c]$ de discriminante Δ representa primitivamente ou não um número inteiro dado n. Em primeiro lugar, temos de checar se a congruência algébrica (3.18) possui alguma solução ou não. Se existe uma solução, encontramos as formas reduzidas de discriminante Δ. Se pudermos determinar a única forma reduzida equivalente à forma $[a, b, c]$ e decidir se esta forma reduzida representa ou não n, o problema original é resolvido. Se o discriminante Δ tem número de classe 1 (ou seja, se existe apenas uma forma reduzida de discriminante Δ), a situação é particularmente simples e, portanto, a forma $[a, b, c]$ representa n se, e somente se, a congruência (3.18) possui alguma solução.

Exemplo 2: Decida se os inteiros 21 ou 24 são primitivamente representáveis pela forma $31x^2 - 27xy + 6y^2$?

Solução: a forma é positiva definida e de discriminante -15. Consequentemente, é equivalente a uma das duas formas positivas definidas reduzidas de discriminante -15, quais sejam, $[1, 1, 4]$

ou $[2,1,2]$. Para determinar a forma reduzida apropriada, podemos utilizar o processo envolvido na demonstração da primeira parte do Teorema 3.4.1, obtendo (com o auxílio de (3.11) e (3.12)) a cadeia de formas equivalentes

$$[31,-27,6] \sim [6,3,1] \sim [1,1,4].$$

Para $n = 21$, a congruência algébrica (3.18) torna-se, nesse caso:

$$x^2 \equiv -15 \pmod{84}. \tag{3.19}$$

Checando o conjunto completo de resíduos 0, ± 1, ± 2, $\pm 3 \pmod 7$, vemos que a congruência algébrica $x^2 \equiv -15 \pmod 7$ não possui solução. Portanto, (3.19) não tem solução, o que implica que 21 não é primitivamente representável por qualquer forma de discriminante -15 e, em particular, não é primitivamente representável pela forma $[31,-27,6]$.

Para $n = 24$, a congruência algébrica (3.18) torna-se

$$x^2 \equiv -15 \pmod{96}. \tag{3.20}$$

As congruências algébricas $x^2 \equiv -15 \pmod{32}$ e $x^2 \equiv -15 \pmod 3$ são ambas solúveis. Então, pelo Teorema Chinês dos Restos, (3.20) possui alguma solução e 24 é primitivamente representável pela forma dada.

Outra possibilidade é encontrar diretamente um par de inteiros x, y tais que

$$x^2 + xy + 4y^2 = 24.$$

Multiplicando essa igualdade por 4 e completando quadrados, obtemos

$$(2x+y)^2 + 15y^2 = 96,$$

o que implica

$$y^2 \leqslant \frac{96}{15} < 7;$$

consequentemente, $|y| \leqslant 2$. Tomando $y = 1$, temos que $(2x+y)^2 = 81$, que é satisfeito com $x = 4$.

Segue que 24 é primitivamente representável pela forma reduzida $[1,1,4]$ e, portanto, pela forma $[31,-27,6]$.

□

4 APLICAÇÕES

Neste capítulo, como aplicação da teoria desenvolvida até aqui, enunciaremos e demonstraremos dois resultados interessantes: o primeiro, atribuído a Fermat, nos fornece uma caracterização dos inteiros positivos que podem ser escritos como soma de dois quadrados; o segundo dá uma condição necessária e suficiente para que um número primo $p > 3$ seja representável por alguma forma quadrática binária de discriminante -24.

4.1 Representação de um inteiro como uma soma de dois quadrados

Para atingir o objetivo desta seção, precisamos da seguinte identidade auxiliar, comumente atribuída a Euler e denominada a **identidade de Euler**.

Lema 4.1.1 *Se m e n são números que podem ser escritos como soma de dois quadrados, então mn também pode ser escrito como soma de dois quadrados.*

Demonstração: supondo que $m = a^2 + b^2$ e $n = c^2 + d^2$, temos

$$\begin{aligned} mn &= (a^2+b^2)(c^2+d^2) \\ &= (ac)^2 + (ad)^2 + (bc)^2 + (bd)^2 + 2abcd - 2abcd \\ &= [(ac)^2 + 2abcd + (bd)^2] + [(bc)^2 - 2abcd + (ad)^2] \\ &= (ac+bd)^2 + (bc-ad)^2. \end{aligned}$$

□

Nesta seção, o problema a ser considerado consiste na representação de inteiros pela forma positiva definida $x^2 + y^2$, o qual pode ser respondido utilizando o método desenvolvido no capítulo anterior.

Primeiro, mostraremos que $x^2 + y^2$ é a única forma positiva definida reduzida de discriminante -4. De (3.1) e (3.10), uma tal forma reduzida $[a,b,c]$ satisfaz as condições $b^2 \leqslant \frac{4}{3}$ e $b \equiv 0 \pmod 2$; portanto, temos $b = 0$. Como $b^2 - 4ac = -4$, segue que $ac = 1$, o que implica $a = c = 1$. Assim, toda forma positiva definida de discriminante -4 é equivalente à forma $[1,0,1]$, ou seja, à forma $x^2 + y^2$.

Do Teorema 3.5.2, temos que um inteiro positivo n pode ser escrito da forma $x^2 + y^2$, em que $(x,y) = 1$, se, e somente se, a congruência algébrica $x^2 \equiv -4 \pmod{4n}$ possui alguma

solução, ou seja, se, e somente se, a congruência algébrica

$$x^2 \equiv -1 \pmod{n} \tag{4.1}$$

possui alguma solução. Em particular, um primo ímpar p pode ser escrito na forma x^2+y^2 se, e somente se, $\left(\frac{-1}{p}\right) = 1$, e, portanto, (pelo corolário 2.3.2) se, e somente se, $p \equiv 1 \pmod{4}$. O primo 2 também pode ser escrito nessa forma, a saber: $2 = 1^2 + 1^2$.

Agora, a partir desses resultados, podemos enunciar e provar o teorema central desta seção.

Teorema 4.1.1 (Fermat) *Um inteiro positivo n pode ser escrito da forma x^2+y^2 se, e somente se, cada fator primo de n da forma $4k+3$ ocorre na fatoração canônica de n elevado a expoente par.*

Demonstração: suponhamos que $n = x^2+y^2$, com $d = (x,y)$. Daí, podemos escrever $n = d^2(a^2+b^2)$, em que $(a,b) = 1$. Se escrevermos $n_1 = a^2+b^2$, então, por (4.1), a congruência algébrica $x^2 \equiv -1 \pmod{n_1}$ possui uma solução. Assim, -1 é um resíduo quadrático de cada fator primo de n_1 e, consequentemente, (novamente pelo corolário 2.3.2) tais primos são da forma $4k+1$ ou 2. Portanto, qualquer fator primo de n da forma $4k+3$ deve ocorrer em d^2, logo, ocorre elevado a um expoente par.

Reciprocamente, suponhamos que $n = d^2 n_1$, em que n_1 não contém primos da forma $4k+3$. Queremos mostrar que n_1 pode ser escrito da forma a^2+b^2, o que dará $n = (da)^2 + (db)^2$.

Se $n_1 = 1$, então $n_1 = 1^2 + 0^2$ e o resultado segue. Observemos que, para todo inteiro $m \geqslant 1$, se $n_1 = 2^m$ ou $n_1 = 2^{m+1}$, com m par, então $n_1 = (2^{\frac{m}{2}})^2 + 0^2$ ou $n_1 = (2^{\frac{m}{2}})^2 + (2^{\frac{m}{2}})^2$, respectivamente; assim, novamente o resultado segue.

Suponhamos, agora, que $n_1 = 2^m p_1 \dots p_s$, em que $m \geqslant 0$ e cada primo p_j, com $1 \leqslant j \leqslant s$, é da forma $4k+1$. Pela discussão introdutória, para algum par de inteiros a_j, b_j, temos $p_j = a_j^2 + b_j^2$, com $1 \leqslant j \leqslant s$, e, para algum par de inteiros u, v, temos $2^m = u^2 + v^2$.

Por fim, em vista do lema 4.1.1, o inteiro

$$n_1 = (u^2+v^2)\prod_{j=1}^{s}(a_j^2+b_j^2)$$

pode ser escrito da forma a^2+b^2, concluindo, assim, a demonstração do teorema.

□

Para o teorema supramencionado, há uma demonsttração mais elementar, que não necessita do desenvolvimento da teoria de formas quadráticas binárias, como veremos a seguir.

Iniciemos pelo caso particular dos números primos, respondido por Fermat, a partir do seguinte teorema.

Teorema 4.1.2 (Fermat) *Para um primo ímpar p, as seguintes condições são equivalentes:*

(a) $p \equiv 1 \ (mod\ 4)$.

(b) A congruência $x^2 \equiv -1 \ (mod\ p)$ *possui alguma solução.*

(c) p pode ser expresso como soma de dois quadrados.

Demosntração:

$(a) \Longrightarrow (b)$: como $p = 4k+1$, decorre, imediatamente, do corolário 2.3.2 que

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

logo, -1 é resíduo quadrático módulo p.

$(b) \Longrightarrow (c)$: seja m um inteiro tal que $m^2 \equiv -1 \pmod{p}$. Consideremos o conjunto

$$A = \{(x,y) \in \mathbb{Z}^2;\ 0 \leqslant x,y < \sqrt{p}\}.$$

Pelo princípio fundamental da contagem, esse conjunto possui $(\lfloor\sqrt{p}\rfloor + 1)^2$ elementos. Agora, como

$$(\lfloor\sqrt{p}\rfloor + 1)^2 > \sqrt{p}^2 = p$$

e há, no máximo, p inteiros não congruentes entre si, módulo p, então, pelo princípio da casa dos pombos, existem pares ordenados distintos $(x_1,y_1),(x_2,y_2) \in A$, tais que

$$mx_1 + y_1 \equiv mx_2 + y_2 \pmod{p},$$

e, daí,

$$m(x_1 - x_2) \equiv y_2 - y_1 \pmod{p}.$$

Pondo $a = |x_1 - x_2|$ e $b = |y_1 - y_2|$, segue que a e b não são ambos nulos e, consequentemente,

$$0 < a^2 + b^2 = |x_1 - x_2|^2 + |y_1 - y_2|^2 < \sqrt{p}^2 + \sqrt{p}^2 = 2p. \tag{4.2}$$

Como

$$a^2+b^2 = |x_1-x_2|^2+|y_1-y_2|^2 \equiv (x_1-x_2)^2+m^2(x_1-x_2)^2$$
$$= (m^2+1)(x_1-x_2)^2 \equiv 0 \pmod{p}$$

e, de (4.2), $0 < a^2+b^2 < 2p$, temos, como única possibilidade, que

$$a^2+b^2 = p.$$

$(c) \Longrightarrow (a)$: sendo $p = a^2+b^2$, com a e b inteiros, segue que a é par e b é ímpar ou vice-versa, uma vez que p é um primo ímpar. Supondo, sem perda de generalidade, que a é par (isto é, da forma $2k'$) e b é ímpar (isto é, da forma $2k''+1$), temos que

$$p = a^2+b^2 = (2k')^2+(2k''+1)^2 \equiv 0+1 \equiv 1 \pmod{p}.$$

□

A seguir, daremos uma demonstração, apoiada em noções mais básicas relativas à Teoria dos Números, do teorema de Fermat, o qual caracteriza os naturais que podem ser escritos como soma de dois quadrados.

Teorema 4.1.3 (Fermat) *Um natural n pode ser escrito como soma de dois quadrados se, e somente se, ele é da forma* $n = 2^m p_1^{\alpha_1} \dots p_s^{\alpha_s} q_1^{\beta_1} \dots q_t^{\beta_t}$, *com* $m, \alpha_j, \beta_i \geqslant 0$, β_i *par,* $p_j \equiv 1 \pmod{4}$ *e* $q_i \equiv 3 \pmod{4}$, *para todos* $1 \leqslant j \leqslant s$ *e* $1 \leqslant i \leqslant t$.

Demonstração: consideremos, inicialmente,

$$n = 2^m p_1^{\alpha_1} \dots p_s^{\alpha_s} q_1^{\beta_1} \dots q_t^{\beta_t},$$

com $m, \alpha_j, \beta_i \geqslant 0$, $p_j \equiv 1 \pmod 4$ e $q_i \equiv 3 \pmod 4$, para todos $1 \leqslant j \leqslant s$ e $1 \leqslant i \leqslant t$. Suponhamos que n pode ser escrito como soma de dois quadrados. Daí, para provarmos que β_i é par, é suficiente mostrarmos que se n pode ser escrito como soma de dois quadrados e $\beta_i \geqslant 1$, então $\beta_i \geqslant 2$ e $\frac{n}{q_i^2}$ também pode ser escrito como soma de dois quadrados. Para isso, se $n = a^2+b^2$, com $a, b \in \mathbb{Z}$, então $a^2+b^2 \equiv 0 \pmod{q_i}$. Agora, se $b \not\equiv 0 \pmod{q_i}$, então $(b, q_i) = 1$, de modo que b é invertível, módulo q_i; tomando e seu inverso, temos que

$$(ae)^2+1 \equiv -b^2e^2+1 \equiv -1+1 \equiv 0 \pmod{q_i},$$

o que contradiz o teorema 4.1.2, visto que $q_i \equiv 3 \pmod 4$. Logo, $b \equiv 0 \pmod{q_i}$ e, consequentemente, $a \equiv 0 \pmod{q_i}$. Portanto, $n = a^2 + b^2 \equiv 0 \pmod{q_i^2}$, de maneira que

$$\beta \geqslant 2 \text{ e } \frac{n}{q_i^2} = \left(\frac{a}{q_i}\right)^2 + \left(\frac{b}{q_i}\right)^2.$$

A demonstração da recíproca desse teorema é idêntica à prova da recíproca do teorema 4.1.1. Assim, finalizamos a demonstração do teorema.

□

O próximo resultado nos mostra que a escrita de um primo da forma $4k+1$ como soma de dois quadrados é essencialmente única.

Proposição 4.1.4 *Se p é um primo da forma $4k+1$, então existem únicos $x, y \in \mathbb{N}$ tais que $x < y$ e $p = x^2 + y^2$.*

Demonstração: o teorema 4.1.2 garante que existem naturais x, y tais que $p = x^2 + y^2$. Suponhamos, então, que exista outra escrita de p como soma de dois quadrados, a saber: $p = a^2 + b^2$, com $a, b \in \mathbb{N}$. Observemos, ainda, que x, y, a e b são todos primos com p e menores do que $\sqrt{p}$. Agora, escolhamos inteiros $1 \leqslant c, d < p$ tais que $xc \equiv y$ e $ad \equiv b \pmod p$.

Utilizando congruência módulo p, temos

$$x^2 + y^2 \equiv x^2 + (xc)^2 = x^2(c^2+1) \pmod p,$$

de sorte que $c^2 \equiv -1 \pmod p$. De modo análogo, $d^2 \equiv 0 \pmod p$. Assim, p divide $c^2 - d^2 = (c+d)(c-d)$, o que implica p divide $c+d$ ou $c-d$. Mas, como $1 \leqslant c, d < p$, temos que $-p < c-d < c+d < 2p$, mostrando que $c = d$ ou $c+d = p$.

Suponhamos, inicialmente, que $c = d$. As escolhas de c e d asseguram que

$$bxc \equiv ady \equiv ayc \pmod p \tag{4.3}$$

e, consequentemente, $bx \equiv ay \pmod p$, Mas, como $0 < x, y, a, b < \sqrt{p}$, segue que $0 < bx, ay < p$ e, daí, $bx = ay$. Logo,

$$p = x^2 + y^2 = \left(\frac{ay}{b}\right)^2 + y^2 = (a^2+b^2)\left(\frac{y}{b}\right)^2 = p\left(\frac{y}{b}\right)^2 \tag{4.4}$$

e, assim, $x = a$ e $y = b$.

Agora, se $c+d=p$, então, empregando o mesmo raciocínio de (4.3), obtemos $bx \equiv -ay \pmod{p}$, o que acarreta $bx+ay=p$. Portanto, tendo em vista o lema 4.1.1, segue que

$$p^2 = (x^2+y^2)(a^2+b^2) = (bx+ay)^2 + (by-ax)^2 = p^2 + (by-ax)^2,$$

o que ocasiona $by=ax$. Outra vez, como em (4.4), deduzimos que $x=b$ e $y=a$, concluindo, desse modo, a prova da proposição.

□

4.2 Representação de um primo $p>3$ por alguma forma quadrática binária de discriminante -24

O objetivo do que segue é obter uma descrição dos números primos $p>3$ que são representáveis por alguma forma de discriminante -24.

Para tanto, começaremos obtendo todas as formas positivas definidas reduzidas de discriminante -24, sendo qualquer forma de discriminante -24 equivalente a uma delas.

A partir de (3.10), como $\Delta=-24$, segue que $b^2 \leqslant 8$. Daí, visto que $\Delta \equiv 0 \pmod 4$, é imediato que $b=0$ ou $|b|=2$. Como $\Delta = b^2-4ac$, temos que $b=0$ implica $ac=6$ e $|b|=2$ implica $ac=7$. Logo, temos dois casos:

i) $b=0$: os pares de inteiros (a,c) que satisfazem (3.9) e a igualdade $ac=6$ são: $(1,6)$; $(-1,-6)$; $(2,3)$ e $(-2,-3)$. Então, obtemos quatro formas reduzidas diferentes de discriminante -24, a saber:

$$[1,0,6],[2,0,3],[-1,0-6] \text{ e } [-2,0,-3];$$

somente as duas primeiras formas positivas definidas.

ii) $|b|=2$: procedendo da mesma maneira que no caso anterior, temos que os pares de inteiros (a,c) tais que $ac=7$ e $0<|a|\leqslant|c|$ são $(1,7)$ e $(-1,-7)$. Mas, por (3.9) e $|b|=2$, as formas $[1,b,7]$ e $[-1,b,-7]$ não são reduzidas.

Portanto, as formas positivas definidas e reduzidas de discriminante -24 são precisamente $[1,0,6]$ e $[2,0,3]$.

Agora, pelo Teorema 3.5.2, um inteiro n, diferente de zero, é primitivamente representável por alguma forma de discriminante -24 se, e somente se, a congruência algébrica $x^2 \equiv -24 \pmod{4|n|}$ tem pelo menos uma solução, ou seja, se, e somente se, a congruência algébrica $x^2 \equiv -6 \pmod{|n|}$ tem pelo menos uma solução.

Em especial, para caracterizarmos um número primo $p > 3$ como representável primitivamente por alguma forma de discriminante -24, devemos resolver a seguinte congruência algébrica:

$$x^2 \equiv -6 \pmod{p}.$$

Pelas propriedades do símbolo de Legendre, pelo critério de Euler e pela lei da reciprocidade quadrática, temos

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

Agora, o corolário 2.3.3 dá

$$\left(\frac{2}{p}\right) = \begin{cases} 1, \text{ se } p \equiv 1 \text{ ou } p \equiv 7 \pmod{8} \\ -1, \text{ se } p \equiv 3 \text{ ou } p \equiv 5 \pmod{8} \end{cases}.$$

Por outro lado,

$$\left(\frac{p}{3}\right) = \begin{cases} \left(\frac{1}{3}\right) = 1, \text{ se } p \equiv 1 \pmod{3} \\ \left(\frac{2}{3}\right) = -1, \text{ se } p \equiv 2 \pmod{3} \end{cases}.$$

Como base no que foi exposto acima, obtemos $\left(\frac{-6}{p}\right) = 1$, se

$$\begin{cases} p \equiv 1 \text{ ou } p \equiv 7 \pmod{8} \\ \quad \text{e} \\ p \equiv 1 \pmod{3} \end{cases} \tag{4.5}$$

ou

$$\begin{cases} p \equiv 3 \text{ ou } p \equiv 5 \pmod{8} \\ \quad \text{e} \\ p \equiv 2 \pmod{3} \end{cases} \tag{4.6}$$

A partir daqui, temos as ferramentas necessárias para provar o seguinte teorema.

Teorema 4.2.1 *Os primos p da forma $24k+1$ ou $24k+7$ são os que podem ser escritos da forma x^2+6y^2; os da forma $24k+5$ ou $24k+11$ são os que podem ser escritos da forma $2x^2+3y^2$.*

Primeiro, notemos que os primos 2 e 3 são ambos representáveis pelas formas x^2+6y^2 e $2x^2+3y^2$. Assim, a partir desse momento, tomaremos $p>3$. Queremos, agora, mostrar que um primo p conforme (4.6) não pode ser escrito da forma x^2+6y^2. Para isso, consideremos os primos que são representáveis por essa forma, isto é, os primos tais que $p=x^2+6y^2$, para algum par de inteiros x,y. Observemos que

$$p=x^2+3\cdot 2y^2\equiv x^2 \pmod 3,$$

o que implica

$$p\equiv 1 \pmod 3.$$

Logo, pelo que foi apresentado na parte preliminar desta seção, temos, como consequência imediata, que a forma $2x^2+3y^2$ representa todo primo $p>3$ que satisfaz (4.6).

Reciprocamente, para finalizar a demonstração deste teorema, devemos mostrar que a forma $2x^2+3y^2$ representa, apenas, todo primo $p>3$ descrito em (4.6). Para tanto, tomando um primo $p>3$ representado por essa forma, temos que

$$p=2x^2+3y^2\equiv 2x^2 \pmod 3.$$

Como $x^2\equiv 1 \pmod 3$ (pois $p>3$), temos que

$$p\equiv 2 \pmod 3.$$

Por fim, como $p=2x^2+3y^2$, temos que y deve ser ímpar, isto é, da forma $2k+1$. Daí, analisaremos os seguintes casos, utilizando congruência módulo 8:

i) Se x for par, isto é, da forma $2k'$, então

$$p=2x^2+3y^2=2(2k')^2+3(2k+1)^2=8k'^2+12k^2+12k+3\equiv 12k^2+12k+3 \pmod 8.$$

Como $12k^2+12k=4\cdot 3k(k+1)$ e $k(k+1)$ é par, temos que $12k^2+12k\equiv 0 \pmod 8$ e, consequentemente, a congruência acima resulta em

$$p\equiv 3 \pmod 8.$$

ii) Se x for ímpar, isto é, da forma $2k'+1$, então

$$p = 2(2k'+1)^2 + 3(2k+1)^2 = 8k'^2 + 8k' + 2 + 12k^2 + 12k + 3 \equiv 12k^2 + 12k + 5 \pmod 8.$$

Novamente, como $12k^2 + 12k \equiv 0 \pmod 8$, segue que

$$p \equiv 5 \pmod 8$$

Portanto, um primo $p > 3$ pode ser representado pela forma $2x^2 + 3y^2$ se, e somente se, p for da forma $24k+5$ ou $24k+11$, enquanto p pode ser escrito da forma $x^2 + 6y^2$ se, e somente se, p for da forma $24k+1$ ou $24k+7$. Com isto, concluímos a demonstração desse teorema central.

□

5 CONCLUSÃO

O objetivo principal deste trabalho foi apresentar um estudo inicial das formas quadráticas binárias $ax^2 + bxy + cy^2$, com $a, b, c \in \mathbb{Z}$, nem todos 0, investigando os inteiros n para os quais existam inteiros x, y tais que $n = ax^2 + bxy + cy^2$ e fazendo emprego de técnicas desdobradas em capítulos anteriores para responder aos questionamentos: qual a caracterização dos inteiros positivos que podem ser escritos como soma de dois quadrados? Quais são os primos $p > 3$ que podem ser representados da forma $2x^2 + 3y^2$ ou da forma $x^2 + 6y^2$?

Nesse sentido, apresentamos alguns tópicos relacionados à Teoria dos Números e à Álgebra Abstrata, visando a relevância desses conteúdos para a compreensão do texto.

Para além do aqui exposto, sugerimos ao leitor interessado as referências (BUELL, 1989), (COX, 1989) e (LANDAU, 2002). Em especial, um desenvolvimento natural a partir daqui é a obtenção de fórmulas para o número de classes.

Como observamos nesta dissertação, além dos elementos da Aritmética, fizemos uso de ferramentas algébricas para demonstrar os resultados centrais abordados aqui. Desse modo, faz-se necessário reconhecermos a importância das inter-relações entre campos diferentes da Matemática, e mesmo entre a Matemática e outras áreas do conhecimento, no desenvovimento das ciências.

Ademais, a partir do início do século XIX, em razão da obra Disquisitiones Arithmeticae de Gauss, a Aritmética torna-se Teoria dos Números, tendo um promissor desenvolvimento. Essas ideias de Gauss foram amplamente desenvolvidas, acarretando o que se denomina, na contemporaneidade, Teoria Algébrica dos Números. À medida que os fundamentos dessa teoria e a noção de ideal foram ampliados, o estudo das formas quadráticas binárias tornou-se apenas um caso especial de uma teoria mais geral.

Outros dois ramos da Teoria dos Números também iniciados no século XIX são a Teoria Analítica dos Números e a Geometria Aritmética, as quais ocupam um papel central na Matemática moderna.

Além das contribuições já relatadas nesta dissertação, almejamos incentivar os leitores, os estudantes de graduação e pós-graduação em Matemática e, em especial, os professores da Educação Básica a se interessarem pelo estudo da Teoria dos Números e a buscarem aprofundar seus conhecimentos relacionados a esse campo da Matemática, dando-lhes uma formação complementar desse tema.

REFERÊNCIAS

ANDREWS, G. **Number Theory**. [S.l.]: Dover, 1994.

BUELL, D. A. **Binary Quadratic Forms**. New York: Springer-Verlag, 1989.

COX, D. A. **Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory and Complex Multiplication**. New York: John Wiley & Sons, 1989.

HUNTER, J. **Number Theory**. University of California: OLIVER & BOYD, 1964.

LANDAU, E. **Teoria Elementar dos Números**. São Paulo: Ciência moderna, 2002.

MOREIRA, C. G. T. D. A.; MARTÍNEZ, F. E. B.; SALDANHA, N. C. **Tópicos de Teoria dos Números**. Rio de Janeiro: SBM, 2012. (Coleção PROFMAT).

____. **Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro**. 4. ed. Rio de Janeiro: IMPA, 2018. (Coleção Projeto Euclides).

NETO, A. C. M. **Tópicos de Matemática Elementar: Teoria dos Números**. 2. ed. Rio de Janeiro: SBM, 2013. (Coleção do Professor de Matemática).

SANTOS, J. P. D. O. **Introdução à Teoria dos Números**. 3. ed. Rio de Janeiro: IMPA, 2017. (Coleção Matemática Universitária).