UNIVERSIDADE
BEIRA INTERIOR

Identidades do tipo Menon

Abrantes Malaquias Belo Caiúve

Tese para obtenção do Grau de Doutor em
Matemática e Aplicações
(3º ciclo de estudos)

Orientador: Prof. Doutor Celino José Martins Miguel

Covilhã, Setembro de 2023

UNIVERSIDADE
BEIRA INTERIOR

Identidades do tipo Menon

Abrantes Malaquias Belo Caiúve

Tese para obtenção do Grau de Doutor em
Matemática e Aplicações
(3º ciclo de estudos)

Orientador: Prof. Doutor Celino José Martins Miguel

Júri:
Professor Doutor Paulo Jorge da Silva Almeida
Professora Doutora Deolinda Isabel da Conceição Mendes
Professor Doutor Manuel Baptista Branco
Professor Doutor Sérgio Manuel Moço Nunes Mendes
Professora Doutora Catarina Araújo Santa Clara Pereira
Professor Doutor Celino José Martins Miguel

Covilhã, 15 de Setembro de 2023

Declaração de Integridade

Eu, Abrantes Malaquias Belo Caiúve, que abaixo assino, estudante com o número de inscrição D2015 do curso de Matemática e Aplicações da Faculdade de Ciências, declaro ter desenvolvido o presente trabalho e elaborado o presente texto em total consonância com o **Código de Integridades da Universidade da Beira Interior**.

Mais concretamente afirmo não ter incorrido em qualquer das variedades de Fraude Académica, e que aqui declaro conhecer, que em particular atendi à exigida referenciação de frases, extratos, imagens e outras formas de trabalho intelectual, e assumindo assim na íntegra as responsabilidades da autoria.

Universidade da Beira Interior, Covilhã, Setembro de 2023.

Dedicatória

Aos meus parentes.
pelo afeto permanente demonstrado
apesar da distância.

Aos meus amigos
cujos nomes não enuncio sob pena de olvidar alguém
pela abrupta interrupção do nosso convívio.

À minha amada
por compreender a razão da alteração dos planos
mantendo a fé mesmo na solidão.

Aos meus filhos
todos nascidos enquanto estudava
por serem meus catalisadores existenciais.

Agradecimentos

Ao INAGBE pela bolsa concedida.

A todo pessoal docente e administrativo do ISCED do Sumbe.

Ao José Arlindo Luciano pelas brilhantes explicações que me concedeu.

Ao Alberto Wissi por me ter aconselhado a seguir a docência universitária.

Ao Eslome Gando Citanela Bicicleta por reconhecer as minhas qualificações.

Ao meu tutor pela postura incansável demonstrada na feitura deste trabalho.

Ao Afonso Domingos Belo Caiúve e ao Fernando Vianeque Agostinho por me incentivarem a estudar.

Ao Evaristo José das Mangas e o Moisés Alfredo da Cunha Ferreira por me terem acolhido em seus aposentos.

Aos meus amigos da Associação dos Jovens Estudantes da Cambanda (AJEC) - o meu laboratório inicial de investigação matemática - pela partilha do conhecimento.

Ao Eurico Cambanda Belo Caiúve e ao João Filipe Sivi pela prestimosa ajuda prestada aquando do tratamento da documentação necessária para os estudos no estrangeiro.

Aos IAQs (Investigadores Altamente Qualificados) - grupo dos angolanos doutorandos chegados na Universidade da Beira Interior em 2016 - pelo espírito de entreajuda e de solidariedade evidenciados.

Aos meus colegas de doutoramento (Domingos Salomão, Zacarias Panga Pedro, Dinis Ventura Gonçalves Amaro, Lopo Ferreira de Jesus, Teófilo Domingos Chihaluca e os manos Anacleto César Xavier Mário e Belchior César Xavier Mário) pelo companheirismo, convívio e partilha científica.

À minha mãe Justina Samba Belo Caiúve, ao meu tio Eliseu Epalanga Domingos, ao meu tio Castro Davoca e à minha tia Júlia Nanjesse Belo Catinda por serem os quatro pilares que sustentaram a minha formação (embora mencionados no fim, são na verdade os primeiros no afeto e no coração).

Pensamentos

Os números são a criação livre da mente humana.

Julius Wilhelm Richard Dedekind (1831 — 1916)

É preciso colocar os pensamentos no lugar dos cálculos.

Johann Peter Gustav Lejeune Dirichlet (1805 — 1859)

Resumo

A expressão Matemática que representa a identidade do tipo Menon envolve essencialmente a função totiente de Euler bem como a função divisor. Desde o seu surgimento até aos nossos dias ela tem sido generalizada em várias direções. Em muitas destas generalizações o somatório incide sobre a totalidade do conjunto das unidades, porém nesse trabalho o nosso principal objetivo é restringir esse somatório somente sobre um subconjunto não vazio de unidades. E para o efeito estendemos primeiramente a identidade de Menon a domínios de Dedekind residualmente finitos e seguidamente utilizamos os carateres de Dirichlet para estabelecermos outras identidades deste tipo. Para provarmos os nossos principais resultados entre as ferramentas utilizadas destacamos o lema de Burnside.

Palavras chave

Carateres de Dirichlet; Caráter de Grupo Abeliano Finito; Domínios de Dedekind Residualmente Finitos; Função Divisor; Função Totiente de Euler; Identidade de Menon; Lema de Burnside.

Abstract

The Mathematical expression representing the Menon-type identity essentially involves the Euler totient function as well as the divisor function. From its inception until nowadays it has been generalized in several directions. In many of these generalizations the sum is applied to the entire set of units, but in this work our main goal is to restrict this sum to only a non-empty subset of units. And for this purpose we first extend the Menon identity to residually finite Dedekind domains and then we use Dirichlet characters to establish other identities of this type. To prove our main results among the tools used, we highlight the Burnside's lemma.

Keywords

Dirichlet Characters; Finite Abelian Group Character; Residually Finite Dedekind Domains; Divisor Function; Euler's Totient Function; Menon Identity; Burnside's Lemma.

Sumário

Introdução **xvi**

1 Breves noções de teoria dos números **3**
1.1 Generalidades 3
1.2 Congruências 5
1.3 Funções aritméticas 8

2 Grupos finitos e carateres **11**
2.1 Generalidades 11
2.2 O grupo de carateres e relações de ortogonalidade 14
2.3 Carateres de Dirichlet 16
2.4 Ação de um grupo sobre um conjunto e lema de Burnside 20

3 Anéis **23**
3.1 Generalidades 23
3.2 Anéis artinianos e domínios de Dedekind 27

4 As identidades de tipo Menon **33**
4.1 A identidade de Menon e algumas generalizações 33
4.2 A identidade de Menon em domínios de Dedekind residualmente finitos 42
4.3 Identidades do tipo Menon com carateres de Dirichlet 53
4.4 Identidades do tipo Menon com relação a conjuntos de unidades 61

Conclusões e Trabalho Futuro **65**

Referências **67**

Índice Remissivo **68**

Introdução

A identidade de Menon estabelece uma relação entre a função totiente de Euler e a função divisor. Para um número natural $n \in \mathbb{N} = \{1, 2, \dots\}$

$$\sum_{k \in \mathbb{Z}_n^*} mdc(k-1, n) = \varphi(n)\sigma(n), \quad (1)$$

onde $\mathbb{Z}_n^* = \{k \in \mathbb{Z}_n : mdc(k, n) = 1\}$, ou seja, $\mathbb{Z}_n^*$ é o grupo de unidades do anel $\mathbb{Z}_n$ das classes residuais módulo n, φ é a função totiente de Euler e $\sigma(n) = \sum_{d|n} 1$ é o número de divisores positivos de n. Esta identidade foi provada pelo matemático indiano Puliyakot Keshava Menon em 1965 [12].

As funções totiente de Euler e a divisor são de grande importância em teoria dos números e são também das mais estudadas, mesmo hoje em dia. É notável esta relação entre ambas as funções aritméticas e até certo ponto intrigante. Para além deste interesse em si própria, a identidade de Menon está também relacionada com alguns conceitos de teoria dos números, teoria dos grupos, teoria de anéis e análise combinatória.

Nestes últimos anos tem existido entre os Matemáticos bastante interesse nesta identidade. Foram provadas várias generalizações em variadas direções e por diversos autores em artigos recentes [13; 14; 24]. Nestas generalizações foram usadas inúmeras ferramentas de diversos ramos da Matemática.

Para além destas generalizações citadas, existem outros trabalhos que empregam técnicas diferentes [19; 23]. Para uma visão geral das distintas abordagens relacionadas com a identidade de tipo Menon consulte-se [25].

É do nosso conhecimento que a aritmética dos inteiros $\mathbb{Z}$ pode ser generalizada, com algumas exceções (como o teorema da decomposição única em produto de primos), a outros sistemas de números. Por exemplo, o anel $\mathbb{F}[x]$ dos polinómios em uma variável e coeficientes num corpo $\mathbb{F}$, os inteiros p-ádicos, o anel $\mathbb{O}_{\mathbb{K}}$ dos inteiros num corpo de números algébricos $\mathbb{K}$ ou, de uma forma mais geral, num domínio de Dedekind. A identidade de Menon pode também ser estabelecida nestes sistemas de números. Neste caso, como é habitual na passagem da aritmética dos inteiros para a aritmética dos inteiros num corpo de números algébricos, é necessário usar ideais em vez de elementos e recorrer à ferramentas de teoria de anéis comutativos.

Em todas as identidades de tipo Menon provadas até agora o somatório é sobre todo o grupo das unidades do anel. Quer o anel seja o das classes residuais $\mathbb{Z}_n$, quer seja uma imagem homomorfa finita de um domínio de Dedekind. No nosso trabalho vamos provar identidades do tipo Menon para o caso em que o somatório não é sobre todo o grupo das unidades, mas apenas sobre um subconjunto não vazio de unidades.

Como é bem sabido, o conjunto de todas as unidades de um anel tem estrutura de grupo multiplicativo. Este facto permite o uso de ferramentas da teoria de grupos como por exemplo o bem conhecido lema de Burnside, o qual é frequentemente usado para estabelecer identidades do tipo Menon. Ao passarmos o somatório do conjunto de todas as unidades para um subconjunto não vazio das unidades perdemos a estrutura de grupo. Este facto criou-nos algumas dificuldades uma vez que deixamos de contar com as ferramentas da teoria de grupos. A forma por nós encontrada para lidar com esses obstáculos foi utilizar a teoria de carateres de grupos abelianos finitos. O uso de carateres permitiu-nos relacionar a soma restringida a uma parte do conjunto das unidades com a soma sobre todo o conjunto das unidades.

Lembremos que a teoria dos carateres foi pela primeira vez usada por Dirichlet para provar a infinidade de números primos numa progressão aritmética e que Euler provou que a série dos inversos dos primos

$$\sum \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \cdots$$

é divergente, estabelecendo assim uma nova prova da infinidade dos primos. Dirichlet provou um resultado correspondente, mas com os primos restritos a uma progressão aritmética $kn + h, n = 0, 1, 2, \ldots$ e com $mdc(h, k) = 1$. O procedimento usado por Dirichlet para restringir a soma aos primos na progressão aritmética foi os carateres hoje conhecidos como carateres de Dirichlet.

Tal como já afirmámos, as generalizações da identidade de Menon envolvem ferramentas de teoria dos números, teoria dos grupos, nomeadamente carateres de grupos e teoria de anéis. Sendo assim, dedicamos parte do trabalho à apresentação dos conceitos destes ramos da Matemática usados nas provas das identidades do tipo Menon a fim de tornar o trabalho tanto quanto possível autossuficiente.

Capítulo 1

Breves noções de teoria dos números

Neste capítulo vamos abordar de forma sucinta algumas noções de teoria dos números que são usadas ao longo do trabalho. Para uma abordagem mais alargada, incluindo a prova de todos os teoremas apresentados, podem ser consultadas as obras [2] e [8].

1.1 Generalidades

O conjunto $1, 2, 3, \ldots$ de todos os números naturais representa-se por $\mathbb{N}$. Não vamos abordar aqui questões filosóficas relativas à sua existência. Supomos que o conjunto $\mathbb{N}$ satisfaz os axiomas de Peano. Podemos então definir a adição e a multiplicação em $\mathbb{N}$ de modo que as propriedades comutativa, associativa e distributiva são válidas. Além disso, temos uma ordem em $\mathbb{N}$ de tal forma que para dois elementos distintos m e n de $\mathbb{N}$ temos sempre $m < n$ ou $n < m$. Temos também o princípio de indução matemática, bem como o princípio da boa ordenação: todo o subconjunto S de $\mathbb{N}$ não vazio tem elemento mínimo.

Como é habitual, usamos a letra $\mathbb{Z}$ para o conjunto dos inteiros $\ldots, -2, -1, 0, 1, 2, \ldots$, e $\mathbb{Q}$ para o conjunto dos racionais, isto é, números da forma $\frac{p}{q}$ com $p \in \mathbb{Z}$ e $q \in \mathbb{N}$.

Sejam a e b elementos de $\mathbb{Z}$ com $b \neq 0$ então diz-se que b divide a, e escreve-se $b \mid a$ se existe $c \in \mathbb{Z}$ tal que $a = bc$.

O seguinte teorema é o chamado algoritmo da divisão.

Teorema 1.1.1. *Dados os inteiros a e b com $b > 0$, existe um único par de inteiros q e r tais que $a = bq + r$, com $0 \leq r < b$. É claro que $r = 0$ se, e somente se, $b \mid a$.*

Observação. Dizemos que q é o quociente e r o resto obtido quando a é dividido por b.

Definição 1.1.2. *O máximo divisor comum de dois números naturais a e b é um elemento $d \in \mathbb{N}$ tal que $d \mid a$ e $d \mid b$ e todo o divisor comum de a e b também divide d. Denotamos o máximo divisor comum de a e b por $mdc(a, b)$ ou apenas por (a, b).*

Vamos provar que existe um número d com estas propriedades. Será certamente único já que qualquer outro d' com as mesmas propriedades dividiria a e b e portanto $d' \mid d$. Da mesma forma se concluiria que $d \mid d'$. Logo $d = d'$.

Consideremos agora o conjunto de todos os números naturais da forma $ax + by$ com $x, y \in \mathbb{Z}$ e $a, b \in \mathbb{N}$. Este conjunto não é vazio já que contém por exemplo a e b.

Pelo princípio da boa ordenação o conjunto tem um elemento mínimo d. Temos então $d = ax + by$ para alguns $x, y \in \mathbb{Z}$. Portanto cada divisor comum de a e b divide necessariamente d. Além disso, pelo algoritmo da divisão temos $a = dq + r$, para $q, r \in \mathbb{Z}$ com $0 \leq r < d$. Pondo $x' = 1 - qx$ e $y' = -qy$ temos que $r = ax' + by'$.

Assim, pela propriedade minimal de d deduzimos que $r = 0$ e portanto $d \mid a$. Da mesma forma se prova que $d \mid b$. Concluímos que d é o máximo divisor comum de a e b. Temos, portanto, o seguinte teorema:

Teorema 1.1.3. *Sejam $a, b \in \mathbb{N}$. Então o máximo divisor comum de a e b é o menor número $d \in \mathbb{N}$ que se escreve na forma*

$$d = ax + by, \quad com \quad x, y \in \mathbb{Z}.$$

Teorema 1.1.4. *Se $mdc(a, b) = 1$ então os números a e b dizem-se primos entre si.*

O anel $\mathbb{Z}$ dos inteiros é um domínio de ideais principais [7, p. 250]. Do Teorema 1.1.3 podemos deduzir o seguinte:

Teorema 1.1.5. *Sejam $a, b \in \mathbb{N}$. Então o ideal do anel $\mathbb{Z}$ gerado por a e b é o ideal principal gerado por $d = mdc(a, b)$.*

Todas estas considerações podem generalizar-se a mais do que dois números. Com efeito, pode provar-se que para $a_1, \ldots, a_m \in \mathbb{N}$ existe um máximo divisor comum $d = mdc(a_1, \ldots, a_m)$ tal que $d = a_1u_1 + \cdots + a_mu_m$ com $u_1, \ldots, u_m \in \mathbb{Z}$ e o ideal principal de $\mathbb{Z}$ gerado por $a_1, \ldots, a_m$ é o ideal gerado por d.

Definição 1.1.6. *O inteiro não negativo m é chamado de mínimo múltiplo comum dos inteiros a e b, e denotamos por $mmc(a, b)$ ou apenas por $[a, b]$, se*

1. *$a \mid m$ e $b \mid m$.*
2. *para qualquer c tal que $a \mid c$ e $b \mid c$ temos $m \mid c$.*

Observação. O $mmc(a, b)$ é o menor inteiro positivo divisível, ao mesmo tempo, por a e por b. Ademais, se a e b são inteiros positivos, então

$$mmc(a, b) \cdot mdc(a, b) = a \cdot b.$$

É claro que todo o número natural a é divisível por 1 e por a (ou seja, por ele próprio).

Definição 1.1.7. *Um factor do número a distinto de 1 e de a diz-se próprio.*

Definição 1.1.8. *Um número $a > 1$ sem fatores próprios diz-se primo.*

Os primeiros primos são $2, 3, 5, 7, 11, 13, \ldots$.

Não é difícil concluir a partir do algoritmo da divisão que um número ou é primo ou pode ser decomposto num produto de primos. O que já não é tão fácil de estabelecer é se essa decomposição é única, a menos da ordem dos fatores primos. Esta unicidade é estabelecida no chamado teorema fundamental da aritmética.

Teorema 1.1.9. *(Teorema Fundamental da Aritmética) - Todo o inteiro $n > 1$ pode representar-se de forma única como um produto de fatores primos, a menos da ordem dos fatores.*

O teorema fundamental da aritmética não é válido para alguns sistemas de números. Para mais detalhes ver [22, p. 82].

A falha do teorema fundamental em alguns anéis de inteiros algébricos confundiu os matemáticos durante séculos. Em 1847 o matemático francês Gabriel Lamé fatorizou a equação de Fermat $x^n + y^n = z^n$ na forma

$$(x + y)(x + \zeta y) \cdots (x + \zeta^{n-1} y) = z^n, \quad (1.1)$$

onde $\zeta = e^{\frac{2\pi i}{n}}$ é uma raiz de índice n da unidade. A partir desta fatorização Lamé julgou ter provado a não existência de soluções inteiras para equação de Fermat $x^n + y^n = z^n$ para $n > 2$, isto é, o último teorema de Fermat. Porém, a prova estava errada porque Lamé assumiu a fatorização única nos anéis $\mathbb{Z}[\zeta]$ quando na verdade tal não sucede. Por exemplo, $\mathbb{Z}[e^{\frac{2\pi i}{23}}]$ não verifica o teorema fundamental. Para melhores pormenores o leitor pode consultar [22, p. 5].

1.2 Congruências

Nesta secção introduzimos algumas noções e resultados sobre congruências que serão utilizados no trabalho.

Definição 1.2.1. *Sejam a, b, m inteiros com $m > 0$. Dizemos que a é congruente a b módulo m, e escrevemos*

$$a \equiv b (mod\, m), \quad (1.2)$$

se m divide a diferença $b - a$. O número m é chamado de módulo da congruência.

O símbolo $\equiv$ foi pela primeira vez usado pelo matemático alemão Johann Carl Friedrich Gauss (1777-1855) para sugerir analogia com o símbolo de igualdade. O próximo teorema, cuja a prova é simples, mostra que na realidade a relação de congruência partilha muitas propriedades com a relação de igualdade.

Teorema 1.2.2. *A relação de congruência é uma relação de equivalência, isto é:*

i) $a \equiv a (mod\, m)$ *(reflexiva)*

ii) $a \equiv b (mod\, m)$ *implica* $b \equiv a (mod\, m)$ *(simétrica)*

iii) $a \equiv b (mod\, m)$ *e* $b \equiv c (mod\, m)$ *implica* $a \equiv c (mod\, m)$ *(transitiva).*

As classes de equivalência da relação de congruência $\equiv$ chamam-se classes residuais. É fácil concluir que, fixado um módulo m, as classes residuais dos elementos

$$0, 1, 2, \ldots, m - 1 \quad (1.3)$$

são disjuntas e a sua união é o conjunto $\mathbb{Z}$ dos inteiros no seu todo. Existem, portanto, m classes residuais distintas módulo m.

É claro que se $a \equiv a' (\mathrm{mod}\, m)$ e $b \equiv b' (\mathrm{mod}\, m)$ então $a+b \equiv a'+b' (\mathrm{mod}\, m)$ e $a-b \equiv a'-b' (\mathrm{mod}\, m)$. Temos ainda que $ab \equiv a'b' (\mathrm{mod}\, m)$.

Definimos assim uma adição e uma multiplicação no conjunto das classes residuais. Estas operações conferem ao conjunto das classes residuais a estrutura de anel. Este anel é denotado por $\mathbb{Z}_m$.

Levando em linha de conta (1.3) podemos escrever

$$\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}.$$

Observação. Também pode provar-se que se $mdc(k, m) = 1$ então as classes residuais de

$$0, k, 2k, \ldots, (m-1)k$$

são também disjuntas e a sua união é o conjunto $\mathbb{Z}$ no seu todo. Isto é, formam um conjunto completo de resíduos módulo m.

Nos três teoremas seguintes expomos a teoria das congruência lineares.

Teorema 1.2.3. *Consideremos $mdc(a, m) = 1$. Então a congruência linear*

$$ax \equiv b (mod\, m) \quad (1.4)$$

tem uma e uma só solução.

Demonstração. Como já vimos $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$. Mas como $mdc(a, m) = 1$ então os elementos

$$0, a, 2a, \ldots, (m-1)a \quad (1.5)$$

formam um conjunto completo de resíduos módulo m. Portanto, um e um só de entre os números (1.5) é congruente a b módulo m. Isto é, existe uma e uma só solução para a congruência linear (1.4).

■

Teorema 1.2.4. *Se $mdc(a, m) = d$. Então a congruência linear*

$$ax \equiv b (mod\, m) \quad (1.6)$$

tem solução se, e somente se, $d \mid b$.

Demonstração. A congruência (1.6) é equivalente à equação diofantina nas variáveis x e y

$$ax - my = b.$$

O resultado segue do Teorema 1.1.3.

■

Estando estabelecidas as condições para a resolubilidade da congruência linear $ax \equiv b(mod\, m)$ vamos de seguida contar o número de soluções.

Teorema 1.2.5. *Seja $mdc(a, m) = d$ e suponhamos que $d \mid b$. Então a congruência linear*

$$ax \equiv b(mod\, m) \quad (1.7)$$

tem exatamente d soluções. Essas soluções são dadas por

$$t, t + \frac{m}{d}, t + 2\frac{m}{d}, \ldots, t + (d-1)\frac{m}{d}, \quad (1.8)$$

onde t é a solução única, módulo $\frac{m}{d}$, da congruência linear

$$\frac{a}{d}x \equiv \frac{b}{d}\left(mod\, \frac{m}{d}\right) \quad (1.9)$$

Demonstração. Toda a solução de (1.9) é também de (1.7). Inversamente, toda a solução de (1.7) satisfaz (1.9). Agora, as d soluções listadas em (1.8) são soluções de (1.9) e portanto de (1.7).

Na lista (1.8) não pode haver elementos congruentes módulo m uma vez que

$$t + r\frac{m}{d} \equiv t + s\frac{m}{d}(mod\, m)$$

com $0 \leq r < d$ e $0 \leq s < d$ implica $r\frac{m}{d} \equiv s\frac{m}{d}(mod\, m)$ e portanto $r \equiv s(mod\, d)$. Mas $0 \leq |r - s| < d$ e logo $r = s$.

Basta agora mostrarmos que (1.7) não tem soluções para além das listadas em (1.8).

Se y é uma solução de (1.7) então $ay \equiv at(mod\, m)$ e portanto $y \equiv t(mod\, \frac{m}{d})$. Assim, $y = t + k\frac{m}{d}$ para algum k. Mas $k \equiv r(mod\, d)$ para algum r com $0 \leq r < d$. Então,

$$k\frac{m}{d} \equiv r\frac{m}{d}(mod\, m)$$

e portanto

$$y \equiv t + r\frac{m}{d}(mod\, m).$$

Assim, y é congruente módulo m com algum dos elementos listados em (1.8).

■

1.3 Funções aritméticas

Definição 1.3.1. *Uma função, real ou complexa, definida no conjunto dos inteiros positivos diz-se uma função aritmética.*

Definição 1.3.2. *Uma função aritmética não nula f diz-se multiplicativa se $f(m{\cdot}n) = f(m)f(n)$ para quaisquer m e n com $mdc(m,n) = 1$.*

Se o número inteiro positivo n se decompõe em primos na forma $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ então para qualquer função aritmética multiplicativa temos

$$f(n) = f(p_1^{\alpha_1}) \cdots f(p_k^{\alpha_k}).$$

Deste modo uma função aritmética fica determinada pelos valores sobre as potências dos primos. Ao longo do trabalho recorreremos frequentemente a esta propriedade.

Para $n \geq 1$, a função totiente de Euler $\varphi(n)$ é definida como sendo a quantidade de números entre 1 e n que são primos com n. É claro que para um primo p e $\alpha \geq 1$ se tem $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$. Por outro lado pode provar-se que φ é multiplicativa.

Portanto se $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ é a decomposição de n em primos temos

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

Outra consequência da propriedade multiplicativa de φ é a seguinte fórmula devida a Gauss:

$$\sum_{d|n} \varphi(d) = n. \quad (1.10)$$

Uma outra função aritmética que vamos usar é a função μ de Möbius. Esta função é definida da seguinte maneira:

$$\mu(1) = 1;$$

se $n > 1$ e se $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ é a decomposição de n em fatores primos então

(a) $\mu(n) = (-1)^k$, se $\alpha_1 = \alpha_2 = \cdots = \alpha_k = 1$,

(b) $\mu(n) = 0$, caso contrário.

É uma consequência imediata da definição que a função de Möbius μ é multiplicativa.

Temos também a igualdade

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

Para x real, denotamos por $[x]$ o maior número inteiro menor ou igual a x.

Teorema 1.3.3. *Se $n \geq 1$ temos*

$$\sum_{d|n} \mu(d) = \left[\frac{1}{n}\right] = \begin{cases} 1 & \text{se } n = 1, \\ 0 & \text{se } n > 1. \end{cases}$$

A função totiente de Euler está relacionada com a função de Möbius através da seguinte fórmula:

Teorema 1.3.4. *Se $n \geq 1$ temos*

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

Para $n \geq 1$ a função divisor $\sigma(n)$ é o número de divisores de n, incluindo 1 e n, enquanto que $\sigma_s(n)$ é a soma das s potências dos divisores de n. Isto é

$$\sigma(n) = \sum_{d|n} 1, \qquad \sigma_s(n) = \sum_{d|n} d^s.$$

temos portanto $\sigma(n) = \sigma_0(n)$. É claro que estas funções são multiplicativas. Se $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ é a decomposição de n em primos então

$$\sigma(n) = \prod_{i=1}^{k}(\alpha_i + 1) \qquad \text{e} \qquad \sigma_s(n) = \prod_{i=1}^{k}\left(\frac{p_i^{(\alpha_i+1)s} - 1}{p_i^s - 1}\right).$$

De seguida vamos definir o produto de Dirichlet de funções aritméticas. Este produto é de grande importância em teoria dos números e vai ser usado por nós em algumas das identidades do tipo Menon.

Definição 1.3.5. *Se f e g são duas funções aritméticas, definimos o seu produto de Dirichlet (ou convolução de Dirichlet) como sendo a função aritmética h definida pela equação*

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

Exemplo 1.3.6.

- *Seja $g(n) = 1$ e $f(n) = n$ para todo $n \in \mathbb{N}$. Então $h(n) = (f * g)(n)$ vai ser igual a soma dos divisores de n, ou seja, $\sigma_1(n)$.*
- *Seja $I(n) = [\frac{1}{n}]$ então $h(n) = (f * I)(n) = f(n)$.*

Como podemos ver no segundo exemplo acima, a função $I(n) = [\frac{1}{n}]$ é a identidade para o produto de Dirichlet. Pode também provar-se que o produto de Dirichlet é associativo e distributivo em relação a adição de funções aritméticas. Na verdade, o conjunto das funções aritméticas tem estrutura de anel comutativo para o produto de Dirichlet e adição de funções aritméticas.

Denotando por identidade N a função $N(n) = n$ para todo n, o Teorema 1.3.4 pode ser escrito na forma

$$\varphi = \mu * N. \quad (1.11)$$

Encerramos esta secção com a bem conhecida fórmula da inversão de Möbius, a qual afirma que

$$f(n) = \sum_{d|n} g(d) \iff g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right), \quad (1.12)$$

ou seja, $f = g * 1$ se, e somente se, $g = f * \mu$.

Capítulo 2

Grupos finitos e carateres

Neste capítulo abordaremos inicialmente a teoria de carateres dos grupos finitos cujo conteúdo aqui apresentado pode ser encontrado em [2]. A seguir veremos a ação de um grupo sobre um conjunto bem como o lema de Burnside.

Embora a noção de caráter possa ser definida em qualquer grupo, os resultados com mais aplicações na teoria dos números são os carateres em grupos abelianos finitos. Vamos nos restringir às propriedades que vão ser aplicadas nas identidades de Menon.

2.1 Generalidades

Definição 2.1.1. *Seja G um grupo arbitrário. Uma função de valor complexo f definida em G é chamada de caráter de G se, e somente se, goza da propriedade multiplicativa*

$$f(ab) = f(a)f(b)$$

para todo $a, b \in G$, e se $f(c) \neq 0$ para algum $c \in G$.

Teorema 2.1.2. *Se f é um caráter de um grupo finito G com elemento identidade e, então $f(e) = 1$ e cada valor da função $f(a)$ é uma raiz da unidade. Na verdade, se $a^n = e$ então $f(a)^n = 1$.*

Demonstração. Escolhamos c tal que $f(c) \neq 0$. Uma vez que $ce = c$ teremos

$$f(c)f(e) = f(c)$$

logo $f(e) = 1$. Se $a^n = e$ então $f(a)^n = f(a^n) = f(e) = 1$.

■

Exemplo 2.1.3. *Um grupo G tem no mínimo um caráter, nomeadamente a função que é identicamente 1 em G. Este é designado o caráter principal.*

Se G' é um subgrupo de um grupo finito G, então para qualquer elemento a em G existe um inteiro n tal que $a^n \in G'$. Se a já está em G', simplesmente tomamos $n = 1$. Se $a \notin G'$ podemos tomar n como sendo a ordem de a, pois $a^n = e \in G'$. No entanto, pode haver uma potência positiva menor de a que se encontra em G'. Pelo princípio da boa ordenação existe um menor inteiro positivo n tal que $a^n \in G'$. Chamamos esse inteiro de indicador de a em G'.

Lema 2.1.4. *[2, p. 132] Seja G' um subgrupo de um grupo abeliano finito G, onde $G' \neq G$. Escolhamos um elemento a em G, $a \notin G'$, e seja h o indicador de a em G'. Então o conjunto de produtos*

$$G'' = \{xa^k : x \in G' \quad e \quad k = 0, 1, 2, 3, \ldots, h-1\}$$

é um subgrupo de G que contém G'. Além disso, a ordem de G'' é h vezes a de G',

$$|G''| = h|G'|.$$

O próximo teorema é de capital importância na teoria de carateres de grupos abelianos finitos.

Teorema 2.1.5. *Um grupo abeliano finito G de ordem n tem exatamente n carateres distintos.*

Demonstração. No Lema 2.1.4 aprendemos como construir, a partir de um dado subgrupo $G' \neq G$, um novo subgrupo G'' contendo G' e pelo menos mais um elemento a não pertencente a G'. Usamos o símbolo $\langle G'; a\rangle$ para denotar o subgrupo G'' construído no Lema 2.1.4. Assim

$$\langle G'; a\rangle = \{xa^k : x \in G' \quad e \quad 0 \leq k < h\}$$

onde h é o indicador de a em G'.

Agora apliquemos esta construção repetidamente, começando com o subgrupo $\{e\}$ que denotamos por G_1. Se $G_1 \neq G$ seja a_1 um elemento de G diferente de e e definamos $G_2 = \langle G_1; a_1\rangle$. Se $G_2 \neq G$ seja a_2 um elemento de G que não esteja em G_2 e definamos $G_3 = \langle G_2; a_2\rangle$. Continuamos o processo para obtermos um conjunto finito de elementos $a_1, a_2, ..., a_t$, e um conjunto correspondente de subgrupos $G_1, G_2, ..., G_{t+1}$ tal que

$$G_{r+1} = \langle G_r; a_r\rangle$$

com

$$G_1 \subset G_2 \subset \cdots \subset G_{t+1} = G.$$

O processo deverá terminar num número finito de passos já que o grupo G dado é finito e cada G_{r+1} contém mais elementos do que o seu predecessor G_r. Considerada uma tal cadeia de subgrupos e provemos o teorema por indução, mostrando que se for verdadeiro para G_r, também deve ser verdadeiro para G_{r+1}.

É evidente que existe apenas um caráter para G_1, nomeadamente a função que é identicamente 1. Assumamos, portanto, que G_r tem ordem m e que existem exatamente m carateres distintos para G_r. Consideremos $G_{r+1} = \langle G_r; a_r\rangle$ e seja h o indicador de a_r em G_r, isto é, o menor inteiro positivo tal que $a_r^h \in G_r$. Mostraremos que existem exatamente h diferentes formas de estender cada caráter de G_r para obtermos um caráter de G_{r+1} e que cada caráter de G_{r+1} é a extensão de algum caráter de G_r. Este facto prova que G_{r+1} tem exatamente mh carateres, e visto que mh é também a ordem de G_{r+1} isto prova o teorema por indução sobre r.

Um elemento típico em G_{r+1} tem a forma

$$xa_r^k, \quad \text{onde} \quad x \in G_r \quad \text{e} \quad 0 \leq k < h.$$

Suponhamos, por enquanto, que seja possível estender um caráter f de G_r para G_{r+1}. Chamemos essa extensão por f^χ e verifiquemos o que pode ser dito sobre $f^\chi(xa_r^k)$. A propriedade multiplicativa

exige que

$$f^{\chi}(xa_r^k) = f^{\chi}(x)f^{\chi}(a_r)^k.$$

Mas $x \in G_r$, então $f^{\chi}(x) = f(x)$ e pela equação acima exposta implica que

$$f^{\chi}(xa_r^k) = f(x)f^{\chi}(a_r)^k.$$

Este facto explica-nos que $f^{\chi}(xa_r^k)$ é determinada assim que $f^{\chi}(a_r)$ é conhecida.

Quais são os possíveis valores para $f^{\chi}(a_r)$?

Seja $c = a_r^h$. Visto que $c \in G_r$, teremos $f^{\chi}(c) = f(c)$, e uma vez que f^{χ} é multiplicativa também teremos $f^{\chi}(c) = f^{\chi}(a_r)^h$. Por conseguinte

$$f^{\chi}(a_r)^h = f(c),$$

então $f^{\chi}(a_r)$ é uma das h-ésimas raízes de $f(c)$. Portanto, existem no máximo h escolhas para $f^{\chi}(a_r)$.

Estas observações mostram-nos como definir f^{χ}. Se f é um dado caráter de G_r, escolhemos uma das h-ésimas raízes de $f(c)$, onde $c = a_r^h$, e definamos $f^{\chi}(a_r)$ como sendo esta raiz. Assim definamos f^{χ} no resto de G_{r+1} pela equação

$$f^{\chi}(xa_r^k) = f(x)f^{\chi}(a_r)^k. \quad (2.1)$$

As h escolhas para $f^{\chi}(a_r)$ são diferentes, logo dá-nos h diferentes maneiras de definir $f^{\chi}(xa_r^k)$. Agora verificamos que a função f^{χ} então definida tem a propriedade multiplicativa que se requer. De (2.1) encontramos

$$\begin{aligned} f^{\chi}(xa_r^k \cdot ya_r^j) &= f^{\chi}(xy \cdot a_r^{k+j}) \\ &= f(xy)f^{\chi}(a_r)^{k+j} \\ &= f(x)f(y)f^{\chi}(a_r)^k f^{\chi}(a_r)^j \\ &= f^{\chi}(xa_r^k)f^{\chi}(ya_r^j), \end{aligned}$$

então f^{χ} é um caráter de G_{r+1}. Não podem existir duas extensões f^{χ} e $\tilde{g}$ idênticas em G_{r+1} porque as funções f e g das quais provêm também seriam então idênticas em G_r. Portanto, cada um dos carateres de G_r pode ser estendido de h maneiras diferentes para produzir um caráter de G_{r+1}. Além disso, se φ é um caráter qualquer de G_{r+1} então a sua restrição em G_r é também um caráter de G_r, logo o processo de extensão produz todos os carateres de G_{r+1}. O que completa a demonstração.

■

Para sermos mais precisos, é necessário especificarmos que tipo de objetos podem aparecer nas entradas da matriz. Por exemplo, o grupo linear geral sobre $\mathbb{Z}$ (o conjunto de números inteiros) é o grupo de $n \times n$ matrizes invertíveis de números inteiros e é denotado por $GL_n(\mathbb{Z})$ ou $GL(n, \mathbb{Z})$.

2.2 O grupo de carateres e relações de ortogonalidade

Neste secção G é um grupo abeliano finito de ordem n. O caráter principal de G é denotado por f_1. Os outros denotados por $f_2, f_3, \ldots, f_n$ são designados *carateres não principais.* Estes gozam da propriedade tal que $f(a) \neq 1$ para algum a em G.

O teorema seguinte estabelece que podemos definir uma estrutura de grupo no conjunto de carateres de um grupo abeliano finito. A prova é simples e será omitida.

Teorema 2.2.1. *Se a multiplicação de carateres for definida pela relação*

$$(f_i f_j)(a) = f_i(a) f_j(a)$$

para cada a pertencente em G, então, o conjunto dos carateres de G formam um grupo abeliano de ordem n. Denotaremos este grupo por $\widehat{G}$. O elemento identidade de $\widehat{G}$ é o caráter principal f_1. O inverso de f_i é o recíproco $1/f_i$.

Observação. Para cada caráter f temos $|f(a)|= 1$. Deste modo, o recíproco $1/f(a)$ é igual ao complexo conjugado $\overline{f(a)}$. Daí, a função $\bar{f}$ definida por $\bar{f}(a) = \overline{f(a)}$ é também um caráter de G. Ademais, temos

$$\begin{aligned} \bar{f}(a) &= \frac{1}{f(a)} \\ &= f(a^{-1}) \end{aligned}$$

para todo a pertencente a G.

Seja G um grupo abeliano finito de ordem n com elementos $a_1, a_2, \ldots, a_n$ e seja $f_1, f_2, \ldots, f_n$ os carateres de G, sendo f_1 o caráter principal.

Denotamos por $A = A(G)$, a matriz $[\, a_{ij}]$ do tipo $n \times n$ cujo o elemento a_{ij} na i-ésima linha e na j-ésima coluna é

$$a_{ij} = f_i(a_j).$$

Demonstraremos que a matriz A tem uma inversa e usaremos este facto para deduzir as chamadas relações de ortogonalidade para carateres. Primeiramente determinemos a soma das entradas de cada linha da matriz A.

Teorema 2.2.2. *A soma das entradas na i-ésima linha da matriz A é dada por*

$$\sum_{r=1}^{n} f_i(a_r) = \begin{cases} n & \text{se } f_i \text{ é o caráter principal (i=1),} \\ 0 & \text{caso contrário.} \end{cases}$$

Demonstração. Seja S a soma em questão. Se $f_i = f_1$, cada termo da soma é 1 e $S = n$. Se $f_i \neq f_1$, existe um elemento b pertencente a G para o qual $f_i(b) \neq 1$. Como a_r percorre todos os elementos de G o mesmo acontece com o produto ba_r. Daí

$$S = \sum_{r=1}^{n} f_i(ba_r)$$

$$= f_i(b) \sum_{r=1}^{n} f_i(a_r)$$

$$= f_i(b)S.$$

Portanto, $S(1 - f_i(b)) = 0$. Visto que $f_i(b) \neq 1$, resulta que $S = 0$.

■

Agora usamos este teorema para mostrar que a matriz A tem inversa.

Teorema 2.2.3. *Seja A^* o conjugado transposto da matriz de A, então teremos*

$$AA^* = nI,$$

onde I é a matriz identidade de ordem $n \times n$. Por isso $n^{-1}A^*$ é o inverso da matriz A.

Demonstração. Seja $B = AA^*$. A entrada b_{ij} na i-ésima linha e j-ésima coluna de B é dada por

$$b_{ij} = \sum_{r=1}^{n} f_i(a_r)\overline{f_j}(a_r)$$

$$= \sum_{r=1}^{n} (f_i\overline{f_j})(a_r)$$

$$= \sum_{r=1}^{n} f_k(a_r),$$

onde $f_k = f_i\overline{f_j} = f_i/f_j$. Agora $f_i/f_j = f_1$ se, e somente se, $i = j$. Consequentemente pelo Teorema 2.2.2 temos

$$b_{ij} = \begin{cases} n & \text{se } i = j, \\ 0 & \text{se } i \neq j. \end{cases}$$

Em outras palavras, $B = nI$

■

No teorema seguinte usamos o facto de a matriz comutar com o seu inverso para deduzir as relações de ortogonalidade para carateres.

Teorema 2.2.4. *Relações de ortogonalidade para os carateres. Temos*

$$\sum_{r=1}^{n} \overline{f_r}(a_i)f_r(a_j) = \begin{cases} n & \text{se } a_i = a_j, \\ 0 & \text{se } a_i \neq a_j. \end{cases} \quad (2.2)$$

Demonstração. A relação $AA^* = nI$ implica que $A^*A = nI$. Mas o elemento da i-ésima linha e j-ésima coluna de A^*A é a soma à esquerda de (2.2). O que completa a demonstração.

■

Observação. Visto que

$$\overline{f_r}(a_i) = f_r(a_i)^{-1} = f_r(a_i^{-1}),$$

o termo geral da soma em (2.2) é igual a

$$f_r(a_i^{-1})f_r(a_j) = f_r(a_i^{-1}a_j).$$

Portanto a relação de ortogonalidade pode ser também expressa da seguinte forma:

$$\sum_{r=1}^{n} f_r(a_i^{-1}a_j) = \begin{cases} n & \text{se } a_i = a_j, \\ 0 & \text{se } a_i \neq a_j. \end{cases} \quad (2.3)$$

Quando a_i é o elemento identidade obtemos:

Teorema 2.2.5. *A soma das entradas na j-ésima coluna de A é dada por*

$$\sum_{r=1}^{n} f_r(a_j) = \begin{cases} n & \textit{se } a_j = e, \\ 0 & \textit{caso contrário.} \end{cases} \quad (2.4)$$

2.3 Carateres de Dirichlet

Um sistema reduzido de restos módulo k é um conjunto de $\varphi(k)$ inteiros $\{a_1, a_2, \ldots, a_{\varphi(k)}\}$ não congruentes módulo k, cada um dos quais é relativamente primo com k. Para cada inteiro a a classe de restos correspondente $\hat{a}$ é o conjunto de todos inteiros congruentes com a módulo k:

$$\hat{a} = \{x : x \equiv a \,(mod\, k)\}.$$

A multiplicação da classe de restos é definida pela relação

$$\hat{a} \cdot \hat{b} \equiv \widehat{ab}. \quad (2.5)$$

Isto é, o produto de duas classes residuais $\hat{a}$ e $\hat{b}$ é a classe residual do produto ab.

Teorema 2.3.1. *Com a multiplicação definida em (2.5) o conjunto das classes reduzidas de restos módulo k é um grupo abeliano finito de ordem $\varphi(k)$. A identidade é a classe residual de $\hat{1}$. O inverso de $\hat{a}$ é a classe residual $\hat{b}$ onde $ab \equiv 1 \,(mod\, k)$.*

Demonstração. A propriedade do fecho é automaticamente verificada a forma como a multiplicação de classes de restos foi definida. A classe $\hat{1}$ é claramente o elemento identidade. Se $mdc(a, k) = 1$, existe um único b tal que $ab \equiv 1 \,(mod\, k)$. Desta maneira o inverso de $\hat{a}$ é $\hat{b}$. Por fim, é claro que o grupo é abeliano e que a sua ordem é $\varphi(k)$.

■

Em seguida vamos introduzir a noção de caráter de Dirichlet. Estes carateres foram pela primeira vez usados em 1831 pelo matemático alemão Johann Peter Gustav Lejeune Dirichlet para a prova da infinidade de números primos numa progressão aritmética. Os carateres de Dirichlet vão constituir uma ferramenta para o nosso resultado sobre identidades de Menon com relação a conjuntos de unidades apresentado na Secção 4.4.

Definição 2.3.2. *Seja G o grupo de classes reduzidas de restos módulo k. Correspondendo a cada caráter de f de G definimos uma função aritmética $\chi = \chi_f$ como se segue:*

$$\chi(n) = f(\hat{n}) \quad se \quad mdc(n, k) = 1,$$

$$\chi(n) = 0 \quad se \quad mdc(n, k) > 1.$$

A função χ é chamada um *caráter de Dirichlet* módulo k. O caráter principal χ_1 é aquele que goza das propriedades

$$\chi_1(n) = \begin{cases} 1 & \text{se} \quad mdc(n,k) = 1, \\ 0 & \text{se} \quad mdc(n,k) > 1. \end{cases} \tag{2.6}$$

Teorema 2.3.3. *Existem $\varphi(k)$ carateres de Dirichlet distintos módulo k, cada um dos quais é completamente multiplicativo e periódico com período k. Isto é, temos*

$$\chi(m.n) = \chi(m)\chi(n) \ \textit{para todo} \ \ m, n \tag{2.7}$$

$$\chi(n+k) = \chi(n) \ \textit{para todo}\, n.$$

Inversamente, se χ é completamente multiplicativo e periódico com período k, e se $\chi(n) = 0$ se $mdc(n,k) > 1$, então χ é um dos carateres de Dirichlet módulo k.

Demonstração. Pelo Teorema 2.1.5 existem $\varphi(k)$ carateres f distintos para o grupo G de classes reduzidas de restos módulo k, por isso $\varphi(k)$ carateres χ_f módulo k. A propriedade multiplicativa (2.7) de χ_f resulta da propriedade multiplicativa de f quando m e n são relativamente primos com k. Se um dos m ou n não for relativamente primo com k também mn não será, como consequência ambos os membros de (2.7) são zero. A propriedade de periodicidade decorre do facto de que $\chi_f(n) = f(\hat{n})$ e que $a \equiv b\,(mod\, k)$ implica que $mdc(a,k) = mdc(b,k)$.

Para provar o recíproco notamos que a função f definida no grupo G pela equação

$$f(\hat{n}) = \chi(n) \quad \text{se} \quad mdc(n,k) = 1$$

é um caráter de G, então χ é um caráter de Dirichlet módulo k.

■

Exemplo 2.3.4. *Quando $k = 1$ ou $k = 2$ teremos $\varphi(k) = 1$ e o único caráter de Dirichlet é o caráter principal χ_1. Para $k \geq 3$, existem pelo menos dois carateres de Dirichlet já que $\varphi(k) \geq 2$. As tabelas seguintes mostram todos os carateres de Dirichlet para $k = 3, 4$ e 5.*

n	1	2	3
$\chi_1(n)$	1	1	0
$\chi_2(n)$	1	-1	0

k= 3; $\varphi(k) = 2$

n	1	2	3	4
$\chi_1(n)$	1	0	1	0
$\chi_2(n)$	1	0	-1	0

k= 4, $\varphi(k) = 2$

n	1	2	3	4	5
$\chi_1(n)$	1	1	1	1	0
$\chi_2(n)$	1	-1	-1	1	0
$\chi_3(n)$	1	i	-i	-1	0
$\chi_4(n)$	1	-i	i	-1	0

k= 5, $\varphi(k) = 4$

Para completar essas tabelas usamos o facto de $\chi(n)^{\varphi(k)} = 1$ sempre que $mdc(n,k) = 1$, logo $\chi(n)$ é uma $\varphi(k)$-ésima raiz da unidade. Notamos também que se χ for um caráter módulo k então também o é o complexo conjugado $\overline{\chi}$. Essa informação é suficiente para completar as tabelas para $k = 3$ e $k = 4$.

O caso $k = 5$ é um pouco mais complexo. Para mais detalhes pode consultar-se [2, p. 139].

Vamos agora abordar a importante noção de condutor de um caráter. Para isso começamos por introduzir a noção de módulo induzido e caráter primitivo.

Definição 2.3.5. *Seja χ um caráter de Dirichlet módulo k e seja d um divisor positivo de k. O número d é chamado um módulo induzido para χ se tivermos*

$$\chi(a) = 1 \quad sempre \quad que \quad mdc(a,\, k) = 1 \quad e \quad a \equiv 1 \,(mod\, d). \quad (2.8)$$

Definição 2.3.6. *Diz-se que um caráter de Dirichlet módulo k é primitivo módulo k se não tem módulos induzidos $d < k$. Por outras palavras, χ é primitivo módulo k se, e somente se, para qualquer divisor d de k, $0 < d < k$, existe um inteiro $a \equiv 1 \,(mod\, d)$, $mdc(a,k) = 1$, tal que $\chi(a) \neq 1$.*

Teorema 2.3.7. *Seja χ um caráter de Dirichlet módulo k e assumamos que $d \mid k, d > 0$. Então d é um módulo induzido para χ se, e somente se,*

$$\chi(a) = \chi(b) \quad sempre \;\; que \quad mdc(a,k) = mdc(b,k) = 1 \quad e \quad a \equiv b (mod\, d). \quad (2.9)$$

Demonstração. Se (2.9) se verifica então d é um módulo induzido uma vez que podemos escolher $b = 1$ com base na equação (2.8).

Escolhamos a e b tais que $mdc(a,k) = mdc(b,k) = 1$ e $a \equiv b (mod\, d)$. Provaremos que $\chi(a) = \chi(b)$. Seja a' o recíproco de $a \bmod k, aa' \equiv 1 \,(mod\, k)$. O recíproco existe porque $mdc(a,k) = 1$. Agora $aa' \equiv 1 \,(mod\, d)$ já que $d \mid k$. Daí $\chi(aa') = 1$ uma vez que d é um módulo induzido. Mas $aa' \equiv ba' \equiv 1 \,(mod\, d)$ porque $a \equiv b \,(mod\, d)$, daí $\chi(aa') = \chi(ba')$, logo

$$\chi(a)\chi(a') = \chi(b)\chi(a')$$

Mas $\chi(a') \neq 0$ pois $\chi(a)\chi(a') = 1$. Cortando $\chi(a')$ temos $\chi(a) = \chi(b)$, e isso completa a demonstração.

■

Teorema 2.3.8. *Seja χ um caráter de Dirichlet módulo k e consideremos $d \mid k, d > 0$. Então são equivalentes:*

i) d é um módulo induzido de χ.

ii) Existe um caráter ψ módulo d tal que

$$\chi(n) = \psi(n)\chi_1(n), \quad para \quad qualquer \quad n, \quad (2.10)$$

onde χ_1 é o caráter principal módulo k.

Demonstração. Suponhamos *ii)* verdadeiro. Escolhamos n que satisfaz $mdc(n,k) = 1$, $n \equiv 1\,(mod\,d)$. Então $\chi_1(n) = \psi(n) = 1$ logo $\chi(n) = 1$ e portanto d é um módulo induzido. Assim, *ii)* implica *i)*.

Consideremos agora *i)* verdadeiro. Vamos construir um caráter ψ módulo d que satisfaz (2.10). Definamos ψ como se segue: Se $mdc(n,d) > 1$, seja $\psi(n) = 0$. Também neste caso temos $mdc(n,k) > 1$, então (2.10) verifica-se porque ambos os membros são zero.

Suponhamos agora $mdc(n,d) = 1$ então, existe um inteiro m tal que $m \equiv n(mod\,d)$ e $mdc(m,k) = 1$. Isto pode ser provado imediatamente com o bem conhecido teorema de Dirichlet [2, p. 154] sobre primos numa progressão aritmética. Usando este teorema a progressão aritmética $xd + n$ contém uma infinidade primos. Escolhamos um desses primos que não divide k, seja ele m. Tendo escolhido m, o qual é único módulo d, definamos

$$\psi(n) = \chi(m).$$

O número $\psi(n)$ está bem definido porque χ toma valores iguais em números que são congruentes módulo d e relativamente primos com k.

Verificamos facilmente que χ é, na verdade, um caráter módulo d. Vamos verificar a equação (2.10) para qualquer n.

Se $mdc(n,k) = 1$ então $mdc(n,d) = 1$ logo $\psi(n) = \chi(m)$ para algum $m \equiv n\,(mod\,d)$. Portanto, pelo Teorema 2.3.7,

$$\chi(n) = \chi(m) = \psi(n) = \psi(n)\chi_1(n)$$

uma vez que $\chi_1 = 1$.

Se $mdc(n,k) > 1$ então $\chi(n) = \chi_1(n) = 0$ e ambos os membros de (2.10) são zero. Assim, (2.10) se verifica para qualquer n.

■

Definição 2.3.9. *Seja χ um caráter de Dirichlet módulo k. O menor módulo induzido d para χ é chamado de condutor de χ.*

Lema 2.3.10. *Todo caráter de Dirichlet χ módulo k pode ser expressado como o produto*

$$\chi(n) = \psi(n)\chi_1(n) \quad (2.11)$$

para qualquer n, onde χ_1 é o caráter principal módulo k e ψ um caráter primitivo módulo o condutor de χ.

Demonstração. Seja d um condutor de χ. Do Teorema 2.3.8 sabemos que χ pode ser expressado como um produto da forma (2.11), onde ψ é um caráter módulo d. Agora provaremos que ψ é primitivo módulo d.

Consideremos que ψ não é primitivo módulo d e cheguemos a uma contradição. Se ψ não for primitivo módulo d então existe um divisor q de d, $q < d$, que é um módulo induzido de ψ. Vamos provar que este q, que divide k, é também um módulo induzido de χ, contradizendo o facto de que

d é o menor módulo induzido de χ.

Escolhamos $n \equiv 1 \,(mod\, q)$, $mdc(n,k) = 1$. Então

$$\chi(n) = \psi(n)\chi_1(n) = \psi(n) = 1$$

porque q é um módulo induzido de ψ. Portanto, q é também um módulo induzido de ψ o que é uma contradição.

■

Vamos também utilizar os chamados carateres aditivos definidos da seguinte maneira:

Definição 2.3.11. *Um caráter aditivo λ_l do anel $\mathbb{Z}_n$ é dado por*

$$\lambda_l(b) = exp(2\pi i w_l b/n),$$

com $0 \leq w_l \leq n-1, w_l \in \mathbb{Z}$ onde $b \in \mathbb{Z}_n$.

2.4 Ação de um grupo sobre um conjunto e lema de Burnside

Nesta secção vamos provar o chamado lema de Burnside. Este lema é de grande utilidade para estabelecer identidades de tipo Menon.

Definição 2.4.1. *Seja G um grupo e S um conjunto não vazio. Diz-se que G opera sobre S (ou que S é um conjunto-G) quando se define uma aplicação*

$$G \times S \to S$$

em que, designando por gs a imagem (nessa aplicação) do par (g,s) se tenha:

1. $(gg')s = g(g's)$
2. $1s = s$

para quaisquer $g, g' \in G$ e $s \in S$.

De seguida vamos introduzir as noções de órbita e de grupo de isotropia.

Definição 2.4.2. *Seja S um conjunto-G e $s \in S$. Chama-se órbita de s ao conjunto*

$$Orb(s) = \{gs \ : \ g \in G\}.$$

Chama-se grupo de isotropia de s ao conjunto

$$G_s = \{g \in G \ : \ gs = s\}.$$

O seguinte teorema vem dar sentido à segunda parte da definição anterior.

Teorema 2.4.3. *Seja S um conjunto-G e $s \in S$. Então, G_s é um subgrupo de G.*

Demonstração. É claro que a identidade de G é elemento de G_s e portanto G_s é não vazio.

Suponhamos agora que $g_1, g_2 \in G_s$, então

$$(g_1 g_2)s = g_1(g_2 s) = g_1 s = s.$$

Portanto, $g_1 g_2 \in G_s$.

Por fim, se $g \in G_s$, então $gs = s$ e portanto

$$g^{-1}s = g^{-1}(gs) = (g^{-1}g)s = s.$$

Assim, $g^{-1} \in G_s$.

■

O teorema seguinte relaciona a órbita de um elemento com o respectivo grupo de isotropia.

Teorema 2.4.4. *Seja G um grupo finito e S um conjunto-G. Então,*

$$|Orb(s)| = [G : G_s].$$

Demonstração. Consideremos a correspondência seguinte entre o conjunto das classes à esquerda definidas por G_s em G e a órbita de s

$$gG_s \to gs.$$

Trata-se de uma aplicação bem definida, já que $gG_s = g'G_s$ equivale a $g^{-1}g' \in G_s$. Assim, $(g^{-1}g')s = s$, donde se conclui que $g's = gs$. É fácil verificar que se trata de uma correspondência bijetiva o que implica então que

$$|Orb(s)| = [G : G_s].$$

■

Lema 2.4.5. *Sejam G um grupo e S um conjunto-G. Sejam $s, s' \in S$ e $y \in G$ tais que $ys = s'$. Então, $G_{s'} = yG_s y^{-1}$.*

Demonstração. Seja $z \in G_{s'}$, isto é, $zs' = s'$. Então, $zys = ys$, portanto $y^{-1}zy \in G_s$. Assim, $z \in yG_s y^{-1}$.

Seja agora $w \in yG_s y^{-1}$. Então, $w = y\bar{w}y^{-1}$ com $\bar{w}s = s$. Temos então

$$ws' = (y\bar{w}y^{-1})s' = (y\bar{w}y^{-1})ys = y\bar{w}s = ys = s'.$$

Logo, $w \in G_{s'}$.

■

O seguinte enunciado é conhecido por lema de Burnside. Este resultado é uma das ferramentas mais usadas para obter identidades do tipo Menon. Para uma análise pormenorizada deste lema o leitor pode consultar [18].

Lema 2.4.6. *Seja G um grupo finito que opera sobre um conjunto S. Seja N o número de órbitas distintas que G determina em S. Seja $S^g = \{s \in S \ : \ gs = s\}$ o número de elementos de S fixados por g. Então,*

$$N = \frac{1}{|G|} \sum_{g \in G} |S^g|.$$

Demonstração. Consideremos o conjunto

$$T = \{(g, s) \in G \times S \ : \ gs = s\}.$$

Podemos contar os elementos de T de dois modos diferentes: ou vendo quantos pares há para cada $g \in G$ e somando os resultados, ou vendo quantos pares há para cada $s \in S$ e somando os resultados. Formalmente:

$$|T| = \sum_{s \in S} |\{g \in G \ : \ gs = s\}| = \sum_{g \in G} |\{s \in S \ : \ gs = s\}|.$$

Isto é,

$$\sum_{s \in S} |G_s| = \sum_{g \in G} |S^g|.$$

Sejam $Orb(s_1), Orb(s_2), ..., Orb(s_N)$ as órbitas distintas em S. Temos então,

$$\sum_{i=1}^{N} \sum_{s \in Orb(s_i)} |G_s| = \sum_{g \in G} |S^g|. \quad (2.12)$$

Invocando o Lema 2.4.5, para cada $s \in Orb(s_i)$ temos que $G_s = xG_{s_i}x^{-1}$, onde $x \in G$ é tal que $xs = s_i$. Logo, para cada $s \in Orb(s_i)$, temos

$$|G_s| = |G_{s_i}|.$$

Assim, a partir da igualdade (2.12) obtemos

$$\sum_{i=1}^{N} |Orb(s_i)|.|G_{s_i}| = \sum_{g \in G} |S^g|.$$

Como pelo Teorema 2.4.4 temos $|Orb(s_i)| = [G : G_s] = \frac{|G|}{|G_{s_i}|}$, obtemos

$$\sum_{i=1}^{N} |G| = \sum_{g \in G} |S^g|.$$

Ou seja,

$$N = \frac{1}{|G|} \sum_{g \in G} |S^g|,$$

tal como queríamos concluir.

■

Capítulo 3

Anéis

Neste capítulo abordamos determinados conceitos sobre anéis usados para estabelecer algumas identidades de Menon. Para o nosso trabalho os anéis mais importantes são os comutativos e de entre estes assumem especial destaque os anéis artinianos e os domínios de Dedekind.

Assumimos que todos os anéis aqui considerados são comutativos e têm identidade uma vez que são estes os usados nas identidades de Menon.

Para uma exposição abrangente da teoria de anéis o leitor pode consultar [1; 4; 15; 17; 20].

3.1 Generalidades

Começamos com as noções de primo e irredutível num domínio de integridade. Estas duas noções, bem como as diferenças entre elas, são de capital importância em teoria dos números.

Definição 3.1.1. *Um domínio de integridade D é um anel com identidade e sem divisores de zero não triviais. Um elemento invertível de D diz-se unidade. O conjunto das unidades denota-se por $U(D)$ ou D^*.*

Exemplo 3.1.2. *O anel $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$ é um domínio de integridade. Outro exemplo muito bem conhecido é do anel $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ dos inteiros de Gauss, onde i é a unidade imaginária.*

Definição 3.1.3. *Dois elementos a e b de um domínio de integridade dizem-se associados se $a \mid b$ e $b \mid a$. Se a e b são associados escrevemos $a \sim b$.*

Em $\mathbb{Z}$, um número primo $p \geq 2$ tem as duas propriedades seguintes:

a) $p = ab \Rightarrow a = \pm 1$ ou $b = \pm 1$. (A)

b) $p \mid ab \Rightarrow p \mid a$ ou $p \mid b$. (B)

A próxima definição generaliza a propriedade (A) a um domínio de integridade.

Definição 3.1.4. *Seja a um elemento não nulo e não unidade de um domínio de integridade D. O elemento a diz-se irredutível se $a = bc$ para $b, c \in D$ implica que b é unidade ou c é unidade.*

Um elemento que não é irredutível diz-se redutível.

Na próxima definição generalizamos a propriedade (B) a domínios de integridade.

Definição 3.1.5. *Seja p um elemento não nulo e não unidade de um domínio de integridade D. O elemento p diz-se primo se $p \mid ab$ para $a, b \in D$ implica que $p \mid a$ ou $p \mid b$.*

Para o domínio de integridade $\mathbb{Z}$ dos números inteiros não existe distinção entre primos e irredutíveis.

No entanto existem domínios de integridade onde se verifica a distinção entre primos e irredutíveis. Por exemplo, no domínio de integridade

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$$

os elementos 2 e 3 são irredutíveis, mas não são primos [22, p. 81].

Teorema 3.1.6. *Num domínio de integridade D um número primo é sempre irredutível.*

Demonstração. Seja $p \in D$ um primo e suponhamos que $p = ab$, com $a, b \in D$.

Como $p \mid ab$ e p é primo devemos ter $p \mid a$ ou $p \mid b$.

Suponhamos, sem perda de generalidade, que $p \mid a$, isto é, $a = pc$, para $c \in D$, temos então

$$p = ab = pcb.$$

Donde concluímos que $p = pcb \Leftrightarrow p(1 - cb) = 0$. Já que $p \neq 0$ e não existem divisores de zero não triviais devemos ter $cb = 1$ e portanto b é uma unidade.

■

Definição 3.1.7. *Um domínio de integridade D diz-se um domínio de ideias principais se todo o seu ideal é principal.*

Um exemplo de um domínio de ideias principais é o anel $\mathbb{Z}$ dos números inteiros. Um exemplo de um domínio de integridade que não é domínio de ideias principais é $\mathbb{Z}[x]$ o anel dos polinómios sobre $\mathbb{Z}$. Com efeito, o ideal $I = \langle 2, x\rangle$ não é principal [20, p. 152].

Teorema 3.1.8. *Num domínio de ideais principais todo elemento irredutível é primo.*

Demonstração. Suponhamos que p é irredutível num domínio de ideais principais D, e que $p \mid ab$. Seja I o ideal gerado por $\{p, b\}$ e d um elemento tal que $I = \langle d\rangle$. Como $p \in \langle d\rangle$ então $p = rd$, para algum $r \in D$. Portanto, como p é irredutível, r é unidade ou d é unidade, mas não ambos, pois, nesse caso, p seria uma unidade.

Se r é unidade então $\langle p\rangle = \langle d\rangle$ e como $b \in \langle d\rangle$ devemos ter $b = sp$ para algum $s \in D$. Assim, $p \mid b$. Se d é unidade então $\langle d\rangle = \langle p, b\rangle = D$ e a identidade pertence ao ideal, o que implica a existência de elementos $u, v \in D$ tais que $1 = up + vb$.

Portanto,

$$a = aup + avb = aup + vtp,$$

para $ab = tp$, pois $p \mid ab$, por hipótese. Logo,

$$p(au + vt) = a,$$

o que significa que p divide a.

■

Portanto, num domínio de ideais principais não há distinção entre irredutíveis e primos.

Definição 3.1.9. *Seja M um ideal de um domínio de integridade D. O ideal M diz-se maximal se $M \neq D$ e se I é um ideal de D tal que $M \subseteq I \subseteq D$ então $I = M$ ou $I = D$.*

Exemplo 3.1.10. *$\langle 5 \rangle$ é um ideal maximal de $\mathbb{Z}$. No entanto em $\mathbb{Z}[i]$, $\langle 5 \rangle$ não é um ideal maximal uma vez que*

$$\langle 5 \rangle \subset \langle 1 + 2i \rangle \subset \mathbb{Z}[i].$$

Teorema 3.1.11. *Seja D um domínio de integridade. Seja $a \in D$ tal que $a \neq 0$ e $a \notin U(D)$. Se $\langle a \rangle$ é um ideal maximal então a é irredutível em D.*

Demonstração. Suponhamos que a não é irredutível. Isto é, $a = bc$, onde b e c não são unidades e são distintos de zero. Então

$$\langle a \rangle \subset \langle b \rangle \subset D,$$

e portanto o ideal $\langle a \rangle$ não é maximal.

■

O próximo exemplo mostra que o inverso do teorema não é em geral verdadeiro.

Exemplo 3.1.12. *O elemento x é irredutível em $\mathbb{Z}[x]$. No entanto o ideal $\langle x \rangle$ não é maximal, uma vez que*

$$\langle x \rangle \subset \langle 2, x \rangle \subset \mathbb{Z}[x].$$

No entanto, para domínios de ideais principais vale o teorema seguinte:

Teorema 3.1.13. *Seja D um domínio de ideais principais. Seja $a \in D$ tal que $a \neq 0$ e $a \notin U(D)$. Então, $\langle a \rangle$ é ideal maximal se, e somente se, a é irredutível em D.*

Demonstração. Em virtude do Teorema 3.1.11 basta demonstrarmos que o ideal gerado por um elemento irredutível é maximal.

Suponhamos que é a irredutível, mas $\langle a \rangle$ não é ideal maximal. Portanto existe um ideal I tal que

$$\langle a \rangle \subset I \subset D.$$

Como D é um domínio de ideais principais, podemos assumir que $I = \langle b \rangle$, para algum $b \in D$. Portanto

$$\langle a \rangle \subset \langle b \rangle \subset D$$

e logo $a = bc$, para algum $c \in D$.

Como $\langle b \rangle \neq D$ temos que b não é unidade. Como $\langle a \rangle \neq \langle b \rangle$ temos que c não é unidade. Portanto a é redutível e esta contradição prova o teorema.

■

Vamos agora introduzir a noção de ideal primo.

Definição 3.1.14. *Seja P um ideal do domínio de integridade D. Este ideal P diz-se primo se $P \neq D$ e para $a, b \in D$ se $ab \in P$ então $a \in P$ ou $b \in P$.*

No próximo teorema caracterizámos os ideais principais primos.

Teorema 3.1.15. *Seja D um domínio de integridade. Seja $a \in D$ tal que $a \neq 0$ e $a \notin U(D)$. Então $\langle a \rangle$ é ideal primo se, e somente se, o elemento a é primo em D.*

Demonstração. Supondo que $\langle a \rangle$ é ideal primo e sejam $b, c \in D$ tal que $a = bc$. Como $bc \in \langle a \rangle$ e $\langle a \rangle$ é ideal primo, devemos ter $b \in \langle a \rangle$ ou $c \in \langle a \rangle$. Ou seja, $a \mid b$ ou $a \mid c$ e portanto a é primo.

Suponhamos agora que a é um elemento primo em D. Sejam $b, c \in D$ e $bc \in \langle a \rangle$. Existe portanto um elemento $d \in D$ tal que $bc = ad$. Logo $a \mid bc$. Como a é primo temos que $a \mid b$ ou $a \mid c$.

Sem perda de generalidade vamos assumir que $a \mid b$, isto é, $b = ae$, para algum $e \in D$. Assim $b \in \langle a \rangle$. Isto demonstra que $\langle a \rangle$ é ideal primo.

■

De seguida abordamos os anéis com condição de cadeia em ideais.

Definição 3.1.16. *Dizemos que um anel R satisfaz a condição de cadeia ascendente se dada uma sequência $\{I_n\}_{n \in \mathbb{N}_0}$ de ideais de R tais que*

$$I_0 \subseteq I_1 \subseteq \cdots \subseteq I_n \subseteq \cdots$$

existe $n_0 \in \mathbb{N}$ tal que se $n > n_0$ então $I_n = I_{n_0}$. Diz-se que a cadeia é estacionária.

O anel R que satisfaz a condição de cadeia ascendente sobre ideais diz-se *anel noetheriano.*

Teorema 3.1.17. *Um anel R é noetheriano se, e somente se, todo o ideal I de R é gerado por um número finito de elementos. Isto é, existem $a_1, a_2, \ldots, a_n$ tais que*

$$I = \langle a_1, a_2, \ldots, a_n \rangle.$$

Demonstração. Se I é o ideal nulo então $I = \langle 0 \rangle$. Caso contrário, seja $a_0 \in I$ um elemento diferente de zero. Se $\langle a_0 \rangle \neq I$ então existe $a_1 \in I - \langle a_0 \rangle$ e $\langle a_0 \rangle \subseteq \langle a_0, a_1 \rangle$.

Se $\langle a_0, a_1 \rangle \neq I$ então existe $a_2 \in I - \langle a_0, a_1 \rangle$ e $\langle a_0 \rangle \subseteq \langle a_0, a_1 \rangle \subseteq \langle a_0, c_1, a_2 \rangle$. Continuando desta forma e usando o facto de o anel R ser noetheriano concluímos que existe um k tal que $I = \langle a_0, a_2, \ldots, a_k \rangle$.

Suponhamos agora que todo o ideal I de R é gerado por um número finito de elementos. Seja

$$I_0 \subseteq I_1 \subseteq \cdots \subseteq I_n \subseteq \cdots$$

uma cadeia ascendente de ideais de R. Consideremos $I = \cup_{n \in \mathbb{N}_0} I_n$. I é um ideal e como todo o ideal é gerado por um número finito de elementos devemos ter $I = \langle a_1, \ldots, a_m \rangle$.

Agora para cada a_j com $j = 1, \ldots, m$ existe $n_j \in \mathbb{N}$ tal que $a_j \in I_{n_j}$. Tomemos $n_0 = máx\{n_1, \ldots, n_m\}$ então para $n > n_0$ temos $a_1, \ldots, a_m \in I_n$ e portanto

$$I = \langle a_1, \ldots, a_m \rangle \subseteq I_n \subseteq \cup_{n \in \mathbb{N}0} I_n = I$$

e assim a cadeia é estacionária.

■

Um exemplo de um anel noetheriano é o anel $\mathbb{Z}$ dos números inteiros. Por outro lado, um exemplo de um anel não noetheriano é o anel $\mathbb{K}[x_1, x_2, \dots]$ dos polinómios num número infinito de variáveis e sobre um corpo. Neste caso

$$\langle x_1 \rangle \subseteq \langle x_1, x_2 \rangle \subseteq \langle x_1, x_2, x_3 \rangle \subseteq \cdots$$

é uma cadeia ascendente não estacionária.

Corolário 3.1.18. *Um domínio de ideais principais é um anel Noetheriano.*

Definição 3.1.19. *Dizemos que um anel R satisfaz a condição de cadeia descendente se dada uma sequência $\{I_n\}_{n\in\mathbb{N}_0}$ de ideais de R tais que*

$$I_0 \supseteq I_1 \supseteq \cdots \supseteq I_n \supseteq \cdots$$

existe $n_0 \in \mathbb{N}$ tal que se $n > n_0$ então $I_n = I_{n_0}$. Diz-se que a cadeia é estacionária.

O anel que satisfaz a condição de cadeia descendente sobre ideais diz-se *artiniano*.

Terminamos esta secção com a noção de elemento integral a qual é frequentemente usada em teoria dos números.

Definição 3.1.20. *Sejam A e B anéis tais que $A \subseteq B$. Um elemento $b \in B$ diz-se integral sobre A, se é raiz de um polinómio mónico*

$$x^n + a_1 x^{n-1} + \cdots + a_n,\ n > 1$$

com coeficientes $a_i \in A$.

O anel B diz-se *integral* sobre A se todos os elementos de B são integrais sobre A.

Definição 3.1.21. *Sejam A e B anéis tais que $A \subseteq B$. O conjunto dos elementos de B que são integrais sobre A diz-se fecho integral de A em B. O anel A diz-se integralmente fechado em B se coincide com o seu fecho integral.*

3.2 Anéis artinianos e domínios de Dedekind

Nesta secção abordamos a estrutura dos anéis comutativos artinianos e a fatorização de ideais em domínios de Dedekind.

Definição 3.2.1. *Um anel comutativo e com um único ideal maximal é chamado de anel local.*

Exemplo 3.2.2. *Se p é primo e $n > 1$, então $\mathbb{Z}_{p^n}$ é um anel local sendo $\langle p \rangle$ o seu único ideal maximal.*

O seguinte resultado será usado para obter identidades de Menon nos domínios de Dedekind residualmente finitos.

Lema 3.2.3. *Seja R um anel local. Se $x, y \in R$ não são unidades então $1 - xy$ é uma unidade.*

Demonstração. É claro que x e y pertencem ao ideal maximal de R. Portanto, xy pertence também a este ideal maximal. Seja agora $1 - xy = t$. Se t não é unidade então $1 = t + xy$ pertence ao ideal maximal. Esta contradição mostra que t é uma unidade.

■

Num anel comutativo com identidade, todo o ideal maximal é primo.

Lema 3.2.4. *Num anel artiniano comutativo R todo o ideal primo é maximal.*

Demonstração. Seja P um ideal primo de R. Então, $D = R/P$ é um domínio de integridade artiniano. Seja $x \in D$ e $x \neq 0$. Pela condição de cadeia descendente temos $\langle x^n \rangle = \langle x^{n+1} \rangle$ para algum $n \in \mathbb{N}$ e portanto,

$$x^n = x^{n+1}y$$

para algum $y \in D$. Então, $x^n(1 - xy) = 0$. Como D é um domínio de integridade devemos ter $xy = 1$. Assim, x é invertível o que prova que $D = R/P$ é um corpo. Consequentemente P é um ideal maximal.

■

Lema 3.2.5. *Um anel artiniano comutativo R tem um número finito de ideais primos.*

Demonstração. Suponhamos que $\{P_i : i \geq 1\}$ é um conjunto infinito de ideais primos distintos. A cadeia descendente

$$P_1 \supseteq P_1 \cap P_2 \supseteq P_1 \cap P_2 \cap P_3 \supseteq \cdots$$

é estacionária. Então, existe um n tal que

$$P_n \supseteq P_1 \cap P_2 \cap \cdots \cap P_{n-1}.$$

Pondo $I_j = P_j + P_n$, para $1 \leq j < n$ temos que

$$P_n = I_1 \cap \cdots \cap I_{n-1}.$$

Como P_n é ideal primo, concluímos que $I_j = P_n$ para algum j. Portanto, $P_j \subseteq P_n$. Como P_j é maximal temos que $P_j = P_n$ o que contradiz o facto dos ideais $\{P_i : i \geq 1\}$ serem distintos. O lema está provado.

■

Definição 3.2.6. *Seja R um anel comutativo. O radical nil de R, denotado por $N(R)$, é a intersecção de todos os ideais primos de R. O radical de Jacobson de R, denotado por $J(R)$, é a intersecção de todos os ideais maximais de R.*

Segue do Lema 3.2.4 que num anel comutativo artiniano o radical nil coincide com o radical de Jacobson.

Num anel artiniano comutativo R o radical nil (e portanto o radical de Jacobson) é nilpotente. Isto é, existe um $k \in \mathbb{N}$ tal que $J(R)^k = 0$ [4, p. 89].

Definição 3.2.7. *Dois ideais I e J de R são coprimos se $I + J = R$.*

No teorema seguinte são caraterizados os anéis comutativos artinianos.

Teorema 3.2.8. *Um anel comutativo artiniano R decompõe-se como uma soma direta de um número finito de anéis locais artinianos.*

Demonstração. Seja $\{M_1, M_2, \ldots, M_n\}$ o conjunto dos ideias maximais de R. Este é também o conjunto dos ideais primos de R. Como ideais maximais distintos são coprimos segue que

$$J(R) = M_1 \cap M_2 \cap \cdots \cap M_n = M_1 \cdot M_2 \cdots M_n.$$

Como $J(R)$ é nilpotente, existe $k > 0$ tal que $M_1^k \cdot M_2^k \cdots M_n^k = 0$. Como $M_1^k, \ldots, M_n^k$ são também coprimos, pelo teorema de [15, p. 171] temos

$$R = R/M_1^k \cdots M_n^k = R/M_1^k \oplus \cdots \oplus R/M_n^k$$

cada R/M_i^k é local com ideal maximal M_i/M_i^k.

■

A noção de domínio de Dedekind permite generalizar a fatorização única válida num domínio de ideais principais (como é o caso dos números inteiros $\mathbb{Z}$) a domínios que não são necessariamente de ideais principais (como é o caso do anel dos inteiros em alguns corpos de números algébricos).

Definição 3.2.9. *Um domínio de Dedekind é um domínio de integridade R que satisfaz as seguintes condições:*

1. *R é um anel noetheriano;*
2. *R é integralmente fechado;*
3. *Cada ideal primo diferente de zero de R é maximal.*

Num domínio de Dedekind existe uma aritmética de ideais semelhante à aritmética de elementos num domínio de ideais principais. Uma das propriedades mais importantes é a fatorização única de um ideal não nulo num produto de ideais primos. Antes de passarmos à demonstração da fatorização única necessitamos de alguns factos sobre ideais primos num domínio de Dedekind.

Lema 3.2.10. *Seja D um domínio de Dedekind. Para todo o ideal $I \neq 0$ de D existem ideais não nulos e primos $P_1, P_2, \ldots, P_r$ tal que*

$$I \supseteq P_1 P_2 \cdots P_r. \quad (3.1)$$

Demonstração. Suponhamos que o conjunto S dos ideais que não satisfazem a condição (3.1) é não vazio. Como D é noetheriano, S tem um elemento maximal A em relação à inclusão. O ideal A não pode ser primo e portanto existem elementos $a, b \in D$ tais que $ab \in A$ mas $a, b \notin A$. Pondo $A_1 = \langle a \rangle + A$ e $A_2 = \langle b \rangle + A$, temos $A \subsetneqq A_1$ e $A \subsetneqq A_2$ e $A_1 A_2 \subseteq A$. Como A é elemento maximal devemos ter que tanto A_1 como A_2 contêm um produto de ideais primos. Mas o produto destes ideais primos está contido em A. Esta contradição prova o lema.

■

Lema 3.2.11. *Seja D um domínio de Dedekind, P um ideal primo de D e $\mathbb{F}$ o corpo das frações de D. Definamos*

$$P^{-1} = \{x \in \mathbb{F} : xP \subseteq D\}$$

e para um ideal A de D definamos

$$AP^{-1} = \Big\{\sum_i a_i x_i : a_i \in A, x_i \in P^{-1}\Big\}.$$

Então, para todo o ideal $A \neq 0$ de D temos que $AP^{-1} \neq A$.

Demonstração. Seja $a \in P$ e $a \neq 0$. Sejam $P_1, P_2, \ldots, P_r$ ideais primos tais que

$$P_1 P_2 \cdots P_r \subseteq \langle a \rangle \subseteq P$$

e com r o menor possível. Necessariamente um dos P_i, por exemplo P_1, está contido em P. Como P_1 é ideal maximal devemos ter $P_1 = P$. Como $P_2 \cdots P_r \nsubseteq \langle a \rangle$, existe $b \in P_2 \cdots P_r$ tal que $b \notin aD$, isto é, $a^{-1}b \notin D$. Por outro lado temos $bP \subseteq \langle a \rangle$, isto é, $a^{-1}bP \subseteq D$ e portanto, $a^{-1}b \in P^{-1}$. Então, temos $P^{-1} \neq D$.

Seja agora A um ideal não nulo de D e $\alpha_1, \ldots, \alpha_n$ um sistema de geradores de A. Assumamos que $AP^{-1} = A$. Então, para todo o $x \in P^{-1}$,

$$x\alpha_i = \sum_j a_{ij}\alpha_j;\ a_{ij} \in D.$$

Denotando por M a matriz cuja entrada (i, j) é dada por $x\delta_{ij} - a_{ij}$ obtemos que

$$M(\alpha_1, \ldots, \alpha_n)^T = 0.$$

Se $d = det(M)$ tem-se que $d\alpha_1 = \cdots = d\alpha_n = 0$ e portanto, $d = 0$. Temos então que x é integral sobre D uma vez que é um zero do polinómio

$$p(X) = det(X\delta_{ij} - a_{ij}) \in D[X].$$

Então, $x \in D$, porque D é integralmente fechado. Mas, então $P^{-1} = D$ o que é contraditório.

■

Estamos agora em condições de provar a existência e unicidade da fatorização de um ideal de um domínio de Dedekind num produto de ideais primos.

Teorema 3.2.12. *Seja D um domínio de Dedekind e I um ideal de D tal que $I \neq 0$ e $I \neq D$, isto é, I é ideal próprio. Então, I é um produto de ideais primos e esta fatorização é única. Isto é,*

$$I = P_1 P_2 \cdots P_k,$$

onde P_i são ideais primos e se

$$P_1 P_2 \cdots P_k = Q_1 Q_2 \cdots Q_n$$

onde Q_i são primos, então, $k = n$ e para qualquer i existe j tal que $P_i = Q_j$.

Demonstração. Existência. Seja S o conjunto de ideais próprios de D que não admitem fatorização em produto de ideiais primos. Se S é não vazio existe um elemento A maximal em S. O ideal A está contido num ideal maximal P. Como $D \subseteq P^{-1}$ temos

$$A \subseteq AP^{-1} \subseteq PP^{-1} \subseteq D$$

Pelo Lema 3.2.11 temos $A \subsetneq AP^{-1}$ e $P \subsetneq PP^{-1} \subseteq D$. Como P é ideal maximal, temos

$$PP^{-1} = D.$$

Como consequência da maximalidade de A em S e como $A \neq P$, isto é $AP^{-1} \neq D$, o ideal AP^{-1} admite uma fatorização em ideais primos, $AP^{-1} = P_1P_2 \cdots P_r$ e portanto

$$A = AP^{-1}P = P_1 \cdots P_rP,$$

o que é contraditório.

Unicidade. Sejam

$$I = P_1P_2 \cdots P_r = Q_1Q_2 \cdots Q_s$$

duas fatorizações em ideais primos do ideal I. Então, $P_1 \supseteq Q_1Q_2 \cdots Q_s$ e assim $P_1 \supseteq Q_i$ para algum i. Sem perda de generalidade suponhamos que $i = 1$. Como Q_1 é maximal temos $P_1 = Q_1$. Agora multiplicando por P_1^{-1} e usando o facto de que $P_1 \neq P_1P_1^{-1} = D$, devemos ter

$$P_2 \cdots P_r = Q_2 \cdots Q_s.$$

repetindo o argumento temos que $r = s$ e $P_i = Q_i$ para todo o i.

■

Capítulo 4

As identidades de tipo Menon

Num artigo publicado em 1965, Puliyakot Keshava Menon provou que

$$\sum_{k\in\mathbb{Z}_n^*} mdc(k-1,n) = \varphi(n)\sigma(n),$$

onde

$$\mathbb{Z}_n^* = \{k \in \mathbb{Z}_n : mdc(k,n) = 1\}$$

é o grupo de unidades do anel $\mathbb{Z}_n$, φ é a função totiente de Euler e $\sigma(n)$ é o número de divisores positivos de n.

Esta identidade tem sido nos últimos anos generalizada em várias direções e também estendida a domínios de Dedekind residualmente finitos.

4.1 A identidade de Menon e algumas generalizações

Vamos começar pela demonstração da já mencionada identidade de Menon original seguindo [12].

Teorema 4.1.1. *Sejam $\mathbb{Z}_n^* = \{k \in \mathbb{Z}_n : mdc(k,n) = 1\}$ o grupo das unidades do anel $\mathbb{Z}_n$, φ é a função totiente de Euler e $\sigma(n)$ o número de divisores positivos de n. Então*

$$\sum_{k\in\mathbb{Z}_n^*} mdc(k-1,n) = \varphi(n)\sigma(n), \quad (4.1)$$

Demonstração. Seja G um grupo abeliano de ordem n. Consideremos a ação de $\mathbb{Z}_n^*$ em G definida da seguinte maneira: A cada $a \in \mathbb{Z}_n^*$ associamos a permutação ψ_a de elementos de G definida por

$$\psi_a(g) = g^a$$

para $g \in G$.

Segundo esta ação dois elementos pertencem a mesma órbita se, e somente se, geram o mesmo subgrupo cíclico.

Sendo assim, o número de órbitas é igual ao número $c(G)$ de subgrupos cíclicos de G. Pelo lema de Burnside temos

$$c(G) = \frac{1}{\varphi(n)} \sum_{a \in \mathbb{Z}_n^*} |G^a|, \quad (4.2)$$

onde G^a é o conjunto de elementos de G fixados por a. Isto é, o conjunto de elementos de G que satisfazem a equação

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

Suponhamos agora que G é um grupo cíclico. Sabemos que todo o subgrupo de um grupo cíclico é cíclico. Mais, se G é um grupo cíclico de ordem n então a ordem de qualquer subgrupo de G é um divisor de n e para cada divisor d de n existe um e um só subgrupo de ordem d. Portanto, no caso em que G é cíclico temos que $c(G)$ coincide com a função divisor $\sigma(n)$. Isto é, $c(G) = \sigma(n)$. Agora $|G^a|$ é o número de soluções da equação

$$x^a = x \Leftrightarrow x^{a-1} = e$$

no grupo G. Como estamos a assumir que G é cíclico, temos que G é isomorfo ao grupo aditivo $\mathbb{Z}_n$ das classes residuais módulo n, podemos assumir que G é o grupo $\mathbb{Z}_n$. Temos então de contar as soluções da equação

$$(a-1)x \equiv 0 \, (mod\, n)$$

Agora, do Teorema 1.2.5 deduz-se que esta equação tem $mdc(a-1, n)$ soluções. No caso de G ser cíclico a equação (4.2) tem então a forma

$$\sigma(n) = \frac{1}{\varphi(n)} \sum_{a \in \mathbb{Z}_n^*} mdc(a-1, n),$$

que é equivalente à equação (4.1).

■

Como podemos observar na demonstração anterior, o lema de Burnside foi fundamental para obter a identidade de Menon (4.1). De seguida vamos usar novamente este lema para generalizar a identidade de Menon (4.1). Vamos seguir o trabalho [23] de B. Sury.

Consideremos o seguinte conjunto de matrizes de ordem r:

$$H = \{h(t_1, t_2, \ldots, t_r) = \begin{bmatrix} t_1 & t_2 & t_3 & \ldots & t_r \\ 0 & 1 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \end{bmatrix} : t_1 \in \mathbb{Z}_n^*, t_i \in \mathbb{Z}_n, \, para\, i > 1\}$$

É claro que o conjunto H é um grupo para a multiplicação de matrizes. Consideremos agora a ação do grupo H no conjunto

$$X = (\mathbb{Z}_n)^r = \{(a_1, \ldots, a_r) : a_i \in \mathbb{Z}_n\} \quad (4.3)$$

definida da seguinte maneira:

Definição 4.1.2. *Dada a matriz $M \in H$ e $x = (a_1, \ldots, a_r) \in X$ o elemento de X correspondente ao par (M, x) é dado pela multiplicação matricial*

$$M \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_r \end{bmatrix} \quad (4.4)$$

Lema 4.1.3. *O número N de órbitas da ação definida em (4.4) é dado por*

$$N = \sigma_{r-1}(n) = \sum_{d|n} d^{r-1}$$

Demonstração. Seja $(a_1, a_2, \ldots, a_r) \in X$ e

$$M = \begin{bmatrix} t_1 & t_2 & t_3 & \ldots & t_r \\ 0 & 1 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \end{bmatrix} \in G.$$

Então

$$M \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_r \end{bmatrix} = \begin{bmatrix} t_1a_1 + t_2a_2 + \cdots + t_ra_r \\ a_2 \\ \vdots \\ a_r \end{bmatrix}$$

então a órbita $O(a_1, a_2, \ldots, a_r)$ do elemento $(a_1, a_2, \ldots, a_r)$ é dada por

$$O(a_1, a_2, \ldots, a_r) = \{(t_1a_1 + t_2a_2 + \cdots + t_ra_r, a_2, \ldots, a_n) : t_1 \in \mathbb{Z}_n^*;\, t_i \in \mathbb{Z}_n, para\, i \geq 2\}.$$

Como podemos observar, todas as coordenadas permanecem fixas excepto a primeira. Usando o teorema chinês do resto podemos também observar que o número de órbitas é uma função multiplicativa de n. Basta então contar o número de órbitas para o caso em que $n = p^k$, sendo p um primo. Vamos dividir o problema em dois casos mutuamente exclusivos e coletivamente exaustivos:

Caso 1. Existe $a_i \in \mathbb{Z}_n^*$ para $2 \leq i \leq r$. Neste caso o conjunto

$$\{t_1a_1 + t_2a_2 + \cdots + t_ra_r : t_1 \in \mathbb{Z}_n^*;\, t_i \in \mathbb{Z}_n, para\, i \geq 2\}$$

coincide com $\mathbb{Z}_n$.

Podemos então observar que para cada escolha de $a_2, \ldots, a_r$ com pelo menos um $a_i \in \mathbb{Z}_n^*$ temos uma órbita

$$\{(u, a_2, \ldots, a_r) : u \in \mathbb{Z}_n\}.$$

O número das órbitas deste tipo é

$$(p^k)^{r-1} - (p^{k-1})^{r-1}.$$

Caso 2. Se $2 \leq i \leq r$ então $a_i \notin \mathbb{Z}_n^*$. Neste caso o elemento é da forma

$$(a_1, pb_2, pb_3, \ldots, pb_r).$$

O facto de $\mathbb{Z}_n^*$ ser um grupo multiplicativo implica que o conjunto

$$\{(a_1, pb_2, pb_3, \ldots, pb_r) : a_1 \in \mathbb{Z}_n^*\}$$

é uma órbita. Temos $(p^{k-1})^{r-1}$ órbitas deste tipo.

Agora, se para $2 \leq i \leq r$ temos $b_i \in \mathbb{Z}_n^*$ então o conjunto

$$\{(pb_0, pb_2, \ldots, pb_r) : b_0 \leq p^{k-1}\}$$

é uma órbita, o argumento é o mesmo que no Caso 1. Existem $(p^{k-1})^{r-1} - (p^{k-2})^{r-1}$ órbitas deste tipo.

Procedendo desta forma, vemos que existem duas órbitas da forma $(a_1, 0, 0, \ldots, 0)$. São elas $\{(a_0, 0, 0, \ldots, 0) : a_0 \in \mathbb{Z}_n^*\}$ e $\{(0, \ldots, 0)\}$.

Portanto o número total de órbitas é

$$((p^k)^{r-1} - (p^{k-1})^{r-1}) + (p^{k-1})^{r-1} + ((p^{k-1})^{r-1} - (p^{k-2})^{r-1}) + \cdots + (p^{r-1} - 1) + 2.$$

Simplificando obtemos

$$p^{k(r-1)} + p^{(k-1)(r-1)} + \cdots + p^{r-1} + 1 = \sigma_{r-1}(p^k),$$

tal como queríamos demonstrar.

■

Lema 4.1.4. *Sejam $b_1, b_2, \ldots, b_r \in \mathbb{Z}_n$. A cardinalidade de*

$$\{(x_1, \ldots, x_r) \in (\mathbb{Z}_n)^r : \sum_{i=1}^{r} b_i x_i = 0\}$$

é $n^{r-1} mdc(n, b_1, b_2, \ldots, b_r)$.

Demonstração. A prova é feita por indução. Pelo Teorema 1.2.5 a congruência linear

$$ax \equiv 0 (mod\, n)$$

tem $d = mdc(a, n)$ soluções. Mais, essas soluções são dadas por $\frac{ln}{d}$, para $1 \leq l \leq d$. O resultado é portanto válido para $r = 1$.

Suponhamos agora $r > 1$ e assumamos que o resultado é válido para $r-1$. Vamos contar as soluções $(x_1, \ldots, x_r)$ de $\sum_{i=1}^{r} b_i x_i \equiv 0 (mod\, n)$. Temos necessariamente

$$\sum_{i=2}^{r} b_i x_i = 0 (mod\, mdc(n, b_1)). \quad (4.5)$$

Pela hipótese indutiva o número de soluções de (4.5) é

$$mdc(n, b_1)^{r-2}\, mdc(n, b_1, b_2, \ldots, b_r).$$

Mas, se $x_2, \ldots, x_r$ variam $mod\, n$, podemos trocar cada x_i por um dos

$$\frac{n}{mdc(n, b_1)}$$

múltiplos de $mdc(n, b_1)$.

Portanto, o número de soluções $(x_2, \ldots, x_r)$ com x_i a variar $mod\, n$ é

$$(n, b_1)^{r-1} mdc(n, b_1, b_2, \ldots, b_r)\Big(\frac{n}{mdc(n, b_r)}\Big)^{r-1}.$$

Agora, quando $(x_2, \ldots, x_r)$ é uma solução de

$$\sum_{i=2}^{r} b_i x \equiv 0\, mod(mdc(n, b_1))$$

a equação

$$\frac{b_1}{mdc(n, b_1)} x_1 + \frac{\sum_{i=2}^{r} b_i x_i}{mdc(n, b_1)} \equiv 0\, mod \frac{n}{mdc(n, b_1)}$$

tem uma única solução

$$x_1\, mod \frac{n}{mdc(n, b_1)}.$$

Portanto, temos $mdc(n, b_1)$ escolhas para $x_1 (mod n)$, para cada $(x_2, \ldots, x_r)$ fixos. Assim, o número total de soluções é

$$mdc(n, b_1) mdc(n, b_1)^{r-2} mdc(n, b_1, b_2, \ldots, b_r)\Big(\frac{n}{mdc(n, b_1)}\Big)^{r-1} = n^{r-1} mdc(n, b_1, \ldots, b_r),$$

tal como queríamos provar.

■

Seja agora $h(t_1, t_2, \ldots, t_r) \in H$. Usando o Lema 4.1.4 concluímos que

$$|X^{h(t_1, \ldots, t_r)}| = n^{r-1} mdc(n, t_1 - 1, t_2, \ldots, t_r).$$

Usando agora o lema de Burnside concluímos uma nova identidade de tipo Menon:

$$\sum_{\substack{t_1 \in \mathbb{Z}_n^* \\ t_2, \ldots, t_r \in \mathbb{Z}_n}} mdc(n, t_1 - 1, t_2, \ldots, t_r) = \varphi(n)\sigma_{r-1}(n). \quad (4.6)$$

Continuando nesta ordem de ideias vamos agora seguir o trabalho [24] de Marius Tărnăuceanu. Seja $GL_r(\mathbb{Z}_n)$ o grupo linear geral de grau r sobre o anel $\mathbb{Z}_n$ das classes residuais módulo n. Consideremos o subgrupo T de $GL_r(\mathbb{Z}_n)$ formado por todas matrizes triangulares superiores. Isto é,

$$T = \left\{ \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1r} \\ 0 & a_{22} & \dots & a_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_{rr} \end{bmatrix} : a_{ii} \in \mathbb{Z}_n^*, \ \forall\ i = 1, \dots, r \ \wedge \ a_{ij} \in \mathbb{Z}_n, \ \forall\ 1 \leq i < j \leq r \right\}.$$

É fácil verificar que o subgrupo T tem ordem $\varphi(n)^r n^{\frac{r(r-1)}{2}}$.

Consideremos a ação de T no conjunto X definido em (4.3) dada pela multiplicação matricial (4.4).

Seja $\sigma_i(n) = \sigma_{i-1} * e$, onde $*$ é o produto de Dirichlet e e é a função aritmética tal que $e(n) = 1$ para todo o $n \in \mathbb{N}$.

Vamos provar o seguinte resultado

Teorema 4.1.5. *Sejam n e r inteiros positivos. Então*

$$\sum_{\substack{a_{ii} \in \mathbb{Z}_n^*, i = \overline{1,r} \\ a_{ij} \in \mathbb{Z}_n, 1 \leq i < j \leq r}} \prod_{k=1}^{r} d_k = n^{\frac{r(r-1)}{2}} \varphi(n)^r \sigma_r(n), \quad (4.7)$$

onde

$$d_k = mdc\left(n, \frac{na_{1k}}{mdc(n, a_{11} - 1, a_{12}, \dots, a_{1k-1})}, \frac{na_{2k}}{mdc(n, a_{22} - 1, a_{23}, \dots, a_{2k-1})} \dots \right.$$

$$\left. \frac{na_{k-1k}}{mdc(n, a_{k-1k-1} - 1)}, a_{kk} - 1 \right) \quad \forall\, k = \overline{1, r}.$$

Demonstração. Vamos usar a indução em r. Para $r = 1$ a igualdade (4.7) é a identidade de Menon (4.1).

Mesmo não sendo necessário vamos estudar o caso $r = 2$ uma vez que ajuda a clarificar o caso geral. Devemos provar que

$$\sum_{\substack{a_{11}, a_{22} \in \mathbb{Z}_n^* \\ a_{12} \in \mathbb{Z}_n}} mdc(n, a_{11} - 1) mdc\Big(n, \frac{na_{12}}{mdc(n, a_{11} - 1)}, a_{22} - 1\Big) = n\varphi(n)^2 \sigma_2(n). \quad (4.8)$$

Dois elementos $x = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$ e $y = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$ de X pertencem à mesma órbita se, e somente se, existe $g = \begin{bmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{bmatrix} \in T$ tal que $y = gx$, ou seja,

$$\begin{cases} a_{11}x_1 + a_{12}x_2 = y_1, \\ a_{22}x_2 = y_2. \end{cases} \quad (4.9)$$

Considerando $\mathbb{Z}_n$ como grupo aditivo é fácil provar que se $a, b \in \mathbb{Z}_n$ e $mdc(a, n) = 1$ então, o subgrupo gerado por ab coincide com o subgrupo gerado por b, isto é, $\langle ab \rangle = \langle b \rangle$. Temos então que

o sistema (4.9) é equivalente a

$$\begin{cases} \langle x_2 \rangle = \langle y_2 \rangle \, (= H), \\ \langle x_1 H \rangle = \langle y_1 H \rangle \, em \, \mathbb{Z}_n / H \end{cases}$$

ou seja,

$$\begin{cases} o(x_2) = o(y_2) = \delta \in L_n \\ o_H(x_1) = o_H(y_1) = \delta' \in L_{\frac{n}{\delta}} \end{cases}$$

onde para um inteiro positivo m denotamos por L_m o reticulado dos divisores de m. Desta forma temos que o número N de órbitas da nossa ação é dada por

$$N = |\{(\delta, \delta') : \delta \in L_n, \delta' \in L_{\frac{n}{\delta}}\}| = \sum_{\delta | n} \sigma\Big(\frac{n}{\delta}\Big) = \sum_{\delta | n} \sigma(\delta) = \sigma_2(n). \quad (4.10)$$

Para o caso $r = 2$ podemos determinar uma fórmula explícita para o número N de órbitas.

Seja $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ a decomposição de n em fatores primos. Então

$$N = \frac{1}{2^s} \prod_{i=1}^{s} (\alpha_i + 1)(\alpha_i + 2).$$

Observemos agora que para um elemento fixo $g = \begin{bmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{bmatrix} \in T$ temos que $x = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \in X^g$ se, e somente se, $gx = x$, ou seja,

$$\begin{cases} (a_{11} - 1)x_1 + a_{12}x_2 = 0, \\ (a_{22} - 1)x_2 = 0. \end{cases} \quad (4.11)$$

multiplicando a primeira equação por

$$\frac{n}{mdc(n, a_{11} - 1)},$$

obtemos que (4.11) é equivalente a

$$\begin{cases} \frac{n a_{12}}{mdc(n, a_{11} - 1)} x_2 = 0, \\ (a_{22} - 1)x_2 = 0 \end{cases}$$

e consequentemente

$$x_2 \in \Big\langle \frac{n}{mdc(n, \frac{n a_{12}}{mdc(n, a_{11} - 1)}} \Big\rangle \cap \Big\langle \frac{n}{mdc(n, a_{22} - 1)} \Big\rangle = \Big\langle \frac{n}{mdc(n, \frac{n a_{12}}{mdc(n, a_{11} - 1)}, a_{22} - 1)} \Big\rangle.$$

Então, x_2 pode ser escolhido de

$$mdc(n, \frac{n a_{12}}{mdc(n, a_{11} - 1)}, a_{22} - 1)$$

maneiras. Mais, para cada uma dessas escolhas x_1 pode ser escolhido de $mdc(n, a_{11} - 1)$ maneiras.

Concluímos então que

$$|X^g| = mdc(n, a_{11}-1)mdc\Big(n, \frac{na_{12}}{mdc(n, a_{11}-1)}, a_{22}-1\Big).$$

Finalmente, aplicando o lema de Burnside temos

$$\sigma_2(n) = \frac{1}{n\varphi(n)^2} \sum_{\substack{a_{11}, a_{22} \in \mathbb{Z}_n^* \\ a_{12} \in \mathbb{Z}_n}} mdc(n, a_{11}-1)mdc\Big(n, \frac{na_{12}}{mdc(n, a_{11}-1)}, a_{22}-1\Big)$$

que é equivalente á fórmula (4.8).

Provemos agora a implicação geral. Consideremos que (4.7) verifica-se para $r-1$. Dois elementos

$$x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_r \end{pmatrix} \quad \text{e} \quad y = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_r \end{pmatrix}$$

de X pertencem à mesma órbita se, e somente se, $y = gx$ para algum

$$g = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1r} \\ 0 & a_{22} & \cdots & a_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_{rr} \end{pmatrix} \in T,$$

isto é

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1r}x_r = y_1, \\ a_{22}x_2 + a_{22}x_3 + \cdots + a_{2r}x_r = y_2, \\ \vdots \\ a_{rr}x_r = y_r. \end{cases} \tag{4.12}$$

As igualdades de (4.12) são equivalentes a

$$\begin{cases} \langle x_r \rangle = \langle y_r \rangle, \\ \langle x_{r-1}H_1 \rangle = \langle y_{r-1}H_1 \rangle \quad em \quad \mathbb{Z}/H_1, \\ \vdots \\ \langle x_1 H_{r-1} \rangle = \langle y_1 H_{r-1} \rangle \quad em \quad \mathbb{Z}/H_{r-1}, \end{cases} \tag{4.13}$$

onde

$$\begin{aligned} H_1 &= \langle x_r \rangle = \langle y_r \rangle, \\ H_2 &= \langle x_{r-1}, x_r \rangle = \langle y_{r-1}, y_r \rangle, \\ &\vdots \\ H_{r-1} &= \langle x_2, x_3, \ldots, x_r \rangle = \langle y_2, y_3, \ldots, y_r \rangle, \end{aligned}$$

o que significa que

$$\begin{cases} o(x_r) = o(y_r) = \delta_1 \in L_n, \\ o_{H_1}(x_{r-1}) = o_{H_1}(y_{r-1}) = \delta_2 \in L_{\frac{n}{\delta_1}}, \\ \vdots \\ o_{H_{r-1}}(x_1) = o_{H_{r-1}}(y_1) = \delta_r \in L_{\frac{n}{\delta_1\delta_2\cdots\delta_{r-1}}}. \end{cases} \tag{4.14}$$

Agora é fácil verificar que

$$N = |\{(\delta_1, \delta_2, \ldots, \delta_r) : \delta_1 \in L_n, \delta_2 \in L_{\frac{n}{\delta_1}}, \ldots, \delta_r \in L_{\frac{n}{\delta_1\delta_2\cdots\delta_{r-1}}}\}|$$

$$= \sum_{\delta_1|n} |\{(\delta_2, \ldots, \delta_r) : \delta_2 \in L_{\frac{n}{\delta_1}}, \ldots, \delta_r \in L_{\frac{n}{\delta_1\delta_2\cdots\delta_{r-1}}}\}| = \ldots$$

$$= \sum_{\delta_1|n} \sum_{\delta_2|\frac{n}{\delta_1}} \cdots \sum_{\delta_{r-1}|\frac{n}{\delta_1\delta_2\cdots\delta_{r-1}}} \sigma\Big(\frac{n}{\delta_1\delta_2\cdots\delta_{r-1}}\Big) = \sigma_r(n). \tag{4.15}$$

Por outro lado, dado

$$g = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1r} \\ 0 & a_{22} & \cdots & a_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_{rr} \end{pmatrix} \in T$$

temos

$$x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_r \end{pmatrix} \in X^g$$

se, e somente se,

$$\begin{cases} (a_{11} - 1)x_1 + a_{12}x_2 + \cdots + a_{1r}x_r = 0, \\ (a_{22} - 1)x_2 + a_{23}x_2 + \cdots + a_{2r}x_r = 0, \\ \vdots \\ (a_{rr} - 1)x_r = 0. \end{cases} \tag{4.16}$$

Multiplicando a primeira equação por

$$\frac{n}{mdc(n, a_{11} - 1, a_{12}, \ldots, a_{1r-1})},$$

a segunda equação por

$$\frac{n}{mdc(n, a_{22} - 1, a_{23}, \ldots, a_{2r-1})}, \ldots,$$

e a última equação por

$$\frac{n}{mdc(n, a_{r-1r-1} - 1)},$$

(4.16) torna-se um sistema em x_r que tem

$$d_r = mdc\Big(\frac{na_{1r}}{mdc(n, a_{11}-1, a_{12}, \ldots, a_{1r-1})}, \ldots, \frac{na_{r-1r}}{mdc(n, a_{r-1r-1}-1)}, a_{rr-1}\Big)$$

soluções, nomeadamente $x_r \in \langle \frac{n}{d_r} \rangle$. Fazendo $x_r = \lambda \frac{n}{d_r}$ com $\lambda \in \{0, 1, \ldots, d_r - 1\}$. Então, (4.16) pode ser escrito como

$$\begin{cases} (a_{11}-1)x_1 + a_{12}x_2 + \cdots + a_{1r-1}x_{r-1} = -\lambda \frac{n}{d_r} a_{1r}, \\ (a_{22}-1)x_2 + a_{23}x_3 + \cdots + a_{2r-1}x_{r-1} = -\lambda \frac{n}{d_r} a_{2r}, \\ \vdots \\ (a_{r-1r-1}-1)x_{r-1} = -\lambda \frac{n}{d_r} a_{r-1}. \end{cases} \tag{4.17}$$

Se $(x_1^0, x_2^0, \ldots, x_{r-1}^0)$ é uma solução particular de (4.17) então, obtemos um sistema homogéneo

$$\begin{cases} (a_{11}-1)(x_1 - x_1^0) + a_{12}(x_2 - x_2^0) + \cdots + a_{1r-1}(x_{r-1} - x_{r-1}^0) = 0, \\ (a_{22}-1)(x_2 - x_2^0) + a_{23}(x_3 - x_3^0) + \cdots + a_{2r-1}(x_{r-1} - x_{r-1}^0) = 0, \\ \vdots \\ (a_{r-1r-1}-1)(x_{r-1} - x_{r-1}^0) = 0 \end{cases} \tag{4.18}$$

com $\prod_{k=1}^{r-1} d_k$ soluções pela hipótese indutiva. Nós inferimos que

$$|X^g| = \prod_{k=1}^{r} d_k,$$

a qual juntamente com (4.15) conduz a igualdade (4.7). O que completa a demonstração.

■

4.2 A identidade de Menon em domínios de Dedekind residualmente finitos

Como é bem sabido, existem outros sistemas de números com propriedades semelhantes aos inteiros racionais. Por exemplo, o anel $\mathbb{F}[x]$ dos polinómios em uma variável e com coeficientes num corpo $\mathbb{F}$, os inteiros p-ádicos, o anel $\mathbb{O}_{\mathbb{K}}$ dos inteiros num corpo de números algébricos $\mathbb{K}$ ou, de forma mais geral, um domínio de Dedekind. Coloca-se, portanto, a questão da possibilidade de estender a identidade de Menon (bem como algumas das suas generalizações) a contextos mais latos.

Nesta secção vamos apresentar os trabalhos [13] e [14] sobre identidades de Menon em domínios de Dedekind residualmente finitos (ou de norma finita, segundo alguns autores).

Definição 4.2.1. *Um domínio de Dedekind $\mathfrak{D}$ é dito residualmente finito quando para todo o ideal $\mathfrak{n}$ não nulo de $\mathfrak{D}$ o anel quociente $\mathfrak{D}/\mathfrak{n}$ é finito. Neste caso o inteiro positivo $N(\mathfrak{n})$ definido por*

$$N(\mathfrak{n}) = |\mathfrak{D}/\mathfrak{n}|$$

diz-se a norma do ideal $\mathfrak{n}$.

Os anéis residualmente finitos têm grande importância na teoria dos números, uma vez que o anel $\mathbb{O}_{\mathbb{K}}$ dos inteiros num corpo de números algébricos $\mathbb{K}$ (ou de uma forma mais geral num corpo global) é um domínio de Dedekind residualmente finito.

Ao contrário do que acontece no conjunto dos inteiros, num domínio de Dedekind não existe necessariamente fatorização única de elementos. Como exemplo, veja [22, p. 82]. No entanto, se em vez de elementos usarmos ideais então passamos a ter fatorização única.

A fatorização única de ideais num domínio de Dedekind permite estabelecer uma aritmética de ideais similar à aritmética de números inteiros (para mais pormenores ver o Capítulo 1. de [16]).

Num domínio de Dedekind residualmente finito podemos definir a função totiente de Euler para um ideal não nulo. Seja $\mathfrak{n}$ um ideal não nulo de um domínio de Dedekind $\mathfrak{D}$, então a função totiente de Euler $\varphi_{\mathfrak{D}}(\mathfrak{n})$ é definida por

$$\varphi_{\mathfrak{D}}(\mathfrak{n}) = \begin{cases} 1 & se \quad \mathfrak{n} = \mathfrak{D} \\ |U(\mathfrak{D}/\mathfrak{n})| & se \quad \mathfrak{n} \neq \mathfrak{D}. \end{cases}$$

Tal como no caso da função totiente de Euler nos inteiros, temos também

$$\varphi_{\mathfrak{D}}(\mathfrak{n}) = N(\mathfrak{n}) \prod_{\mathfrak{p}|\mathfrak{n}} \left(1 - \frac{1}{N(\mathfrak{p})}\right),$$

onde o produto é sobre todos os ideais primos que dividem $\mathfrak{n}$ (para mais pormenores consultar [16, p. 13]).

Para um ideal não nulo $\mathfrak{n}$ podemos também definir a função divisor $\sigma_{\mathfrak{D}}(\mathfrak{n})$ da seguinte maneira:

$$\sigma_{\mathfrak{D}}(\mathfrak{n}) = \sum_{\mathfrak{d}|\mathfrak{n}} 1.$$

Notemos que num domínio de Dedekind o ideal $\mathfrak{d}$ divide o ideal $\mathfrak{n}$ se, e somente se, o ideal $\mathfrak{d}$ contém o ideal $\mathfrak{n}$.

Num domínio de Dedekind um ideal não nulo está contido num número finito de ideais [16, p. 8]. Portanto, a função $\sigma_{\mathfrak{D}}$ só toma valores finitos.

No teorema seguinte generalizamos a identidade de Menon original (4.1) a domínios de Dedekind residualmente finitos.

Teorema 4.2.2. *Seja $\mathfrak{D}$ um domínio de Dedekind residualmente finito, $\mathfrak{n}$ um ideal não nulo de $\mathfrak{D}$ e $U(\mathfrak{D}/\mathfrak{n})$ o grupo de unidades de $\mathfrak{D}/\mathfrak{n}$. Então*

$$\sum_{a \in U(\mathfrak{D}/\mathfrak{n})} N(\langle a-1 \rangle + \mathfrak{n}) = \varphi_{\mathfrak{D}}(\mathfrak{n})\sigma_{\mathfrak{D}}(\mathfrak{n}). \quad (4.19)$$

Notemos que a identidade (4.1) é um caso particular da identidade (4.19). Na verdade, todo o número natural n gera um ideal principal $\langle n \rangle = \{an : a \in \mathbb{Z}\}$ nos racionais inteiros e, inversamente, todo o ideal não nulo I nos racionais inteiros é gerado por um único número natural n, nomeadamente a norma $N(I) = |\mathbb{Z}/I|$ daquele ideal. Assim sendo, para dois números naturais a e

b temos que $\langle a\rangle + \langle b\rangle = \langle c\rangle$, onde $c = mdc(a, b)$. Por isso, no caso dos racionais inteiros temos

$$N(\langle a-1\rangle + \langle n\rangle) = N(\langle mdc(a-1, n)\rangle) = mdc(a-1, n). \quad (4.20)$$

A demonstração da identidade (4.19), além do Lema de Burnside que já foi usado no contexto dos inteiros, exige algumas ferramentas algébricas. Portanto, antes de passarmos à prova vamos estabelecer as ferramentas algébricas necessárias.

Vamos começar pela unicidade dos geradores de ideais principais. Sejam a e b elementos de um anel comutativo com identidade R. É fácil provar que os elementos a e b são associados se, e somente se, existe uma unidade u pertencente a R tal que $a = ub$. É evidente que dois elementos associados geram o mesmo ideal principal. No entanto, podemos ter dois elementos que geram o mesmo ideal, mas não são associados.

Com efeito, consideremos os pares $(n, f(x))$, onde n é um inteiro racional, $f(x)$ é um polinómio com coeficientes no corpo de Galois de cinco elementos $GF(5)$, e o termo constante de f é congruente com n módulo 5. A adição e a multiplicação são definidas componente a componente. Temos que os elementos $(0, x)$ e $(0, 2x)$ geram o mesmo ideal principal, mas não são associados. Este exemplo deve-se a Kaplansky ([9, p. 466]). Para mais pormenores sobre os geradores dos ideais principais pode ser consultada a obra [21].

No lema seguinte provamos que para anéis comutativos e artinianos dois elementos são associados se, e somente se, geram o mesmo ideal principal.

Lema 4.2.3. *Seja R um anel comutativo com identidade e artiniano. Para dois elementos $a, b \in R$ temos que $\langle a\rangle = \langle b\rangle$ se, e somente se, existe uma unidade $u \in R$ tal que $a = ub$.*

Demonstração. Pelo Teorema 3.2.8, o anel comutativo e artiniano R pode ser decomposto numa soma finita de anéis locais artinianos. Isto é,

$$R \cong R_1 \oplus \cdots \oplus R_k \quad (4.21)$$

onde cada R_i, para $i = 1, \ldots, k$ é um anel local. Portanto, cada elemento $r \in R$ identificado com um $r-$uplo $(r_1, \ldots, r_k)$, onde $r_i \in R_i$, para $i = 1, \ldots, k$ com adição e multiplicação definida componente a componente. Desta forma um ideal $\langle r\rangle$ é decomposto na forma $\langle r_i\rangle \oplus \cdots \oplus \langle r_k\rangle$. Portanto, basta provar o resultado para o caso em que o anel é local.

Suponhamos então que o anel R é local. Como já observámos anteriormente é óbvio que elementos associados geram o mesmo ideal. Suponhamos agora que $\langle a\rangle = \langle b\rangle$. Existem, portanto, $x, y \in R$ tais que $a = bx$ e $b = ay$. Se $a = 0$ ou $b = 0$, não existe nada a provar. Suponhamos que tanto a como b são diferentes de zero.

Se um dos x e y é unidade o resultado é imediato. Caso contrário, usando o facto do anel ser local, temos que $1 - xy$ é uma unidade. Agora $a(1 - xy) = 0$ e portanto, $a = 0$, o que é contraditório.

■

Definição 4.2.4. *Dado um elemento a de um anel comutativo R, o anulador de a em R é dado por*

$$ann_R(a) = \{x \in R : ax = 0\}.$$

O anulador $ann_R(a)$ é um ideal de R.

Lema 4.2.5. *Seja R um anel comutativo residualmente finito com identidade, I um ideal de R e $a \in R$. Se $\psi : R \to R/I$ denota o epimorfismo canónico, então,*

$$|ann_{R/I}(\psi(a))| = |R/(\langle a\rangle + I)|\,.$$

Demonstração. Considere a composição de epimorfismos canónicos

$$R \underset{\psi}{\longrightarrow} R/I \underset{\phi}{\longrightarrow} (R/I)/\langle\psi(a)\rangle.$$

É fácil verificar que o núcleo desta composição é $\langle a\rangle + I$. Portanto, pelo primeiro teorema de isomorfismos para anéis, obtemos

$$R/(\langle a\rangle + I) \cong (R/I)/\langle\psi(a)\rangle. \quad (4.22)$$

Agora consideremos o anel quociente R/I como um $\mathbb{Z}$-módulo e definamos a função $\mathbb{Z}$-linear $L : R/I \to R/I$ por $L(x) = \psi(a)x$. Uma vez que $L(R/I) = \langle\psi(a)\rangle$ e $ker(L) = ann_{R/I}\psi(a)$, pelo primeiro teorema de isomorfismo para módulos segue que

$$(R/I)/ann_{R/I}(\psi(a)) \cong \langle\psi(a)\rangle. \quad (4.23)$$

Finalmente, combinando a equação (4.22) com a equação (4.23), temos que

$$|ann_{R/I}(\psi(a))| = |(R/I)/\langle\psi(a)\rangle| = |R/(\langle a\rangle + I)|\,,$$

como afirmamos.

■

Como já vimos anteriormente no Teorema 1.2.5, a congruência linear $ax \equiv b\,(mod\,n)$ é solúvel se, e somente se, $d = mdc(a, n)$ divide b. Mais, a congruência tem exatamente d soluções distintas módulo n. De seguida vamos generalizar este resultado a domínios de Dedekind residualmente finitos.

Definição 4.2.6. *Dois elementos a e b de um domínio de Dedekind $\mathfrak{D}$ dizem-se congruentes módulo o ideal $\mathfrak{n}$, denota-se por $a \equiv b\,(mod\,\mathfrak{n})$, se, e somente se, $a - b \in \mathfrak{n}$.*

Teorema 4.2.7. *Seja $\mathfrak{D}$ um domínio Dedekind residualmente finito e $\mathfrak{n}$ um ideal de $\mathfrak{D}$. Para $a, b \in \mathfrak{D}$, a congruência linear*

$$ax \equiv b\,(mod\,\mathfrak{n}) \quad (4.24)$$

é solúvel se, e somente se, $b \in \langle a\rangle + \mathfrak{n}$. Além disso, se a congruência é solúvel então, ela tem exatamente $N(\langle a\rangle + \mathfrak{n})$ soluções incongruentes módulo $\mathfrak{n}$.

Demonstração. Suponhamos que a congruência (4.24) seja solúvel e que x_0 seja uma solução. Assim, $ax_0 - b \in \mathfrak{n}$, e, portanto, $b = ax_0 + z$, para algum $z \in \mathfrak{n}$. Assim, $b \in \langle a\rangle + \mathfrak{n}$. Por outro

lado, se $b \in \langle a \rangle + \mathfrak{n}$, então $b = au + v$, para algum $u \in \mathfrak{D}$ e $v \in \mathfrak{n}$. Portanto, u é uma solução de congruência (4.24).

Para contarmos o número de soluções, notamos que a congruência (4.24) é equivalente à seguinte equação no anel quociente $\mathfrak{D}/\mathfrak{n}$

$$\psi(a)x = \psi(b), \quad (4.25)$$

onde ψ denota o epimorfismo canónico de $\mathfrak{D}$ para $\mathfrak{D}/\mathfrak{n}$. Observemos que todas as soluções de (4.25) podem ser escritas na forma $s + h$, onde s é uma solução particular e h pertence ao anulador de $\psi(a)$. Assim, a cardinalidade do conjunto de solução da congruência (4.24) é igual à cardinalidade do anulador de a $\psi(a)$ no anel fatorial $\mathfrak{D}$ para $\mathfrak{D}/\mathfrak{n}$. O resultado segue imediatamente do Lema 4.2.5.

■

O seguinte resultado é bem conhecido na teoria dos números algébricos. Para uma prova pode ser consultada a obra [3, p. 8, Capítulo 3].

Lema 4.2.8. *Seja $\mathfrak{D}$ um domínio de Dedekind. Para todo o ideal não nulo $\mathfrak{n}$ de $\mathfrak{D}$ e $0 \neq a \in \mathfrak{a}$, existe $b \in \mathfrak{n}$ tal que $\mathfrak{n} = \langle a, b \rangle$.*

Podemos agora demonstrar o Teorema 4.2.2.

Demonstração. Seja $\mathfrak{D}$ um domínio de Dedekind residualmente finito e seja $\mathfrak{n}$ um ideal não nulo de $\mathfrak{D}$. Seja o grupo $G = U(\mathfrak{D}/\mathfrak{n})$ de unidades em $\mathfrak{D}/\mathfrak{n}$ que atua em $X = \mathfrak{D}/\mathfrak{n}$ por $(a, b) \mapsto ab$. Assim sendo, para cada $a \in G$ o conjunto $X^a = \{b \in \mathfrak{D}/\mathfrak{n} : ab = b\}$ de elementos em X que são fixados por a tem ordem $N(\langle a - 1 \rangle + \mathfrak{n})$. Esta é uma consequência do Teorema 4.2.7.

Para contarmos o número N de órbitas da ação, observemos que de acordo com o Lema 4.2.3 dois elementos pertencem à mesma órbita se, e somente se, geram o mesmo ideal. Portanto, o número N de órbitas é igual ao número de ideais principais de $\mathfrak{D}/\mathfrak{n}$.

Mostremos que $\mathfrak{D}/\mathfrak{n}$ é um anel de ideais principais. Observemos que os ideais de $\mathfrak{D}/\mathfrak{n}$ são da forma $\mathfrak{a}/\mathfrak{n}$ onde $\mathfrak{a}$ é um ideal de $\mathfrak{D}$ que contém $\mathfrak{n}$. Portanto, seja $\mathfrak{a}/\mathfrak{n}$ um ideal de $\mathfrak{D}/\mathfrak{n}$. Como $\mathfrak{n} \subset \mathfrak{a}$ segue pelo Lema 4.2.8 que existem $b, c, d \in \mathfrak{D}$ tais que $\mathfrak{a} = \langle d, b \rangle$ e $\mathfrak{n} = \langle d, c \rangle$. Consequentemente, $\mathfrak{a}/\mathfrak{n}$ é o ideal principal gerado por $b + \mathfrak{n}$. Como $\sigma_{\mathfrak{D}}(\mathfrak{n})$ é o número de ideais em $\mathfrak{D}/\mathfrak{n}$ segue que $\sigma_{\mathfrak{D}}(\mathfrak{n})$ é igual ao número de órbitas.

Finalmente, aplicando o lema de Burnside, obtemos

$$\sum_{a \in U(\mathfrak{D}/\mathfrak{n})} N(\langle a - 1 \rangle + \mathfrak{n}) = \varphi_{\mathfrak{D}}(\mathfrak{n})\sigma_{\mathfrak{D}}(\mathfrak{n}),$$

como requerido.

■

De seguida vamos generalizar a identidade de B. Sury (4.6) ao contexto dos domínios de Dedekind residualmente finitos.

Para um número inteiro não negativo k, a função divisor generalizada é definida por

$$\sigma_{k\mathfrak{D}}(\mathfrak{n}) = \sum_{\mathfrak{d}|\mathfrak{n}} N(\mathfrak{d})^k,$$

a soma das k-ésimas potências da norma dos ideais que dividem $\mathfrak{n}$. Observemos que, uma vez que consideramos apenas domínios de Dedekind residualmente finitos, segue-se que $\sigma_{k\mathfrak{D}}$ só toma valores finitos.

Teorema 4.2.9. *Seja $\mathfrak{D}$ um domínio de Dedekind residualmente finito e $\mathfrak{n}$ um ideal não nulo de $\mathfrak{D}$. Então,*

$$\sum_{t_1 \in U(\mathfrak{D}/\mathfrak{n}), t_2, \ldots, t_r \in \mathfrak{D}/\mathfrak{n}} N(\langle t_1 - 1, t_2, \ldots, t_r \rangle + \mathfrak{n}) = \varphi_{\mathfrak{D}}(\mathfrak{n}) \sigma_{r-1\mathfrak{D}}(\mathfrak{n}). \quad (4.26)$$

Notemos que um ideal nos inteiros $\mathbb{Z}$ gerados por um conjunto finito de elementos $a_1, \ldots, a_s$ é igual ao ideal principal gerado pelo máximo divisor comum $mdc(a_1, \ldots, a_s)$ dos elementos $a_1, \ldots, a_s$. Segue-se que no caso dos inteiros racionais tem-se

$$N(\langle t_1 - 1, t_2, \ldots, t_r \rangle + \langle n \rangle) = N(\langle t_1 - 1, t_2, \ldots, t_r, n \rangle) = mdc(t_1 - 1, t_2, \ldots, t_r, n).$$

Assim, a equação (4.26) reduz-se à equação (4.6) no caso de inteiros racionais.

Tal como no caso da identidade (4.19), uma das ferramentas chave para a demonstração da identidade (4.26) é o lema de Burnside.

Vamos calcular ambos os lados do lema de Burnside para a ação do grupo multiplicativo de matrizes

$$G = \left\{ g(t_1, \ldots, t_r) = \begin{bmatrix} t_1 & t_2 & t_3 & \ldots & t_r \\ 0 & 1 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \end{bmatrix} : t_1 \in U(\mathfrak{D}/\mathfrak{n}),\ t_i \in \mathfrak{D}/\mathfrak{n} \ \forall\ i > 1 \right\} \quad (4.27)$$

no conjunto

$$X = (\mathfrak{D}/\mathfrak{n})^r = \{(a_1, \ldots, a_r) : \ a_i \in \mathfrak{D}/\mathfrak{n}\}$$

como multiplicação da matriz à esquerda nos vetores coluna. Para este cálculo precisamos de alguns resultados sobre ideais em domínios de Dedekind que são estabelecidos a seguir.

Lema 4.2.10. *Seja $\mathfrak{D}$ um domínio de Dedekind residualmente finito, e sejam $\mathfrak{n}$ e $\mathfrak{m}$ ideais não nulos de $\mathfrak{D}$. Se $\psi : \mathfrak{D} \to \mathfrak{D}/\mathfrak{n}$ denota o epimorfismo canónico, então,*

$$|ann_{\mathfrak{D}/\mathfrak{n}}(\psi(\mathfrak{m}))| = |\mathfrak{D}/(\mathfrak{m} + \mathfrak{n})|.$$

Demonstração. Considere a composição de epimorfismos canónicos

$$\mathfrak{D} \underset{\psi}{\longrightarrow} \mathfrak{D}/\mathfrak{n} \underset{\phi}{\longrightarrow} (\mathfrak{D}/\mathfrak{n})/\psi(\mathfrak{m}).$$

É fácil verificar que o núcleo desta composição é $\mathfrak{m} + \mathfrak{n}$. Portanto, pelo primeiro teorema do isomorfismo para anéis obtemos

$$\mathfrak{D}/(\mathfrak{m} + \mathfrak{n}) \cong (\mathfrak{D}/\mathfrak{n})/\psi(\mathfrak{m}). \quad (4.28)$$

Como vimos na demonstração do Teorema 4.2.2, o anel $\mathfrak{D}/\mathfrak{n}$ é um domínio de ideais principais. Segue-se que $\psi(\mathfrak{m}) = \langle a \rangle$, por algum $a \in \mathfrak{D}/\mathfrak{n}$.

Consideremos agora o anel quociente $\mathfrak{D}/\mathfrak{n}$ como um $\mathbb{Z}$-módulo e definamos a função $\mathbb{Z}$-linear $L : \mathfrak{D}/\mathfrak{n} \to \mathfrak{D}/\mathfrak{n}$ por $L(x) = ax$. Visto que $L(\mathfrak{D}/\mathfrak{n}) = \psi(\mathfrak{m})$ e $ker(L) = ann_{\mathfrak{D}/\mathfrak{n}}\psi(\mathfrak{m})$, pelo primeiro teorema de isomorfismo para módulos segue que

$$(\mathfrak{D}/\mathfrak{n})/ann_{\mathfrak{D}/\mathfrak{n}}\psi(\mathfrak{m}) \cong \psi(\mathfrak{m}). \quad (4.29)$$

Finalmente, combinando a equação (4.28) com a equação (4.29) encontramos

$$|ann_{\mathfrak{D}/\mathfrak{n}}\psi(\mathfrak{m})| = |(\mathfrak{D}/\mathfrak{n})/\psi(\mathfrak{m})| = |\mathfrak{D}/(\mathfrak{m} + \mathfrak{n})|,$$

conforme declarado.

■

Lema 4.2.11. *Seja $\mathfrak{D}$ um domínio de Dedekind residualmente finito, $\mathfrak{n}$ um ideal não nulo de $\mathfrak{D}$ e $\psi : \mathfrak{D} \to \mathfrak{D}/\mathfrak{n}$ o epimorfismo canónico. Para $a_1, \ldots, a_r \in \mathfrak{D}$ a cardinalidade do conjunto*

$$S = \left\{ (x_1, \ldots, x_r) \in (\mathfrak{D}/\mathfrak{n})^r : \sum_{i=1}^{r} \psi(a_i)x_i = 0 \right\}$$

é

$$N(\mathfrak{n})^{r-1} N(\langle a_1, \ldots, a_r \rangle + \mathfrak{n}).$$

Demonstração. Consideremos $\mathfrak{D}/\mathfrak{n}$ e $(\mathfrak{D}/\mathfrak{n})^r$ como $\mathfrak{D}/\mathfrak{n}$-módulos e definamos o homomorfismo de $\mathfrak{D}/\mathfrak{n}$-módulos $\varphi : (\mathfrak{D}/\mathfrak{n})^r \longrightarrow \mathfrak{D}/\mathfrak{n}$ por

$$\varphi(x_1, \ldots, x_r) = \sum_{i=1}^{r} \psi(a_i)x_i.$$

É claro que a imagem de φ é o ideal $\langle \psi(a_1), \ldots, \psi(a_r) \rangle$, e o núcleo de φ é o conjunto S. Observemos que $\langle \psi(a_1), \ldots, \psi(a_r) \rangle = \psi(\langle a_1, \ldots, a_r \rangle)$. Assim, pelo primeiro teorema de isomorfismo para módulos segue que

$$(\mathfrak{D}/\mathfrak{n})^r / Ker(\varphi) \cong \psi(\langle a_1, \ldots, a_r \rangle),$$

e portanto,

$$|S| = |Ker(\varphi)| = \frac{N(\mathfrak{n})^r}{|\psi(\langle a_1, \ldots, a_r \rangle)|}. \quad (4.30)$$

Para encontrarmos a ordem do ideal $\psi(\langle a_1, \ldots, a_r\rangle)$ usamos o fato de $\mathfrak{D}/\mathfrak{n}$ ser um anel de ideais principais. Portanto, podemos assumir que $\psi(\langle a_1, \ldots, a_r\rangle) = \langle w\rangle$ para um elemento fixo $w \in \mathfrak{D}/\mathfrak{n}$. Desta forma consideremos o anel quociente $\mathfrak{D}/\mathfrak{n}$ como um $\mathbb{Z}$-módulo e definamos a função $\mathbb{Z}$-linear de $L : \mathfrak{D}/\mathfrak{n} \to \mathfrak{D}/\mathfrak{n}$ por $L(x) = wx$. Uma vez que $L(\mathfrak{D}/\mathfrak{n}) = \langle w\rangle$ e $Ker(L) = ann_{\mathfrak{D}/\mathfrak{n}}\langle w\rangle$ segue-se do primeiro teorema do homomorfismo para módulos que

$$\langle w\rangle \cong (\mathfrak{D}/\mathfrak{n})/ann_{\mathfrak{D}/\mathfrak{n}}\langle w\rangle, \quad (4.31)$$

como $\mathbb{Z}$-módulos. Usando o Lema 4.2.10 e o isomorfismo (4.31) temos

$$|\psi(\langle a_1, \ldots, a_r\rangle)| = |\langle w\rangle| = |(\mathfrak{D}/\mathfrak{n})/ann_{\mathfrak{D}/\mathfrak{n}}\langle w\rangle| = \frac{N(\mathfrak{n})}{N(\langle a_1, \ldots, a_r\rangle + \mathfrak{n})}. \quad (4.32)$$

Finalmente, combinando a equação (4.30) com a equação (4.32) encontramos

$$|S| = N(\mathfrak{n})^{r-1}N(\langle a_1, \ldots, a_r\rangle + \mathfrak{n}),$$

conforme declarado.

■

Pelo Teorema 3.2.12, cada ideal $\mathfrak{n}$ diferente de zero de um domínio de Dedekind $\mathfrak{D}$ pode ser escrito de forma única como $\mathfrak{n} = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_s^{\alpha_s}$, onde $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ são ideais distintos diferentes de zero e $\alpha_1, \ldots, \alpha_s$ são inteiros positivos. Portanto, usando o teorema chinês do resto, segue-se que

$$\mathfrak{D}/\mathfrak{n} \cong \mathfrak{D}/\mathfrak{p}_1^{\alpha_1} \oplus \cdots \oplus \mathfrak{D}/\mathfrak{p}_s^{\alpha_s}.$$

Para um ideal primo não nulo $\mathfrak{p}$ e um número inteiro positivo α, o anel $\mathfrak{D}/\mathfrak{p}^\alpha$ é um anel local com ideal maximal $\mathfrak{p}/\mathfrak{p}^\alpha$. Além disso, o anel local $\mathfrak{D}/\mathfrak{p}^\alpha$ é um anel cujos ideais formam uma cadeia para a inclusão. De fato, se $a \in \mathfrak{p}/\mathfrak{p}^\alpha$ é um gerador fixo do ideal maximal $\mathfrak{p}/\mathfrak{p}^\alpha$, então os ideais de $\mathfrak{D}/\mathfrak{p}^\alpha$ formam a cadeia.

$$0 = \langle a^\alpha\rangle \subset \langle a^{\alpha-1}\rangle \subset \langle a^{\alpha-2}\rangle \subset \ldots \subset \langle a\rangle \subset \langle a^0\rangle = \mathfrak{D}/\mathfrak{p}^\alpha.$$

Observemos que para $0 \leq \beta \leq \alpha$ temos

$$|\langle a^\beta\rangle| = |\mathfrak{p}^\beta/\mathfrak{p}^\alpha| = N(\mathfrak{p})^{\alpha-\beta}.$$

Para um elemento não nulo $x \in \mathfrak{D}/\mathfrak{p}^\alpha$ denotemos por $w(x)$ o maior inteiro m para o qual $x \in \langle a^m\rangle$. Notemos que se $w(x) = m$ então x pode ser representado exclusivamente na forma $x = ua^m$, onde u é a unidade em $\mathfrak{D}/\mathfrak{p}^\alpha$. Adotamos a convenção de que $w(0) = \infty$. Para quaisquer $x, y \in \mathfrak{D}/\mathfrak{p}^\alpha$ as seguintes propriedades são válidas:

1. $w(x) = 0$, se, e somente se, x é uma unidade;
2. $w(xy) = w(x) + w(y)$;
3. $w(x + y) \geq min\{w(x), w(y)\}$, com igualdade se $w(x) \neq w(y)$.

A relação $\sim$ definida em $\mathfrak{D}/\mathfrak{p}^\alpha$ por $x \sim y$ se, e somente, se $w(x) = w(y)$ é uma relação de equivalência. A classe de equivalência de um elemento não nulo $x \in \mathfrak{D}/\mathfrak{p}^\alpha$ é

$$[x] = U(\mathfrak{D}/\mathfrak{p}^\alpha)a^{w(x)}.$$

Portanto, esta relação de equivalência dá origem à seguinte partição de $\mathfrak{D}/\mathfrak{p}^\alpha$

$$\mathfrak{D}/\mathfrak{p}^\alpha = \{0\} \cup U(\mathfrak{D}/\mathfrak{p}^\alpha) \cup U(\mathfrak{D}/\mathfrak{p}^\alpha)a \cup U(\mathfrak{D}/\mathfrak{p}^\alpha)a^2 \cup \ldots \cup U(\mathfrak{D}/\mathfrak{p}^\alpha)a^{\alpha-1}. \quad (4.33)$$

Para determinar as órbitas da ação do grupo definido em (4.27) no conjunto X vejamos os dois lemas seguintes.

Lema 4.2.12. *Seja $\mathfrak{p}$ um ideal não nulo de um domínio de Dedekind residualmente finito $\mathfrak{D}$ e α um número inteiro positivo. Seja a um gerador fixo do ideal maximal $\mathfrak{p}/\mathfrak{p}^\alpha$ do anel local $\mathfrak{D}/\mathfrak{p}^\alpha$. Se s e l são dois números inteiros que satisfazem $0 \leq s, l \leq \alpha$, então*

$$U(\mathfrak{D}/\mathfrak{p}^\alpha)a^l + \langle a^s \rangle = \begin{cases} \langle a^s \rangle & \text{se } l \geq s, \\ U(\mathfrak{D}/\mathfrak{p}^\alpha)a^l & \text{caso contrário.} \end{cases}$$

Demonstração. Primeiro assumamos que $l \geq s$. A inclusão

$$U(\mathfrak{D}/\mathfrak{p}^\alpha)a^l + \langle a^s \rangle \subseteq \langle a^s \rangle$$

é trivial. Por outro lado, se $x \in \langle a^s \rangle$ então $x = za^s$, para algum $z \in \mathfrak{D}/\mathfrak{p}^\alpha$. Seja $y = z - a^{l-s}$, logo

$$x = za^s = a^l + ya^s \in U(\mathfrak{D}/\mathfrak{p}^\alpha)a^l + \langle a^s \rangle.$$

Assim,

$$\langle a^s \rangle \subseteq U(\mathfrak{D}/\mathfrak{p}^\alpha)a^l + \langle a^s \rangle.$$

Agora assumamos que $l < s$. Claramente

$$U(\mathfrak{D}/\mathfrak{p}^\alpha)a^l \subseteq U(\mathfrak{D}/\mathfrak{p}^\alpha)a^l + \langle a^s \rangle.$$

Por outro lado, se $x \in U(\mathfrak{D}/\mathfrak{p}^\alpha)a^l + \langle a^s \rangle$ então $x = ua^l + za^s$ para alguns elementos $z \in \mathfrak{D}/\mathfrak{p}^\alpha$ e $u \in U(\mathfrak{D}/\mathfrak{p}^\alpha)$. Temos

$$x = ua^l + za^s = ua^l + za^{s-l}a^l = (u + za^{s-l})a^l.$$

Uma vez que num anel local finito a soma de um divisor de zero e uma unidade resulta numa unidade, segue-se que $u + za^{s-l}$ é uma unidade. Por isso, $(u + za^{s-l})a^l \in U(\mathfrak{D}/\mathfrak{p}^\alpha)a^l$ e consequentemente

$$U(\mathfrak{D}/\mathfrak{p}^\alpha)a^l + \langle a^s \rangle \subseteq U(\mathfrak{D}/\mathfrak{p}^\alpha)a^l.$$

■

Lema 4.2.13. *Seja $\mathfrak{p}$ um ideal não nulo de um domínio de Dedekind residualmente finito $\mathfrak{D}$ e α um inteiro positivo. Seja a um gerador fixo do ideal maximal $\mathfrak{p}/\mathfrak{p}^\alpha$ do anel local $\mathfrak{D}/\mathfrak{p}^\alpha$. Se $0 \leq \beta \leq \alpha - 1$, então a ordem do conjunto L definido por*

$$L = \left\{(x_1, \ldots, x_l) \in (\mathfrak{D}/\mathfrak{p}^\alpha)^l : \langle x_1, \ldots, x_l \rangle = \langle a^\beta \rangle\right\}$$

é

$$N(\mathfrak{p}^{\alpha-\beta})^l - N(\mathfrak{p}^{\alpha-\beta-1})^l.$$

Demonstração. Definamos o conjunto

$$S(\beta) = \left\{(x_1, \ldots, x_l) \in (\mathfrak{D}/\mathfrak{p}^\alpha)^l : \langle x_1, \ldots, x_l\rangle \subseteq \langle a^\beta\rangle\right\}.$$

Claramente, um elemento $(x_1, \ldots, x_l)$ pertence a $S(\beta)$ se, e somente se, cada x_i, para $i = 1, \ldots, l$, pertence ao ideal $\langle a^\beta\rangle$. Portanto, a ordem de $S(\beta)$ é $N(\mathfrak{p}^{\alpha-\beta})^l$. Uma vez que os ideais $\mathfrak{D}/\mathfrak{p}^\alpha$ formam uma cadeia de anéis, segue-se que

$$L = S(\beta) - S(\beta + 1),$$

e consequentemente

$$|L| = |S(\beta)| - |S(\beta + 1)| = N(\mathfrak{p}^{\alpha-\beta})^l - N(\mathfrak{p}^{\alpha-\beta-1})^l,$$

tal como queríamos concluir.

■

Vamos agora provar o Teorema 4.2.9.

Demonstração. Seja $\mathfrak{n}$ um ideal não nulo de um domínio de Dedekind residualmente finito $\mathfrak{D}$. Seja o grupo G definido na equação (4.27) que atua no conjunto

$$X = (\mathfrak{D}/\mathfrak{n})^r = \{(a_1, \ldots, a_r) \ : \ a_i \in \mathfrak{D}/\mathfrak{n}\}$$

como a multiplicação de matrizes à esquerda de vetores coluna.

Primeiro, vamos calcular os pontos fixos de um elemento do grupo, $g(t_1, \ldots, t_r) \in G$. Um elemento $(a_1, \ldots, a_r) \in (\mathfrak{D}/\mathfrak{n})^r$ é um ponto fixo de $g(t_1, \ldots, t_r)$ se, e somente se,

$$(t_1 - 1)a_1 + t_2a_2 + \cdots + t_ra_r = 0.$$

Consequentemente, pelo Lemma 4.2.11 o conjunto $X^{g(t_1,\ldots,t_r)}$ de pontos fixos de $g(t_1, \ldots, t_r)$ tem ordem

$$N(\mathfrak{n})^{r-1}N(\langle t_1 - 1, t_2, \ldots, t_r\rangle + \mathfrak{n}).$$

Para contar as órbitas da ação, notemos que o número de órbitas é uma função multiplicativa no conjunto de ideais de $\mathfrak{D}$. Mais precisamente, se $\mathfrak{n} = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_s^{\alpha_s}$ é a decomposição do ideal $\mathfrak{n}$ em potências de ideais primos não nulos, então,

$$|(\mathfrak{D}/\mathfrak{n})^r/G| = \prod_{i=1}^{s} |(\mathfrak{D}/\mathfrak{p}_i^{\alpha_i})^r/G|.$$

Esta é uma consequência do teorema chinês do resto. Portanto, é suficiente contar o número de órbitas para o caso em que o ideal $\mathfrak{n}$ é uma potência de um ideal primo não nulo.

Então, assumamos que $\mathfrak{n} = \mathfrak{p}^\alpha$ onde $\mathfrak{p}$ é um ideal primo não nulo de $\mathfrak{D}$ e α é um número inteiro positivo. Seja a um gerador fixo do ideal maximal $\mathfrak{p}/\mathfrak{p}^\alpha$ do anel local $\mathfrak{D}/\mathfrak{p}^\alpha$. Analisemos a órbita de um elemento $(a_1, \ldots, a_r) \in (\mathfrak{D}/\mathfrak{p}^\alpha)^r$. As últimas $r - 1$ coordenadas são fixadas por qualquer

elemento $g(t_1,\ldots,t_r)\in G$ e o primeiro percorre o conjunto

$$L=\{t_1a_1+t_2a_2+\cdots+t_ra_r\ :\ t_1\in U(\mathfrak{D}/\mathfrak{p}^\alpha),\ \text{e}\ t_2,\ldots,t_r\in\mathfrak{D}/\mathfrak{p}^\alpha\}\,.$$

Notemos que $L=U(\mathfrak{D}/\mathfrak{p}^\alpha)a^{w(a_1)}+\langle a_2,\ldots,a_r\rangle$ se $a_1\neq 0$, e $L=\langle a_2,\ldots,a_r\rangle$, caso contrário. Primeiro, assumamos que o ideal $\langle a_2,\ldots,a_r\rangle$ é não nulo, isto é, $\langle a_2,\ldots,a_r\rangle=\langle a^\beta\rangle$ para um número inteiro fixo $0\leq\beta\leq\alpha-1$. De acordo com o Lema 4.2.12, para este caso as órbitas distintas são

$$\begin{aligned}
O_0&=\{(z_1,a_2,\ldots,a_r)\ :\ w(z_1)=0\};\\
O_1&=\{(z_1,a_2,\ldots,a_r)\ :\ w(z_1)=1\};\\
O_2&=\{(z_1,a_2,\ldots,a_r)\ :\ w(z_1)=2\};\\
&\vdots\\
O_{\beta-1}&=\{(z_1,a_2,\ldots,a_r)\ :\ w(z_1)=\beta-1\};\\
O_\beta&=\{(z_1,a_2,\ldots,a_r)\ :\ w(z_1)\geq\beta\}.
\end{aligned}$$

Desta maneira, pelo Lema 4.2.13 concluímos que o número de órbitas em que todos os elementos $(x_1,\ldots,x_r)$ satisfazem $\langle x_2,\ldots,x_r\rangle=\langle a^\beta\rangle$ é dado por

$$(\beta+1)\left(N(\mathfrak{p}^{\alpha-\beta})^{r-1}-N(\mathfrak{p}^{\alpha-\beta-1})^{r-1}\right).$$

Somando todos os valores possíveis de β obtemos para o número de órbitas quando o ideal $\langle a_2,\ldots,a_r\rangle$ é não nulo

$$\sum_{\beta=0}^{\alpha-1}(\beta+1)\left(N(\mathfrak{p}^{\alpha-\beta})^{r-1}-N(\mathfrak{p}^{\alpha-\beta-1})^{r-1}\right)=N(\mathfrak{p}^\alpha)^{r-1}+N(\mathfrak{p}^{\alpha-1})^{r-1}+\cdots+N(\mathfrak{p})^{r-1}-\alpha.$$

Quando $\langle a_2,\ldots,a_r\rangle$ é o ideal nulo, todos a_i, para $i=2,\ldots,r$, são nulos, e se

$$g(t_1,\ldots,t_r)(a_1,0,\ldots,0)=(a_1',0,\ldots,0),$$

então, $w(a_1)=w(a_1')$. Consequentemente, tendo em conta a partição (4.33) existem $\alpha+1$ órbitas deste tipo. Assim, o número total de órbitas é

$$|(\mathfrak{D}/\mathfrak{p}^\alpha)^r/G|=\sum_{\beta=0}^{\alpha}N(\mathfrak{p}^{\alpha-\beta})^{r-1}=\sigma_{r-1\mathfrak{D}}(\mathfrak{p}^\alpha).$$

Segue-se da propriedade multiplicativa que para um ideal não nulo $\mathfrak{n}$ o número de órbitas $|(\mathfrak{D}/\mathfrak{n})^r/G|$ é igual a $\sigma_{r-1\mathfrak{D}}(\mathfrak{n})$.

Finalmente, uma vez que o grupo G tem ordem $\varphi_{\mathfrak{D}}(\mathfrak{n})N(\mathfrak{n})^{r-1}$ e a ordem do conjunto fixo de um elemento do grupo $g(t_1,\ldots,t_r)$ é

$$N(\mathfrak{n})^{r-1}N(\langle t_1-1,t_2\ldots,t_r\rangle+\mathfrak{n}),$$

pelo lema de Burnside temos a equação (4.26) como requerido.

■

4.3 Identidades do tipo Menon com carateres de Dirichlet

Nesta secção vamos apresentar o trabalho de Xiao-Peng Zhao e Zhen-Fu Cao [27] sobre identidades de Menon usando carateres de Dirichlet.

Antes de passarmos ao enunciado e as provas das identidades vamos estabelecer alguns resultados sobre carateres de Dirichlet.

Lema 4.3.1. *Seja χ um caráter de Dirichlet primitivo $(mod\, p^n)$, onde p é primo e n é um inteiro positivo. Se m é um inteiro positivo e $1 \leq m < n$, temos*

$$\sum_{\substack{k=1 \\ mdc(k,p)=1}}^{p^{n-m}} \chi(kp^m+1) = \begin{cases} 0 & se \quad 1 \leq m < n-1; \\ -1 & se \quad m = n-1. \end{cases}$$

Demonstração. O condutor de um caráter de Dirichlet primitivo $(mod\, p^n)$ é p^n. Primeiro provemos o caso em que $m = n-1$. Existe um inteiro b $(1 \leq b < p)$ tal que $\chi(bp^{n-1}+1) \neq 1$, já que p^{n-1} não é um módulo induzido para χ. Note que neste caso temos necessariamente $n > 1$. Portanto, $mdc(bp^{n-1}+1, p^n) = 1$. Temos, então,

$$\chi(bp^{n-1}+1)\sum_{k=0}^{p-1}\chi(kp^{n-1}+1) = \sum_{k=0}^{p-1}\chi((k+b)p^{n-1}+1) = \sum_{k=0}^{p-1}\chi(kp^{n-1}+1).$$

Portanto, temos

$$\sum_{k=0}^{p-1}\chi(kp^{n-1}+1) = 0$$

uma vez que $\chi(bp^{n-1}+1) \neq 1$. Concluímos, então, que

$$\sum_{\substack{k=1 \\ mdc(k,p)=1}}^{p} \chi(kp^{n-1}+1) = -1,$$

tal como queríamos provar.

A prova do caso de $1 \leq m < n-1$ é similar ao caso em que $m = n-1$. Temos

$$\chi(bp^{n-1}+1) \sum_{\substack{k=1 \\ mdc(k,p)=1}}^{p^{n-m}} \chi(kp^m+1) = \sum_{\substack{k=1 \\ mdc(k,p)=1}}^{p^{n-m}} \chi(kp^m+bp^{n-1}+1).$$

Queremos mostrar que $kp^m+bp^{n-1}+1$ onde $1 \leq k \leq p^{n-m}, mdc(k,p) = 1$ constitui o mesmo sistema reduzido de restos $(mod\, p^n)$ como kp^m+1. Suponhamos que $1 \leq k_1 \leq p^{n-m}$, $mdc(k_1,p) = 1$. Se

$$c \equiv k_1p^m + bp^{n-1} + 1 (mod\, p^n),$$

para o inteiro c, então, seja

$$k_2 \equiv k_1 + bp^{n-1-m} (mod\, p^{n-m}),$$

deduzimos que

$$1 \leq k_2 \leq p^{n-m},\ mdc(k_2,p) = 1,\ k_2p^m + 1 \equiv c (mod\, p^n).$$

Se

$$k_1p^m + bp^{n-1} + 1 \equiv k_1'p^m + bp^{n-1} + 1 (mod\, p^n) \quad \text{e} \quad k_2p^m + 1 \equiv k_2'p^m + 1 (mod\, p^n)$$

para os inteiros k_1' e k_2' temos, então,

$$k_1 \equiv k_1'(mod\, p^{n-m}) \qquad \text{e} \qquad k_2 \equiv k_2'(mod\, p^{n-m}).$$

Como ambos os sistemas reduzidos de restos têm $\varphi(p^{n-m})$ elementos diferentes, obtemos o resultado. Por conseguinte, temos que

$$\sum_{\substack{k=1 \\ mdc(k,p)=1}}^{p^{n-m}} \chi(kp^m + bp^{n-1} + 1) = \sum_{\substack{k=1 \\ mdc(k,p)=1}}^{p^{n-m}} \chi(kp^m + 1)$$

Isto prova que a última soma é zero quando $1 \leq m < n-1$, completando a demonstração.

■

Lema 4.3.2. *Seja χ um caráter de Dirichlet primitivo $(mod\, p^n)$, onde p é primo e n é um inteiro positivo. Temos*

$$\sum_{\substack{1 \leq k \leq p^n \\ k \equiv 1\,(mod\, p)}} \chi(k) = \begin{cases} 1 & se \quad n = 1; \\ 0 & se \quad n > 1. \end{cases}$$

Demonstração. O resultado é obviamente verdadeiro para $n = 1$.

Para $n > 1$ temos

$$\sum_{\substack{1 \leq k \leq p^n \\ k \equiv 1\,(mod\, p)}} \chi(k) = \frac{1}{p-1} \sum_{k=1}^{p^n} \chi(k) \left(\sum_{i=1}^{p-1} \psi_i(k) \right) = \frac{1}{p-1} \sum_{i=1}^{p-1} \sum_{k=1}^{p^n} (\chi\psi_i)(k),$$

onde $\psi_1, \ldots, \psi_{p-1}$ são todos os carateres de Dirichlet distintos $(mod\, p)$. Notemos que $\chi\psi_i$ é um carater de Dirichlet $(mod\, p^n)$ e não pode ser principal uma vez que χ é primitivo e ψ_i $(1 \leq i \leq p-1)$ não é primitivo como um caráter $(mod\, p^n)$, onde $n > 1$. Portanto, a soma é zero para qualquer i $(1 \leq i \leq p-1)$.

■

Lema 4.3.3. *Seja χ um caráter de Dirichlet não principal $(mod\, p^n)$ onde p é um primo e n um inteiro positivo. Seja $p^l (1 \leq l \leq n)$ o condutor de χ. Se m é um inteiro positivo e $1 \leq m < n$, temos*

$$\sum_{\substack{k=1 \\ mdc(k,p)=1}}^{p^{n-m}} \chi(kp^m + 1) = \begin{cases} \varphi(p^{n-m}) & se \quad l \leq m < n; \\ -p^{n-l} & se \quad m = l-1; \\ 0 & se \quad 1 \leq m < l-1. \end{cases}$$

Demonstração. O caso em que $l \leq m < n$ é evidente. Por outro lado, para $1 \leq m < l-1$, seja ψ um caráter primitivo módulo o condutor de χ e χ_1 o caráter principal $(mod\, p^n)$. Considerando o Lema 4.3.1 e o Teorema 2.3.10 temos

$$\sum_{\substack{k=1 \\ mdc(k,p)=1}}^{p^{n-m}} \chi(kp^m + 1) = p^{n-l} \sum_{\substack{k=1 \\ mdc(k,p)=1}}^{p^{l-m}} \psi(kp^m + 1)\chi_1(kp^m + 1)$$

$$= p^{n-l} \sum_{\substack{k=1 \\ mdc(k,p)=1}}^{p^{l-m}} \psi(kp^m + 1)$$

$$= \begin{cases} -p^{n-l} & se \quad m = l-1; \\ 0 & se \quad 1 \leq m < l-1. \end{cases}$$

■

Lema 4.3.4. *Usando a notação do Lema 4.3.3 temos*

$$\sum_{\substack{1 \leq k \leq p^n \\ k \equiv 1 \, (mod\, p)}} \chi(k) = \begin{cases} p^{n-1} & se \quad p \quad é \quad o \quad condutor \quad de \quad \chi; \\ 0 & caso \quad contrário. \end{cases}$$

Demonstração. Pela demonstração do Lema 4.3.3 obtemos

$$\sum_{\substack{1 \leq k \leq p^n \\ k \equiv 1 \, (mod\, p)}} \chi(k) = p^{n-l} \sum_{\substack{1 \leq k \leq p^l \\ k \equiv 1 \, (mod\, p)}} \psi(k)\chi_1(k) = p^{n-l} \sum_{\substack{1 \leq k \leq p^l \\ k \equiv 1 \, (mod\, p)}} \psi(k).$$

Pelo Lema 4.3.2 a demonstração está completa.

■

Depois de apresentarmos e provarmos os quatro lemas desta secção estamos em melhores condições de enunciarmos e demonstrarmos os teoremas que se seguem.

Teorema 4.3.5. *Seja χ um caráter de Dirichlet primitivo $(mod\ n)$. Então, temos a identidade seguinte*

$$\sum_{\substack{k=1 \\ mdc(k,n)=1}}^{n} mdc(k-1, n)\chi(k) = \varphi(n). \quad (4.34)$$

Demonstração. Definamos

$$f(n) = \sum_{\substack{k=1 \\ mdc(k,n)=1}}^{n} mdc(k-1, n)\chi_n(k)$$

onde χ_n é algum caráter $(mod\, n)$. Para $s, t \in \mathbb{N}$ tal que $mdc(s,t) = 1$, temos

$$\begin{aligned} f(st) &= \sum_{\substack{k=1 \\ mdc(k,st)=1}}^{st} mdc(k-1, st)\chi_{st}(k) \\ &= \sum_{\substack{k_1=1 \\ mdc(k_1,s)=1}}^{s} \sum_{\substack{k_2=1 \\ mdc(k_2,t)=1}}^{t} mdc(k_1t + k_2s - 1, st)\chi_s(k_1t + k_2s)\chi_t(k_1t + k_2s) \\ &= \sum_{\substack{k_1=1 \\ mdc(k_1,s)=1}}^{s} \sum_{\substack{k_2=1 \\ mdc(k_2,t)=1}}^{t} mdc(k_1t - 1, s)mdc(k_2s - 1, t)\chi_s(k_1t)\chi_t(k_2s) \\ &= \sum_{\substack{k_1=1 \\ mdc(k_1,s)=1}}^{s} mdc(k_1t - 1, s)\chi_s(k_1t) \sum_{\substack{k_2=1 \\ mdc(k_2,t)=1}}^{t} mdc(k_2s - 1, t)\chi_t(k_2s) \\ &= f(s)f(t). \end{aligned}$$

Portanto, a função aritmética f é multiplicativa. Notemos que qualquer carácter $\chi \pmod k$ pode ser fatorizado de forma única como um produto da forma $\chi = \chi_{k_1}\chi_{k_2}\cdots\chi_{k_r}$, onde $k = k_1k_2\cdots k_r$ para os primos relativos dois a dois: $mdc(k_i, k_j) = 1$ se $i \neq j$. Se χ é um caráter primitivo, cada χ_{k_i} é um caráter primitivo $(mod\, k_i)$. Se obtivermos a equação $f(p^a) = \varphi(p^a)$ para qualquer p^a onde p é um primo e a é um inteiro positivo, a prova está feita. Mas isto é verdade porque

$$\begin{aligned} f(p^a) &= \sum_{\substack{k=1 \\ mdc(k,p^a)=1}}^{p^a} mdc(k-1,p^a)\chi_{p^a}(k) = \sum_{k=1}^{p^a} mdc(k-1,p^a)\chi_{p^a}(k) \\ &= \sum_{\substack{k=1 \\ mdc(k-1,p^a)\neq 1}}^{p^k} mdc(k-1,p^a)\chi_{p^a}(k) + \sum_{\substack{k=1 \\ mdc(k-1,p^a)=1}}^{p^a} \chi_{p^a}(k) \\ &= \sum_{m=1}^{a} \sum_{\substack{k=1 \\ mdc(k-1,p^a)=p^m}}^{p^a} p^m\chi_{p^a}(k) + \sum_{k=1}^{p^a}\chi_{p^a}(k) - \sum_{\substack{k=1 \\ k\equiv 1 \,(mod\, p)}}^{p^a} \chi_{p^a}(k) \\ &= p^a + \sum_{m=1}^{a-1} p^m \sum_{\substack{j=1 \\ mdc(j,p)=1}}^{p^{a-m}} \chi_{p^a}(jp^m+1) + 0 - \sum_{\substack{k=1 \\ k\equiv 1 \,(mod\, p)}}^{p^a} \chi_{p^a}(k). \end{aligned}$$

Pelos Lemas 4.3.1 e 4.3.2 obtemos

$$p^a + \sum_{m=1}^{a-1} p^m \sum_{\substack{j=1 \\ mdc(j,p)=1}}^{p^{a-m}} \chi_{p^a}(jp^m+1) + \sum_{\substack{k=1 \\ k\equiv 1 \,(mod\, p)}}^{p^a} \chi_{p^a}(k) = p^a - p^{a-1} = \varphi(p^a).$$

o que completa a demonstração.

■

Antes de enunciarmos e demonstrarmos o próximo teorema apresentemos primeiramente o lema seguinte.

Lema 4.3.6. *Seja χ o caráter de Dirichlet $(mod\, p^a)$ onde p é um primo e a é um inteiro positivo. Se $p^l (0 \leq l \leq a)$ é o condutor de χ, então temos a identidade*

$$\sum_{\substack{k=1 \\ mdc(k,p^a)=1}}^{p^a} mdc(k-1,p^a)\chi(k) = (a-l+1)\varphi(p^a).$$

Demonstração. Para $l = 0$ é equivalente a χ ser o caráter principal e $l = a$, implica que χ é um caráter primitivo. Em ambos os casos a identidade é satisfeita. De acordo com a demonstração do Teorema 4.3.5, se p é o condutor de χ, facilmente obtemos

$$\sum_{\substack{k=1 \\ mdc(k,p^a)=1}}^{p^a} mdc(k-1,p^a)\chi(k) = a\varphi(p^a).$$

Para os demais casos, pelos Lemas 4.3.3 e 4.3.4 temos

$$\sum_{\substack{k=1\\ mdc(k,p^a)=1}}^{p^a} mdc(k-1,p^a)\chi(k) = p^a + \sum_{m=1}^{a-1} p^m \sum_{\substack{j=1\\ mdc(j,p)=1}}^{p^{a-m}} \chi(jp^m+1) - \sum_{\substack{k=1\\ k\equiv 1 (mod\, p)}}^{p^a} \chi(k)$$

$$= p^a + 0 - p^{l-1}p^{a-l} + \sum_{m=l}^{a-1} p^m \varphi(p^{a-m}) - 0$$

$$= p^a - p^{a-1} + (a-l)(p^a - p^{a-1})$$

$$= (a-l+1)\varphi(p^a).$$

■

Agora estamos em melhores condições de apresentarmos o resultado que generaliza o Teorema 4.3.5.

Teorema 4.3.7. *Seja $n \in \mathbb{N}$ e seja χ um caráter de Dirichlet (mod n) com condutor d. Então,*

$$\sum_{\substack{k=1\\ mdc(k,n)=1}}^{n} mdc(k-1,n)\chi(k) = \varphi(n)\sigma\left(\frac{n}{d}\right). \quad (4.35)$$

Observação. Notemos que se χ é o caráter principal módulo n então a identidade (4.35) reduz-se a (4.34) (o caso em que $d = 1$).

Demonstração. Sejam

$$n = \prod_{i=1}^{r} p_i^{a_i} \quad \text{e} \quad d = \prod_{i=1}^{r} p_i^{b_i} \ (0 \le b_i \le a_i)$$

do Teorema 4.3.5 respetivamente. Consideremos que $\chi = \chi_{p_1}\chi_{p_2}\cdots\chi_{p_r}$ e $g(\chi_{p_i})$ denotam o condutor de χ_{p_i}, podemos concluir que

$$g(\chi) = g(\chi_{p_1})g(\chi_{p_2})\cdots g(\chi_{p_r}) \quad \text{e} \quad g(\chi_{p_i}) = p_i^{b_i} \ (1 \le i \le r).$$

Notemos que a função

$$f(n) = \sum_{\substack{k=1\\ mdc(k,n)=1}}^{n} mdc(k-1,n)\chi(k)$$

é multiplicativa para qualquer caráter de Dirichlet χ $(mod\, n)$. Pelo Lema 4.3.6 temos

$$\sum_{\substack{k=1\\ mdc(k,n)=1}}^{n} mdc(k-1,n)\chi(k) = \prod_{i=1}^{r} \left(\sum_{\substack{k=1\\ mdc(k,p_i^{a_i})=1}}^{n} mdc(k-1,p_i^{a_i})\chi_{k_i}(k) \right)$$

$$= \prod_{i=1}^{r} (a_i - b_i + 1)\varphi(n) = \varphi(n)\sigma\left(\frac{n}{d}\right).$$

o que completa a demonstração.

■

De seguida, usando o produto de Dirichlet definido na Secção 1.3, apresentamos uma identidade provada em [26].

Teorema 4.3.8. *Seja F uma função aritmética arbitrária, seja $s_j \in \mathbb{Z}$, sejam χ_j carateres de Dirichlet (mod n) com condutores $d_j (1 \leq j \leq m)$ e λ_l os carateres aditivos $b \to \lambda_l(b) = exp(2\pi i w_l b/n)$ do grupo $\mathbb{Z}_n$ com $0 \leq w_l \leq n-1, w_l \in \mathbb{Z}\,(1 \leq l \leq k)$ onde $b \in \mathbb{Z}_n$. Então,*

$$\sum_{a_1,\ldots,a_m,b_1,\ldots,b_k=1}^{n} F(mdc(a_1-s_1,\ldots,a_m-s_m,b_1,\ldots,b_k,n))\chi_1(a_1)\cdots\chi_m(a_m)\lambda_1(b_1)\cdots\lambda_k(b_k) =$$

$$= \varphi(n)^m \chi_1^*(s_1)\cdots\chi_m^*(s_m) \sum_{\substack{e \mid mdc(n/d_1,\ldots,n/d_m,w_1,\ldots,w_k) \\ mdc(n/e,s_1\cdots s_m)=1}} \frac{e^k (u*F)(n/e)}{\varphi(n/e)^m}, \quad (4.36)$$

onde χ_j^* são carateres primitivos (mod d_j) induzidos por χ_j $(1 \leq j \leq m)$.

Notemos que se existe um s_j tal que $mdc(s_j, d_j) > 1$ então a soma à esquerda da identidade (4.36) anula-se.

Para provarmos o Teorema 4.3.8 precisamos dos três lemas seguintes.

Lema 4.3.9. *Sejam $n, d, e \in \mathbb{N}, d \mid n, e \mid n$ e sejam $r, s \in \mathbb{Z}$. Então,*

$$\sum_{\substack{a=1 \\ mdc(a,n)=1 \\ a \equiv r\,(mod\,d) \\ a \equiv s\,(mod\,e)}}^{n} 1 = \begin{cases} \frac{\varphi(n)}{\varphi(de)} mdc(d,e) & \text{se } mdc(r,d) = mdc(s,e) = 1 \quad e \quad mdc(d,e) \mid r-s, \\ 0 & \text{caso contrário.} \end{cases}$$

O caso especial em que $e = 1$ é bem conhecido na literatura, frequentemente provado pelo princípio da inclusão-exclusão [2, Teorema 5.32, p. 124]. Vamos fazer uma abordagem diferente.

Demonstração. Para cada termo da soma, já que $mdc(a, n) = 1$, temos $mdc(r, d) = mdc(a, d) = 1$ e $mdc(s, e) = mdc(a, e) = 1$. De igual forma, as congruências dadas implicam $mdc(d, e) \mid r - s$. Assumamos que essas condições são satisfeitas (caso contrário a soma é vazia e igual a zero).

Usando as propriedades da função de Möbius apresentadas da Secção 1.3, a soma dada, digamos S, pode ser escrita como

$$S = \sum_{\substack{a=1 \\ a \equiv r\,(mod\,d) \\ a \equiv s\,(mod\,e)}}^{n} \sum_{\delta \mid mdc(a,n)} \mu(\delta) = \sum_{\delta \mid n} \mu(\delta) \sum_{\substack{j=1 \\ \delta j \equiv r\,(mod\,d) \\ \delta j \equiv s\,(mod\,e)}}^{n/\delta} 1. \quad (4.37)$$

Seja $\delta \mid n$ fixo. A congruência linear $\delta j \equiv r\,(mod\,d)$ tem soluções em j se, e somente se, $mdc(\delta, n) \mid r$, o que quer dizer que $mdc(\delta, n) = 1$, pois $mdc(r, d) = 1$. De modo similar, a congruência $\delta j \equiv s\,(mod\,e)$ tem soluções em j se, e somente se, $mdc(\delta, e) \mid s$, o que significa que $mdc(\delta, e) = 1$, uma vez que $mdc(s, e) = 1$. Estas duas congruências têm soluções comuns em j devido a condição $mdc(d, e) \mid r - s$. Além disso, se j_1 e j_2 são soluções simultâneas destas congruências, então $\delta j_1 \equiv \delta j_2 (mod\,d)$ e $\delta j_1 \equiv \delta j_2 (mod\,e)$. Visto que $mdc(\delta, d) = 1$, obtemos $j_1 \equiv j_2 (mod\,mmc(d, e))$. Deduzimos que existem

$$N = \frac{n}{\delta\, mmc(d,e)}$$

soluções $(mod\, n/\delta)$ e a soma em (4.37) é N. Isto nos dá

$$S = \frac{n}{\delta\, mmc(d,e)} \sum_{\substack{d|n \\ mdc(\delta,de)=1}} \frac{\mu(\delta)}{\delta} = \frac{n}{mmc(d,e)} \times \frac{\varphi(n)/n}{\varphi(de)/(de)} = \frac{\varphi(n)}{\varphi(de)} mdc(d,e).$$

■

Lema 4.3.10. *Seja $n \in \mathbb{N}$ e χ um caráter primitivo $(mod\, n)$. Então para qualquer $e \mid n$, $e < n$ e qualquer $s \in \mathbb{Z}$,*

$$\sum_{\substack{a=1 \\ a \equiv s (mod\, e)}}^{n} \chi(a) = 0.$$

Demonstração. Uma vez que χ é um caráter primitivo, para um dado $e \mid n$, $e < n$ existe $c \in \mathbb{Z}$ tal que $mdc(c,n) = 1, c \equiv 1\,(mod\, e)$ e $\chi(c) \neq 1$. Temos

$$S := \sum_{\substack{a=1 \\ a \equiv s (mod\, e)}}^{n} \chi(a) = \sum_{t\,(mod\, n/e)} \chi(s + te).$$

Agora, já que $mdc(c,n) = 1$, como t percorre uma classe completa de resíduos $(mod\, n/e)$, os números $j = cs + tce$ percorrem também uma classe completa de resíduos $(mod\, n)$, onde $j \equiv cs \equiv s\,(mod\, e)$. Portanto,

$$S = \sum_{t\,(mod\, n/e)} \chi(cs + tce) = \chi(c) \sum_{t\,(mod\, n/e)} \chi(s + te) = \chi(c) S.$$

Visto que $\chi(c) \neq 1$, resulta que $S = 0$.

■

Lema 4.3.11. *Seja χ um caráter de Dirichlet $(mod\, n)$ com condutor d $(n \in \mathbb{N}, d \mid n)$ e seja $e \mid n, s \in \mathbb{Z}$. Então,*

$$\sum_{\substack{a=1 \\ a \equiv s (mod\, e)}}^{n} \chi(a) = \begin{cases} \frac{\varphi(n)}{\varphi(e)} \chi^*(s) & \text{se } d \mid e \quad e \quad mdc(s,e) = 1, \\ 0 & \text{caso contrário,} \end{cases}$$

onde χ^* é o caráter primitivo $(mod\, d)$ que induz χ.

Demonstração. Nesta soma podemos assumir que $mdc(a,n) = 1$. Se $a \equiv s\,(mod\, e)$, então $mdc(s,e) = mdc(a,e) = 1$. Dado o caráter de Dirichlet $\chi\,(mod\, n)$, o caráter primitivo $\chi^*\,(mod\, d)$ que induz χ é definido por

$$\chi(a) = \begin{cases} \chi^*(a) & \text{se } mdc(a,n) = 1, \\ 0 & \text{se } mdc(a,n) > 1. \end{cases}$$

Temos que

$$T := \sum_{\substack{a=1 \\ a \equiv s\,(mod\, e)}}^{n} \chi(a) = \sum_{\substack{a=1 \\ mdc(a,n)=1 \\ a \equiv s\,(mod\, e)}}^{n} \chi^*(a) = \sum_{r=1}^{d} \chi^*(r) \sum_{\substack{a=1 \\ mdc(a,n)=1 \\ a \equiv r\,(mod\, d) \\ a \equiv s\,(mod\, e)}}^{n} 1,$$

a soma

$$\sum_{\substack{a=1\\ mdc(a,n)=1\\ a\equiv r\,(mod\,d)\\ a\equiv s\,(mod\,e)}}^{n} 1$$

é calculada no Lema 4.3.9. Como $mdc(s,e)=1$, segue que

$$T=\sum_{\substack{r=1\\ mdc(r,d)=1\\ mdc(d,e)|r-s}}^{d}\chi^*(r)\frac{\varphi(n)}{\varphi(de)}mdc(d,e)=\frac{\varphi(n)}{\varphi(de)}mdc(d,e)\sum_{\substack{r=1\\ mdc(r,d)=1\\ r\equiv s\,(mod\,mdc(d,e))}}^{d}\chi^*(r)=\frac{\varphi(n)}{\varphi(de)}mdc(d,e)\chi^*(s),$$

pelo Lema 4.3.10, no caso em que $mdc(d,e)=d$, isto é $d\mid e$. Concluímos que

$$T=\frac{\varphi(n)}{\varphi(de)}d\chi^*(s)=\frac{\varphi(n)}{\varphi(e)}\chi^*(s).$$

Se $d\nmid e$, então $T=0$.

■

Demonstração. (do **Teorema 4.3.8**) Denotemos por V a soma dada. Usando a identidade $F(n)=\sum_{e|n}(\mu*F)(e)$, que é uma consequência da fórmula da inversão de Möbius (1.12), temos

$$V=\sum_{a_1,\ldots,a_m,b_1,\ldots,b_k=1}^{n}\chi_1(a_1)\cdots\chi_m(a_m)\lambda_1(b_1)\cdots\lambda_k(b_k)\sum_{e|mdc(a_1-s_1,\ldots,a_m-s_m,b_1,\ldots,b_k,n)}(\mu*F)(e)$$

$$=\sum_{e|n}(\mu*F)(e)\sum_{\substack{a_1=1\\ a_1\equiv s_1\,(mod\,e)}}^{n}\chi_1(a_1)\cdots\sum_{\substack{a_m=1\\ a_m\equiv s_m\,(mod\,e)}}^{n}\chi_m(a_m)\sum_{\substack{b_1=1\\ e|b_1}}^{n}\lambda_1(b_1)\cdots\sum_{\substack{b_k=1\\ e|b_k}}^{n}\lambda_k(b_k).$$

onde para todo $1\le l\le k$,

$$\sum_{\substack{b_l=1\\ e|b_l}}^{n}\lambda_l(b_l)=\sum_{c_l=1}^{n/e}\exp(2\pi i w_l c_l/(n/e))=\begin{cases}\frac{n}{e} & \text{se } \frac{n}{e}\mid w_l,\\ 0 & \text{caso contrário,}\end{cases}$$

usando o Lema 4.3.11 deduzimos que

$$V=\chi_1^*(s_1)\cdots\chi_m^*(s_m)\sum{}'(\mu*F)(e)\left(\frac{\varphi(n)}{\varphi(e)}\right)^m\left(\frac{n}{e}\right)^k,$$

onde a soma $\sum'$ é sobre $e\mid n$ tal que $d_j\mid e$, $mdc(e,s_j)=1$ para todo $1\le j\le m$ e $n/e\mid w_l$ para todo $1\le l\le k$. Trocando e e n/e, a soma é sobre e tal que $e\mid n/d_j$, $mdc(n/e,s_j)=1$ para todo $1\le j\le m$ e $e\mid w_l$ para todo $1\le l\le k$. Isto completa a demonstração.

■

4.4 Identidades do tipo Menon com relação a conjuntos de unidades

Até agora o somatório nas identidades do tipo Menon tem sido sobre todas as unidades do anel $\mathbb{Z}_n$, ou todas as unidades do anel $\mathfrak{D}/\mathfrak{n}$ no caso das identidades do tipo Menon nos domínios de Dedekind residualmente finitos. O facto de este conjunto de unidades ter estrutura de grupo abeliano permitiu o uso de algumas ferramentas da teoria dos grupos como, por exemplo, o Lema de Burnside.

Nesta secção apresentamos o nosso trabalho [5] e vamos estender as identidades do tipo Menon numa nova direção. Vamos considerar o caso em que o somatório não é sobre todas as unidades de $\mathbb{Z}_n$ ou $\mathfrak{D}/\mathfrak{n}$, mas sim sobre um subconjunto S não vazio de unidades. Ao considerarmos um subconjunto do grupo das unidades $\mathbb{Z}_n^*$ este pode ser ou não ser subgrupo de $\mathbb{Z}_n^*$. Este facto vai ter importância para o estabelecimento das identidades. No caso em que o subconjunto S não tem estrutura de subgrupo não podemos fazer o uso dos resultados da teoria dos grupos. Na verdade, no caso em que o subconjunto S de $\mathbb{Z}_n^*$ tem a estrutura de subgrupo podemos simplificar a identidade obtida.

Assumamos que no Teorema 4.3.8 temos $F(n) = n$, para todo $n \in \mathbb{N}$, $w_1 = \cdots = w_k = 0$ e para todo i cada s_i é uma unidade u_i. Então, usando a Fórmula (1.11) obtemos para $k \geq 0$ e $u_1, \ldots, u_m \in \mathbb{Z}_n^*$ a fórmula

$$\sum_{\substack{a_1,\ldots,a_m \in \mathbb{Z}_n^* \\ b_1,\ldots,b_k \in \mathbb{Z}_n}} mdc(a_1 - u_1, \ldots, a_m - u_m, b_1, \ldots, b_k, n)\chi_1(a_1)\cdots\chi_m(a_m) =$$

$$= \varphi(n)^m \chi_1^*(u_1)\cdots\chi_m^*(u_m)G(mdc(n/d_1, \ldots, n/d_m)), \quad (4.38)$$

onde χ_j são os carateres de Dirichlet com condutores d_j $(1 \leq j \leq m)$, χ_j^* são carateres primitivos $(mod\, d_j)$ que são induzidos por χ_j e

$$G(t) = \sum_{\delta | t} \delta^k \varphi(n/\delta)^{1-m}. \quad (4.39)$$

Agora, recorrendo à relação de ortogonalidade (2.2) vamos expressar a função indicadora de um subconjunto não vazio S de um grupo abeliano finito G em termos de carateres. Isto vai permitir restringir o somatório nas identidades de Menon ao conjunto S.

Seja G um grupo abeliano finito e seja $\widehat{G}$ o grupo de carateres de G. Se definirmos a função δ_g de G para $\{0, 1\}$ por

$$\delta_g(x) = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \overline{\chi}(g)\chi(x) \quad (4.40)$$

temos que $\delta_g(x) = 1$ se $x = g$ e 0, caso contrário. Assim sendo, para um subconjunto não vazio S

de um grupo abeliano finito G, seja

$$\delta_S(x) = \sum_{s \in S} \delta_s(x). \quad (4.41)$$

É claro que $\delta_S(x) = 1$ se $x \in S$ e 0, caso contrário.

Estamos agora em condições de provar uma identidade do tipo Menon onde o somatório não é sobre todo o grupo de unidades, mas apenas sobre um subconjunto não vazio de unidades.

Teorema 4.4.1. *Sejam $m, n \geq 1$ números inteiros positivos, $u_1, \ldots, u_m \in \mathbb{Z}_n^*$ e $S_1, \ldots, S_m$ subconjuntos não vazios de unidades de $\mathbb{Z}_n^*$. Se $k \geq 0, m + k \geq 1$ e $\widehat{\mathbb{Z}_n^*}$ é o grupo de carateres de $\mathbb{Z}_n^*$, então*

$$\sum_{\substack{a_1 \in S_1, \ldots, a_m \in S_m \\ b_1, \ldots, b_k \in \mathbb{Z}_n}} mdc(a_1 - u_1, \ldots, a_m - u_m, b_1, \ldots, b_k, n) =$$

$$= \sum_{\substack{x_1 \in S_1, \ldots, x_m \in S_m \\ \chi_1, \ldots, \chi_m \in \widehat{\mathbb{Z}_n^*}}} \overline{\chi}_1(x_1) \cdots \overline{\chi}_m(x_m) \chi_1^*(u_1) \cdots \chi_m^*(u_m) G(mdc(n/d_1, \ldots, n/d_m)),$$

onde d_i é o condutor do caráter χ_i e G é a função (4.39).

Demonstração. Podemos escrever

$$\sum_{\substack{a_1 \in S_1, \ldots, a_m \in S_m \\ b_1, \ldots, b_k \in \mathbb{Z}_n}} mdc(a_1 - u_1, \ldots, a_m - u_m, b_1, \ldots, b_k, n) =$$

$$= \sum_{\substack{a_1, \ldots, a_m \in \mathbb{Z}_n^* \\ b_1, \ldots, b_k \in \mathbb{Z}_n}} \delta_{S_1}(a_1) \delta_{S_2}(a_2) \cdots \delta_{S_m}(a_m) mdc(a_1 - u_1, \ldots, a_m - u_m, b_1, \ldots, b_k, n). \quad (4.42)$$

Por outro lado, tendo em consideração (4.40) e (4.41) temos

$$\delta_{S_1}(a_1) \cdots \delta_{S_m}(a_m) = \sum_{x_1 \in S_1, \ldots, x_m \in S_m} \delta_{x_1}(a_1) \cdots \delta_{x_m}(a_m) =$$

$$= \frac{1}{|\mathbb{Z}_n^*|^m} \sum_{\substack{x_1 \in S_1, \ldots, x_m \in S_m \\ \chi_1, \ldots, \chi_m \in \widehat{\mathbb{Z}_n^*}}} \overline{\chi}_1(x_1) \cdots \overline{\chi}_m(x_m) \chi_1(a_1) \cdots \chi_m(a_m).$$

Consequentemente, o membro direito de (4.42) pode ser expandido como

$$\frac{1}{|\mathbb{Z}_n^*|^m} \sum_{\substack{a_1, \ldots, a_m \in \mathbb{Z}_n^* \\ b_1, \ldots, b_k \in \mathbb{Z}_n}} \sum_{\substack{x_1 \in S_1, \ldots, x_m \in S_m \\ \chi_1, \ldots, \chi_m \in \widehat{\mathbb{Z}_n^*}}} \overline{\chi}_1(x_1) \cdots \overline{\chi}_m(x_m) \chi_1(a_1) \cdots \chi_m(a_m) \times$$

$$\times mdc(a_1 - u_1, \ldots, a_m - u_m, b_1, \ldots, b_k, n). \quad (4.43)$$

Mudando a ordem dos somatórios podemos escrever (4.43) como

$$\frac{1}{|\mathbb{Z}_n^*|^m} \sum_{\substack{x_1 \in S_1, \ldots, x_m \in S_m \\ \chi_1, \ldots, \chi_m \in \widehat{\mathbb{Z}_n^*}}} \overline{\chi}_1(x_1) \cdots \overline{\chi}_m(x_m) \sum_{\substack{a_1, \ldots, a_m \in \mathbb{Z}_n^* \\ b_1, \ldots, b_k \in \mathbb{Z}_n}} \chi_1(a_1) \cdots \chi_m(a_m) \times$$

$$\times mdc(a_1 - u_1, \ldots, a_m - u_m, b_1, \ldots, b_k, n).$$

Finalmente, aplicando (4.38), obtemos a igualdade

$$\sum_{\substack{a_1 \in S_1, \ldots, a_m \in S_m \\ b_1, \ldots, b_k \in \mathbb{Z}_n}} mdc(a_1 - u_1, \ldots, a_m - u_m, b_1, \ldots, b_k, n) =$$

$$= \sum_{\substack{x_1 \in S_1, \ldots, x_m \in S_m \\ \chi_1, \ldots, \chi_m \in \widehat{\mathbb{Z}_n^*}}} \overline{\chi}_1(x_1) \ldots \overline{\chi}_m(x_m) \chi_1^*(u_1) \cdots \chi_m^*(u_m) G(mdc(n/d_1, \ldots, n/d_m)),$$

como declarado.

■

Para o caso especial em que cada subconjunto S_i, para $i = 1, \ldots, m$, tem a estrutura de subgrupo de $\mathbb{Z}_n^*$ provamos o seguinte:

Corolário 4.4.2. *Sejam $m, n \geq 1$ números inteiros positivos e $u_1, \ldots, u_m \in \mathbb{Z}_n^*$. Sejam $S_1, \ldots, S_m$ subgrupos do grupo de unidades $\mathbb{Z}_n^*$ e denotemos por $\widehat{\mathbb{Z}_{n\,S_i}^*}$ o conjunto de carateres de $\mathbb{Z}_n^*$ cujos núcleos contêm S_i. Se $k \geq 0$ e $m + k \geq 1$, então*

$$\sum_{\substack{a_1 \in S_1, \ldots, a_m \in S_m \\ b_1, \ldots, b_k \in \mathbb{Z}_n}} mdc(a_1 - u_1, \ldots, a_m - u_m, b_1, \ldots, b_k, n) =$$

$$= \sum_{\chi_1 \in \widehat{\mathbb{Z}_{n\,S_1}^*}, \ldots, \chi_m \in \widehat{\mathbb{Z}_{n\,S_m}^*}} |S_1| \cdots |S_m| \chi_1^*(u_1) \cdots \chi_m^*(u_m) G(mdc(n/d_1, \ldots, n/d_m)). \quad (4.44)$$

Demonstração. Para o subgrupo H do grupo abeliano finito G seja $\widehat{G}_H$ o conjunto de carateres de G cujos núcleos contêm H, isto é, elementos de $\widehat{G}$ que fazem corresponder todo $h \in H$ a identidade 1. É fácil demonstrar que $\widehat{G}_H$ é um subgrupo de $\widehat{G}$ [11, p. 40]. Por outro lado, resulta do Teorema 2.2.2 que

$$\sum_{s \in H} \overline{\chi}(s) = \begin{cases} |H| & se\ \overline{\chi} = \chi_0, \\ 0 & \text{caso contrário,} \end{cases} \quad (4.45)$$

onde χ_0 é o caráter principal de H, tal que $\chi_0 \in \widehat{G}_H$.

Agora observemos que o grupo de carateres do produto direto $S_1 \times \cdots \times S_m$ é isomorfo ao produto direto $\widehat{S}_1 \times \cdots \times \widehat{S}_m$. Por conseguinte, se $x_1 \in S_1, \ldots, x_m \in S_m$, então,

$$\sum_{x_1\in S_1,\ldots,x_m\in S_m}\overline{\chi}_1(x_1)\cdots\overline{\chi}_m(x_m)=\begin{cases}|S_1|\cdots|S_m|, & \text{se cada } \chi_i \text{ é}\\ & \text{o caráter principal em } S_i.\\ & \text{Isto é, } \chi_i\in\widehat{\mathbb{Z}^*_{nS_i}},\\ 0, \quad \text{caso contrário.}\end{cases}$$

Portanto, temos

$$\sum_{\substack{x_1\in S_1,\ldots,x_m\in S_m\\ \chi_1,\ldots,\chi_m\in\widehat{\mathbb{Z}^*_n}}}\overline{\chi}_1(x_1)\cdots\overline{\chi}_m(x_m)\chi_1^*(u_1)\cdots\chi_m^*(u_m)G(mdc(n/d_1,\ldots,n/d_m))=$$

$$=\sum_{\chi_1\in\widehat{\mathbb{Z}^*_{nS_1}},\ldots,\chi_m\in\widehat{\mathbb{Z}^*_{nS_m}}}\chi_1^*(u_1)\cdots\chi_m^*(u_m)G(mdc(n/d_1,\ldots,n/d_m))\sum_{x_1\in S_1,\ldots,x_m\in S_m}\overline{\chi}_1(x_1)\cdots\overline{\chi}_m(x_m)=$$

$$=\sum_{\chi_1\in\widehat{\mathbb{Z}^*_{nS_1}},\ldots,\chi_m\in\widehat{\mathbb{Z}^*_{nS_m}}}|S_1|\cdots|S_m|\chi_1^*(u_1)\cdots\chi_m^*(u_m)G(mdc(n/d_1,\ldots,n/d_m)),$$

como declarado.

■

Em [19], num trabalho sobre o número de subgrupos cíclicos de um grupo abeliano finito, Richards provou que se f é um polinómio com coeficientes inteiros então

$$\sum_{t\in\mathbb{Z}_n^*}mdc(f(t),n)=\varphi(n)\sum_{d|n}|\{t\in\mathbb{Z}_d^*:f(t)\equiv 0\,mod\,d\}|. \quad (4.46)$$

Vamos também generalizar a identidade (4.46) para subconjuntos não vazios de $\mathbb{Z}_n^*$.

Teorema 4.4.3. *Seja f qualquer polinómio com coeficientes inteiros, $n\geq 1$ um número inteiro positivo e S um subconjunto não vazio de $\mathbb{Z}_n^*$. Então,*

$$\sum_{t\in S}mdc(f(t),n)=\sum_{d|n}|\{t\in S:f(t)\equiv 0\,mod\,d\}|\varphi(d). \quad (4.47)$$

Demonstração. Se $n\geq 1$, então pela fórmula de Gauss (1.10), obtemos

$$\sum_{t\in S}mdc(f(t),n)=\sum_{t\in S}\sum_{d|mdc(f(t),n)}\varphi(d)=\sum_{t\in S}\sum_{\substack{d|f(t)\\ d|n}}\varphi(d)=\sum_{d|n}\varphi(d)\sum_{\substack{f(t)\equiv 0(mod\,d)\\ t\in S}}1.$$

Isto é exatamente (4.47).

■

Conclusões e Trabalho Futuro

Durante a feitura do nosso trabalho constatámos que para além das generalizações que a identidade de Menon tem sido objeto é igualmente possível estendê-la a domínios de Dedekind residualmente finitos. Ainda verificámos que podemos utilizar os carateres de Dirichlet para estabelecermos essas mesmas identidades.

Diferentemente das generalizações até aqui conhecidas que apontam o somatório das identidades do tipo Menon sobre todas as unidades do anel $\mathbb{Z}_n$, conseguimos direcionar o nosso estudo apenas sobre um subconjunto S não vazio de unidades.

Para trabalho futuro destacamos duas vias:

- Prova de identidades do tipo Menon em domínios de Dedekind residualmente finitos com o somatório restrito a um subconjunto não vazio de unidades;
- Prova de identidades de Menon em domínios de Krull.

No primeiro caso parece-nos que as dificuldades levantadas poderão ser ultrapassadas com técnicas semelhantes às utilizadas para o caso dos inteiros $\mathbb{Z}$. Ou seja, fazendo uso da teoria dos carateres em grupos abelianos finitos. Notemos que para um domínio de Dedekind residualmente finito $\mathfrak{D}$ e um ideal próprio I, o conjunto das unidades do anel fatorial $\mathfrak{D}/I$ é um grupo multiplicativo abeliano e finito. Podemos, assim, fazer uso da teoria de carateres de grupos abelianos finitos, tal como no caso do grupo de unidades de $\mathbb{Z}_n$

O segundo caso, prova da identidade de Menon em domínios de Krull, parece-nos de uma complexidade técnica mais elevada. Os domínios de Krull, estudados pela primeira vez por Wolfgang Krull [10], constituem a classe de anéis mais geral na qual existe uma aritmética semelhante à aritmética nos inteiros racionais. Os domínios de Krull são uma generalização a dimensão (dimensão de Krull) maior do que 1 dos domínios de Dedekind. Um domínio de Krull com dimensão 1 é necessariamente um domínio de Dedekind. Seria interessante estudar identidades do tipo Menon nos domínios de Krull. Um dos maiores obstáculos neste contexto é a existência de ideais que não são finitamente gerados. Na verdade foi provado por I. S. Cohen em [6], que se num domínio de Krull todo o ideal é finitamente gerado então o anel é noetheriano e com dimensão de Krull 1. Isto é, um domínio de Dedekind.

Referências Bibliográficas

[1] Anderson, Frank W.; Fuller, Kent R. Rings and categories of modules, Graduate Texts in Mathematics, 13 (2^{nd} ed.), New York: Springer-Verlag. 1992. 23

[2] Apostol, Tom M. Introduction to Analytic Number Theory. Springer. 1976. 3, 11, 12, 18, 19, 58

[3] Ash, Robert B. A course in algebraic number theory. Dover Publications, Inc., Mineola, NY. 2010. 46

[4] Atiyah, M. F; MacDonald, I. G. Introduction to Commutative Algebra. Addison-Wesley Publishing Company. 1969. 23, 28

[5] Caiúve, Abrantes M. B.; Miguel, C. Menon-type identities with respect to sets of units. The Ramanujan Journal. 2021. 61

[6] Cohen, I. S. Commutative rings with restricted minimum condition. Duke Math. J. 17, 27–42. 1950. 65

[7] Fraleigh, J. B. A first course in abstract algebra. Addison-Wesley. 2003. 4

[8] Hardy, G. H.; Wright, E. M. An introduction to the theory of numbers. Sixth edition. Revised by D. R. Heath-Brown and J. H. Silverman. With a foreword by Andrew Wiles. Oxford University Press, Oxford. 2008. 3

[9] Kaplansky, I. Commutative rings, ed. rev. University of Chicago Press. Chicago. 1974. 44

[10] Krull, W. Allgemeine Bewertungstheorie. J. Reine Angew. Math, 167, 160-196. 1932. 65
characters by Tóth's method, Miskolc Math. Notes, 22 (2021), 763–768.

[11] Luong, Bao. Fourier analysis on finite abelian groups. Applied and Numerical Harmonic Analysis. Birkhuser Boston, Inc., Boston, MA. 2009. 63

[12] Menon, P. K. On the sum $\sum(a-1,n)[(a,n)=1]$. J. Indian Math. Soc. 29, 155–163. 1965. 1, 33

[13] Miguel, C. Menon's identity in residually finite Dedekind domains. J. Number Theory 137, 179-185. 2014. 1, 42

[14] Miguel, C. A Menon-type identity in residually finite Dedekind domains. J. Number Theory 164, 43-51. 2016. 1, 42

[15] Monteiro, António J.; Matos, Isabel T. Álgebra - Um primeiro curso. Escolar Editora. 1995. 23, 29

[16] Narkiewicz, W. Elementary and Analytic Theory of Algebraic Numbers. 3^{rd} edition. Springer Monographs in Mathematics. Springer Verlag. Berlin. 2004. 43

[17] Neukirch, Jürgen. Algebraic number theory. Translated from the 1992 German original and with a note by Norbert Schappacher. With a foreword by G. Harder. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 322. Springer-Verlag, Berlin Heidelgerg. 1999. 23

[18] Neumann, P. M. A lemma that is not Burnside's, Math. Sci. 4, 133-141. 1979. 21

[19] Richards, I. M. A remark on the number of cyclic subgroups of a finite group. Amer. Math. Monthly 91, no. 9, 571-572. 1984. 1, 64

[20] Sobral, Manuela. Álgebra. Universidade Aberta. 1996. 23, 24

[21] Spellman, Dennis; Benkart, Georgia M.; Gaglione, Anthony M.; David, V. W.; Kidwell, Mark E.; Meyerson, Mark D. Wardlaw, William P. Principal ideals and associate rings. JP J. Algebra Number Theory Appl. 2 (2) 181–193. 2002. 44

[22] Stewart, Ian.; Tall, David. O. Algebraic Number Theory, Softcover, John Wiley Sons, Incorporated, New York. 1979. 5, 24, 43

[23] Sury, B. Some number-theoretic identities from group actions. Rend. Circ. Mat. Palermo (2) 58, no. 1, 99-108. 2009. 1, 34

[24] Tărnăuceanu, Marius. A generalization of Menon's identity. J. Number Theory 132, no. 11, 2568-2573. 2012. 1, 37

[25] Tóth, László. Proofs, generalizations and analogs of Menon's identity: a survey, arXiv: 2110.07271, 2021. 1

[26] Tóth, L. Short proof and generalization of a Menon-type identity by Li, Hu and Kim. Taiwanese J. Math. 23, no. 3, 557-561. 2019. 58

[27] Zhao, Xiaopeng; Cao, Zhen-Fu. Another generalization of Menon's identity. International Journal of Number Theory. 2017. 53

Índice Remissivo

Anel Comutativo Artiniano, 23, 27, 28

Caráter, 11–14, 16–19, 55, 56, 61
Caráter aditivo, 20, 58
Caráter de Dirichlet, 2, 16–19, 53, 54, 56–59, 61
Caráter de Dirichlet primitivo, 53–55
Caráter de grupo, 2, 11, 63
Caráter primitivo, 18, 19, 54, 56, 58, 59
Caráter principal, 11, 14, 17–19, 54, 56, 57, 63
Condutor, 19, 54, 56–59, 61
Condutor do caráter, 18, 62
Conjunto, 12, 16, 20–22, 27, 34, 51, 52
Conjunto dos carateres, 14, 63
Conjunto finito, 12, 47

Divisores positivos, 1, 33
Domínio de Dedekind, 1, 27, 29, 42, 43, 45–47, 49, 65
Domínio de Dedekind residualmente finito, 42, 43, 45–48, 50, 51, 61, 65
Domínio de Integridade, 23

Função aritmética, 1, 8, 9, 16, 56, 58
Função de Möbius, 8, 9, 58
Função divisor, 1, 43, 47
Função multiplicativa, 8, 9, 35, 51, 56
Função totiente de Euler, 1, 8, 9, 33, 43
Fórmula de Gauss, 64
Fórmula de Möbius, 9, 60

Grupo abeliano, 12, 14, 16, 33, 61
Grupo abeliano finito, 14, 16, 61–63, 65
Grupo de carateres, 61, 62
Grupo de unidades, 33, 43, 46, 63
Grupo finito, 11, 21, 22

Identidade de Menon, 1, 2, 9, 11, 20, 23, 34, 37, 38, 42, 43, 53, 61, 65
Indicador, 11, 12
Inteiros de Gauss, 23

Lema de Burnside, 2, 20, 21, 33, 37, 40, 44, 46, 47, 52, 61

Módulo induzido, 18–20, 53

Polinómio com coeficientes inteiros, 64
Produto de Dirichlet, 9, 38
Propriedade multiplicativa, 11–13, 17, 52

Relação de ortogonalidade, 16, 61
Relação de ortogonalidade para carateres, 14, 15

Subconjunto não vazio, 61, 64
Subconjunto não vazio de unidades, 1, 2, 61, 62, 65

Unidades, 2, 23, 25, 49, 50, 61, 65