UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO
DEPARTAMENTO DE MATEMÁTICA
PROGRAMA DE PÓS GRADUAÇÃO EM MATEMÁTICA

ALEXANDRE SILVA DOS REIS

FORMAS MODULARES E O PROBLEMA DOS NÚMEROS CONGRUENTES

VITÓRIA
2015

ALEXANDRE SILVA DOS REIS

FORMAS MODULARES E O PROBLEMA DOS NÚMEROS CONGRUENTES

Dissertação apresentada ao Programa de Pós Graduação em Matemática da Universidade Federal do Espírito Santo - PPGMAT, UFES - como requisito parcial para a obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. José Gilvan de Oliveira.

VITÓRIA

2015

Alexandre Silva dos Reis

Formas Modulares e o Problema dos Números Congruentes / Alexandre Silva dos Reis - Vitória, 2015.

60 f.

Orientador: Prof. José Gilvan de Oliveira.

Dissertação de Mestrado Acadêmico

Programa de Pós-Graduação em Matemática - PPGMAT

Universidade Federal do Espírito Santo.

1. Curvas Elípticas. 2. Números Congruentes. I. José Gilvan de Oliveira. II. Universidade Federal do Espírito Santo. III. Departamento de Matemática. IV. Formas Modulares e o Problema dos Números Congruentes.

UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO
Centro de Ciências Exatas
Programa de Pós-Graduação em Matemática

"Formas Modulares e o Problema dos Números Congruentes"

Alexandre Silva dos Reis

Dissertação submetida ao Programa de Pós-Graduação em Matemática da Universidade Federal do Espírito Santo como requisito parcial para a obtenção do título de Mestre em Matemática.

Aprovada em 29/10/2015 por:

José Gilvan de Oliveira – UFES

Valmecir Antonio dos Santos Bayer – UFES

Luciane Quoos Conte – UFRJ

"Feliz é a pessoa que encontra a Sabedoria,
a pessoa que adquire entendimento;
sua riqueza excede a prata, ganhá-la é melhor que ouro,
ela é mais preciosa que pérolas -
nada que você queira pode comparar-se a ela."
(Bíblia Sagrada, Provérbios 3: 13 a 15)

Agradecimentos

Agradeço primeiramente a Deus, pelo dom da Vida, pelo Seu infinito amor e por sempre renovar minhas forças.

Agradeço aos meus pais Antonio e Ana pelo amor incondicional, pelos exemplos de vida, pela dedicação e pelo apoio sempre presente. Ser filho deles é o meu maior orgulho! Agradeço aos meus irmãos Eduardo, Sandro e Raquel, pela convivência e afeto.

Agradeço aos meus amigos Filipe, Marcus Vinícius (Galo) e Stéfani, com quem convivi desde o início da minha jornada, ainda na graduação, e cujo companheirismo e convivência foram fundamentais em minha vida acadêmica. Agradeço também a Solon, Roberta e Franciane, amigos com os quais pude estreitar laços durante o mestrado. A presença, o apoio e a lealdade de cada um deles muito enriqueceram minha vida. Sem eles eu não teria chegado até aqui!

Agradeço ao meu orientador Prof. José Gilvan Oliveira, pela paciência, atenção e disponibilidade a mim dispensadas durante a realização deste trabalho. Guardarei com zelo todo o aprendizado adquirido com suas aulas e seus exemplos como profissional! Agradeço também à todos os professores do PPGMAT, pela formação que adquiri por meio deles.

Agradeço à CAPES, pelo apoio financeiro.

Resumo

Reticulados complexos, toros complexos e curvas elípticas são objetos que embora possuindo natureza e estruturas distintas, são equivalentes de alguma forma. É possível por meio de um reticulado complexo obter um toro complexo e daí, obter uma curva elíptica. Além disso esse "caminho" pode ser percorrido também de maneira inversa. Essa conexão será o principal objeto de estudo nesse trabalho, que também abordará de maneira criteriosa alguns assuntos relacionados, tais como o grupo linear especial, formas modulares e curvas modulares. Ao final, como aplicação dos conceitos e ferramentas estudadas, será considerado o problema dos números congruentes, que além de estar estreitamente relacionado com as curvas elípticas, possui relação com a famosa Conjectura de Birch e Swinnerton-Dyer, esse que é um dos Problemas do Milênio.

Palavras-chaves: Reticulados Complexos. Curvas Elípticas. Formas Modulares. Números Congruentes.

Abstract

Complex lattices, complex tori and elliptic curves are objects that although having different structures and nature, are equivalent. It is possible by means of a complex lattice to obtain a complex torus and hence, to obtain an elliptic curve; and that "path"' can also be done in reverse. This connection will be the main object of study in this work, which will also address a careful manner some issues related to it, such as the special linear group, modular forms and modular curves. Finally, as an application of the concepts and tools studied, the congruent numbers problem is considered. This problem besides being closely related to elliptic curves, has a relationship with the famous Birch and Swinnerton-Dyer conjecture, one of the Millennium Problems.

Key-words: Complex Lattices. Elliptic Curves. Modular Forms. Congruent Numbers.

Sumário

Introdução

A teoria das curvas elípticas, além de ser uma das mais belas de toda a matemática, destaca-se também pela sua versatilidade. Com aplicações em Geometria Diferencial (superfícies mínimas), Criptografia e Geometria Algébrica sobre corpos finitos (nesta área se destaca o Teorema de Hasse-Weil), essa versatilidade foi coroada em 1995, quando Andrew Wiles publicou sua histórica prova do Último Teorema de Fermat, concluída após a demonstração de uma versão da conjectura de Taniyama-Shimura, relacionando curvas elípticas e curvas modulares.

Neste trabalho abordaremos as curvas elípticas por meio da função $\wp$ de Weierstrass, a qual é associada a um reticulado do plano complexo. Cada reticulado determina uma estrutura algébrica e analítica chamada toro complexo. Veremos também que estes três objetos - curvas elípticas, reticulados e toros complexos - podem ser agrupados (cada um a seu modo) em classes de equivalência, e que cada uma dessas respectivas classes pode ser determinada por um único ponto no semiplano superior complexo.

Essa associação com pontos do semiplano superior complexo possui dupla importância: em primeiro lugar, por meio dela obtemos um critério para decidir se duas curvas elípticas são isomorfas ou não e; em segundo, pelo fato de que tal associação abre caminho para a teoria das curvas modulares. Para o entendimento de tais conceitos estudaremos dois objetos: as formas modulares, que são funções meromorfas específicas definidas no semiplano superior complexo, e o grupo linear especial, no qual cada elemento descreve uma aplicação racional nesse semiplano.

Como aplicação da teoria desenvolvida consideraremos o Problema dos Números Congruentes, isto é, dos números inteiros que são realizados como áreas de triângulos retângulos cujas medidas dos lados são números racionais. Esse Problema, como veremos, está estreitamente relacionado às curvas elípticas e sua solução geral depende da conhecida conjectura de Birch e Swinnerton-Dyer, um dos problemas do milênio.

A respeito do texto em si, no primeiro capítulo trataremos dos reticulados complexos e do grupo linear especial, as estruturas que serão as bases sobre as quais tudo o mais será feito. No capítulo 2 abordaremos as funções elípticas e as formas modulares, funções meromorfas cujas propriedades estão relacionadas com os reticulados complexos e com o grupo linear especial, respectivamente.

No capítulo 3 serão considerados os toros complexos e a função $\wp$ de Weierstrass. As funções $\wp$ e $\wp'$, como veremos, não só possuem uma propriedade fundamental que permite definir uma

curva elíptica, mas permitem também caracterizar todo o corpo de funções elípticas em relação à um reticulado.

No capítulo 4 trataremos das curvas elípticas, objeto central deste trabalho, destacando sua propriedade de grupo abeliano. Na segunda parte do capítulo trataremos brevemente das curvas modulares, estruturas analíticas nas quais cada ponto é uma classe de curvas elípticas isomorfas. Além disso, obteremos um critério por meio do qual decidir se duas curvas elípticas são isomorfas ou não.

O capítulo 5 será dedicado ao Problema dos Números Congruentes. Demonstraremos na primeira seção algumas caracterizações do problema, também relacionando-o com curvas elípticas. Na segunda seção do capítulo trataremos da função L de Hasse-Weil, a qual a Conjectura de Birch e Swinnerton-Dyer faz menção, e consideraremos os avanços mais recentes relacionados ao problema.

Capítulo 1

RETICULADOS E O GRUPO UNIMODULAR

No presente capítulo trataremos primeiramente dos reticulados complexos, que são certos subgrupos do grupo abeliano aditivo $\mathbb{C}$ dos números complexos, obtidos a partir de uma base do $\mathbb{R}$-espaço vetorial $\mathbb{C}$. Destacaremos também uma condição de dependência de um reticulado em relação à uma base de $\mathbb{C}$. Tal condição leva automaticamente ao segundo objeto a ser considerado nesse capítulo, que é o grupo linear especial $SL_2(\mathbb{Z})$ das matrizes de ordem 2 com entradas em $\mathbb{Z}$ e com determinante 1. Destacaremos algumas propriedades desse grupo e alguns de seus subgrupos, calculando os seus respectivos índices. A importância desses dois objetos será posta em relevo no Capítulo 3.

A abordagem que aqui faremos de tais objetos segue a mesma linha do capítulo 1 de [2]. Mais detalhes podem ser conferidos tanto lá quanto no capítulo 3 de [5].

1.1 Reticulados Complexos

O conjunto $\mathbb{C}$ dos números complexos é um espaço vetorial real de dimensão 2. Dada uma base ordenada $\{\omega_1, \omega_2\}$ de $\mathbb{C}$, o subgrupo Ω definido por

$$\Omega = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z} = \{a\omega_1 + b\omega_2;\ a, b \in \mathbb{Z}\} = [\omega_1, \omega_2]$$

é um *reticulado* em $\mathbb{C}$. Note que a condição do conjunto $\{\omega_1, \omega_2\}$ ser uma base de $\mathbb{C}$ equivale à condição $Im(\frac{\omega_2}{\omega_1}) \neq 0$. Assim, substituindo ω_2 por $-\omega_2$ se necessário, podemos sempre considerar $Im(\frac{\omega_2}{\omega_1}) > 0$.

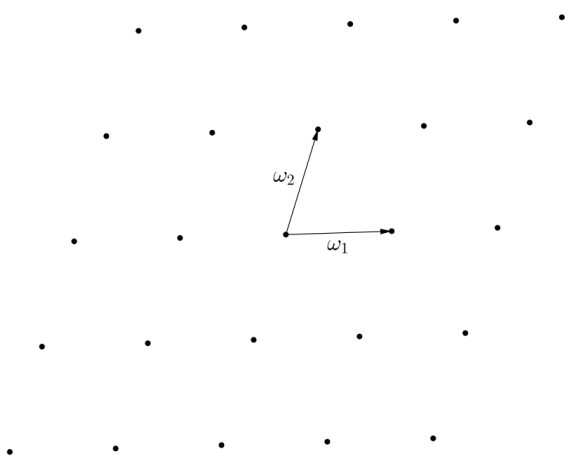

Figura 1.1: Exemplo de reticulado.

A relação de dependência de um reticulado $\Omega = [\omega_1, \omega_2]$ com uma base ordenada $\{\omega_1, \omega_2\}$ é esclarecida na Proposição seguinte.

Proposição 1.1.1. *Dois reticulados $\Omega = [\omega_1, \omega_2]$ e $\Omega' = [\omega_1', \omega_2']$ são iguais se, e somente se, existem $a, b, c, d \in \mathbb{Z}$, com $ad - bc = 1$, tais que*

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix} = \begin{bmatrix} \omega_1' \\ \omega_2' \end{bmatrix}.$$

Demonstração. A recíproca é evidente, pois a matriz quadrada de ordem 2 acima é invertível. Se $\Omega = \Omega'$, então existem $a, b, c, d, r, s, t, u \in \mathbb{Z}$ tais que

$$\begin{cases} \omega_2' = b\omega_1 + a\omega_2 \\ \omega_1' = d\omega_1 + c\omega_2 \end{cases} \text{ e } \begin{cases} \omega_1 = s\omega_1' + r\omega_2' \\ \omega_2 = u\omega_1' + t\omega_2' \end{cases}$$

Portanto, como $\{\omega_1, \omega_2\}$ e $\{\omega_1', \omega_2'\}$ são bases de $\mathbb{C}$, temos que $(ad-bc)(ru-st) = 1$, e como cada fator é um número inteiro, segue $ad - bc = \pm 1$.

Agora, observe que $\frac{\omega_2'}{\omega_1'} = \frac{b\omega_1 + a\omega_2}{d\omega_1 + c\omega_2} = \frac{a\left(\frac{\omega_2}{\omega_1}\right) + b}{c\left(\frac{\omega_2}{\omega_1}\right) + d}$. Ou seja, considerando a aplicação $A(\tau) = \frac{a\tau + b}{c\tau + d}$, $\tau \in \mathbb{C}$, como

$$A(\tau) = \frac{(a\tau + b)(c\bar{\tau} + d)}{|c\tau + d|^2} = \frac{(ac|\tau|^2 + (ad + bc)Re(\tau) + bd) + i \cdot (ad - bc)Im(\tau)}{|c\tau + d|^2}, \tag{1.1}$$

e como temos pela hipótese que $Im\left(\frac{\omega_2'}{\omega_1'}\right) = (ad-bc)\dfrac{Im\left(\frac{\omega_2}{\omega_1}\right)}{\left|c\left(\frac{\omega_2}{\omega_1}\right) + d\right|^2} > 0$, segue então que $ad-bc = 1$. Assim A é uma aplicação com $Im(A(\tau)) > 0$ se $Im(\tau) > 0$.

□

Podemos ainda ter o caso onde um reticulado é obtido por multiplicação de um número complexo não-nulo.

Definição 1.1.2. *Dois reticulados Ω e Ω' são equivalentes se existe $m \in \mathbb{C}^* = \mathbb{C}\backslash\{0\}$ tal que $m\Omega = \Omega'$.*

Um fato importante é que um reticulado complexo Ω é equivalente a um reticulado do tipo $\Omega_\omega = [\omega, 1]$. Nos capítulos subsequentes, veremos que reticulados equivalentes fornecem isomorfismos de toros complexos e de curvas elípticas, estruturas analíticas e algébricas a serem tratadas nos capítulos 3 e 4.

1.2 O Grupo Linear Especial $SL_2(\mathbb{Z})$

A partir da Proposição 1.1.1 e da consideração feita no fim da seção anterior fica claro que se quisermos entender melhor as relações entre os reticulados complexos, devemos estudar o semiplano superior complexo $\mathcal{H} = \{\tau \in \mathbb{C};\ Im(\tau) > 0\}$ e ações de grupos de matrizes neste semiplano. Seja $SL_2(\mathbb{Z})$ o *grupo linear especial* das matrizes de ordem 2 com entradas em $\mathbb{Z}$ e com determinante 1. Como vimos na demonstração da Proposição 1.1.1, dado $\tau \in \mathcal{H}$ e $A \in SL_2(\mathbb{Z})$, temos que $A(\tau) \in \mathcal{H}$. O semiplano superior complexo $\mathcal{H}$, por sua vez, será estudado com mais detalhes no capítulo 3. Já o grupo $SL_2(\mathbb{Z})$ e subgrupos específicos serão estudados nessa seção e até o fim do capítulo. Por motivos que ficarão claros adiante, usaremos a notação $\Gamma(1) = SL_2(\mathbb{Z})$.

Um fato importante sobre $\Gamma(1)$ é demonstrado abaixo.

Proposição 1.2.1. *Se* $T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ *e* $S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, *então* $\Gamma(1) = \langle T, S \rangle$.

Demonstração. É claro que $\langle T, S \rangle \subset \Gamma(1)$.

Seja $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma(1)$. Vamos provar que $A \in \langle T, S \rangle$.

Como $S^2 = -I$, substituindo A por $-A$ se necessário, podemos supor $c \geq 0$.

Dito isto, suponhamos primeiramente $c = 0$. Como $\det(A) = ad - bc = ad = 1$, segue que $a = d = \pm 1$. Então, novamente substituindo A por $-A$ se necessário, podemos considerar

$$A = \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix},\ b \in \mathbb{Z},$$

ou seja, $A = T^b$, $b \in \mathbb{Z}$. Portanto no caso $c = 0$ temos $A \in \langle T, S \rangle$, como queríamos.

Suponhamos agora $c = 1$. Temos da condição $\det(A) = 1$ que

$$A = \begin{bmatrix} a & ad-1 \\ 1 & d \end{bmatrix} = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & d \\ 0 & 1 \end{bmatrix},$$

e portanto $A = T^a \cdot S \cdot T^d \in \langle T, S \rangle$.

Finalmente, suponhamos $c > 0$ qualquer. Como $ad - bc = 1$, temos que $mdc\{d, c\} = 1$, e existem $q, r \in \mathbb{Z},\ 1 \leq r < c$, tais que $d = qc + r$. Então

$$A \cdot T^{-q} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} 1 & -q \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & b-aq \\ c & d-qc \end{bmatrix} = \begin{bmatrix} a & b-aq \\ c & r \end{bmatrix},$$

e daí

$$B = A \cdot T^{-q} \cdot S = \begin{bmatrix} a & b-aq \\ c & r \end{bmatrix} \cdot \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} b-aq & -a \\ r & -c \end{bmatrix}.$$

Portanto $A = B \cdot S^{-1} \cdot T^q$. Como $1 \leq r < c$, repetindo o processo um número finito de vezes podemos concluir que $A \in \langle T, S \rangle$.

□

Seja N um inteiro positivo. Chamamos de *subgrupo principal de congruência de nível N* o conjunto

$$\Gamma(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma(1);\ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} mod(N) \right\},$$

onde a congruência das matrizes é definida pela congruência módulo N das entradas correspondentes. De acordo com essa definição, $N = 1$ nos dá $\Gamma(1) = SL_2(\mathbb{Z})$, o que justifica a notação que utilizamos.

Definição 1.2.2. *Um subgrupo Γ de $\Gamma(1)$ é um subgrupo de congruência de nível N se existe um inteiro positivo N tal que $\Gamma(N) \subset \Gamma$.*

Além do subgrupo principal, outros importantes subgrupos de congruência são

$$\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma(1);\ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} mod(N) \right\}$$

e

$$\Gamma_1(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma(1);\ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} mod(N) \right\},$$

onde "$*$" denota que a entrada correspondente é arbitrária. É claro que $\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset SL_2(\mathbb{Z})$. A Proposição abaixo lista alguns índices desses grupos.

Proposição 1.2.3. *Seja N um inteiro positivo e seja $\mathbb{Z}_N = \mathbb{Z}/N\mathbb{Z}$ o anel dos inteiros congruentes módulo N.*

(a) O homomorfismo canônico $SL_2(\mathbb{Z}) \longrightarrow SL_2(\mathbb{Z}_N)$ é sobrejetivo.

(b) Se $e \in \mathbb{N}$ e p é um primo positivo, então $|SL_2(\mathbb{Z}_{p^e})| = p^{3e}\Big(1 - \frac{1}{p^2}\Big)$.

(c) $[SL_2(\mathbb{Z}) : \Gamma(N)] = N^3\Pi_{p|N}\Big(1 - \dfrac{1}{p^2}\Big)$.

(d) $[\Gamma_1(N) : \Gamma(N)] = N$ e $[\Gamma_0(N) : \Gamma(N)] = \phi(N)$, onde ϕ é a função de Euler.

(e) $[SL_2(\mathbb{Z}) : \Gamma_0(N)] = N \cdot \Pi_{p|N}\Big(1 + \dfrac{1}{p}\Big)$.

Demonstração. (a) Claramente podemos ver que o núcleo do homomorfismo canônico é $\Gamma(N)$. Seja $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{Z})$ tal que $\overline{A} = \begin{bmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{bmatrix} \in SL_2(\mathbb{Z}_N)$. Primeiramente observamos que $mdc\{c, d, N\} = 1$, pois chamando $g = mdc\{c, d\}$, $c = g \cdot c_0$ e $d = g \cdot d_0$, temos

$$\begin{aligned} (ad - bc) - 1 = \lambda N,\ \lambda \in \mathbb{Z} &\Leftrightarrow g(ad_0 - bc_0) - \lambda N = 1 \\ &\Leftrightarrow mdc\{g, N\} = mdc\{c, d, N\} = 1. \end{aligned}$$

Nossa meta é mostrar que existe uma tal matriz $A \in SL_2(\mathbb{Z})$. O primeiro passo para isso é mostrar que existem $c, d \in \mathbb{Z}$ nessas condições tais que $mdc\{c, d\} = 1$. Suponhamos primeiramente $c \neq 0$.

Sejam $c = p_1^{r_1} \dots p_n^{r_n}$ e $N = p_{i_1}^{s_{i_1}} \dots p_{i_m}^{s_{i_m}} \cdot q_1^{t_1} \dots q_k^{t_k}$, $m \geq 0$, as fatorações de c e N em produto de potências de números primos distintos, onde os primos p_{i_l} são os fatores comuns de c e N. Sejam $c' = \frac{c}{c''}$ e $c'' = p_{i_1}^{r_{i_1}} \dots p_{i_m}^{r_{i_m}}$, se $m > 0$ ou $c'' = 1$ caso contrário. Então $mdc\{c', N\} = 1$ e cada divisor primo de c'' é também divisor de N.

Como $mdc\{c', N\} = 1$, existem $u, v \in \mathbb{Z}$ tais que $uc' + vN = 1$. Daí $1 - d = [(1 - d)u]c' + [(1 - d)v]N$, e portanto $1 = lc' + (d + kN)$, onde $l = (1 - d)u$ e $k = (1 - d)v$. Em particular temos que c' e $d + kN$ são primos entre si. Como cada divisor primo de c'' é também divisor de N e $mdc\{c, d, N\} = 1$, concluímos que $mcd\{c, d + kN\} = 1$. Caso $c = 0$, então devemos ter $d \neq 0$, e repetimos o mesmo argumento acima agora para o inteiro d, e assim, substituindo d por $d + kN$ podemos considerar a matriz $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ com $mdc\{c, d\} = 1$.

Tomemos então uma matriz

$$A = \begin{bmatrix} a + mN & b + nN \\ c & d \end{bmatrix},\ m, n \in \mathbb{Z}.$$

Temos que $det(A) = ad - bc + N(md - cn) = 1 + N(\lambda + md - cn)$, pois como vimos no início da demonstração, $(ad - bc) - 1 = \lambda N$. Como $mdc\{c, d\} = 1$, existem $m_0, n_0 \in \mathbb{Z}$ tais que $\lambda = n_0 c - m_0 d$, e assim, tomando $m = m_0$ e $n = n_0$, a matriz $A \in SL_2(\mathbb{Z})$, como queríamos.

(b) Vamos provar este ítem por indução sobre e. Para $e = 1$, consideremos o homomorfismo

$$\begin{array}{rcl} \delta : GL_2(\mathbb{Z}_p) & \longrightarrow & \mathbb{Z}_p^* \\ A & \longmapsto & \delta(A) = det(A) \end{array}$$

Claramente δ é sobrejetiva e $Ker(\delta) = SL_2(\mathbb{Z}_p)$, e pelo Teorema dos Homomorfismos temos

$$\Big|\frac{GL_2(\mathbb{Z}_p)}{SL_2(\mathbb{Z}_p)}\Big| = |\mathbb{Z}_p^*| = p - 1.$$

Vamos agora calcular $|GL_2(\mathbb{Z}_p)|$. Como $GL_2(\mathbb{Z}_p)$ pode ser visto como o conjunto das bases do plano cartesiano $\mathbb{Z}_p^2$, temos que para cada um dos $p^2 - 1$ elementos não nulos de $\mathbb{Z}_p^2$ existem $p^2 - p$ bases de $\mathbb{Z}_p^2$. Daí $|GL_2(\mathbb{Z}_p)| = (p^2 - 1)(p^2 - p)$. Assim segue que $|SL_2(\mathbb{Z}_p)| = p(p^2 - 1) = p^3\Big(1 - \frac{1}{p^2}\Big)$.

Se

$$|SL_2(\mathbb{Z}_{p^e})| = p^{3e}\Big(1 - \frac{1}{p^2}\Big),\ e \geq 1,$$

então seja η o homomorfismo natural

$$\begin{array}{rcl} \eta : SL_2(\mathbb{Z}_{p^{e+1}}) & \longrightarrow & SL_2(\mathbb{Z}_{p^e}) \\ \begin{bmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{bmatrix} & \longmapsto & \begin{bmatrix} \widetilde{a} & \widetilde{b} \\ \widetilde{c} & \widetilde{d} \end{bmatrix} \end{array}$$

onde "$\overline{x}$" representa a classe de x módulo p^{e+1} e "$\widetilde{x}$" representa a classe de x módulo p^e. Pelo ítem anterior sabemos que a aplicação $SL_2(\mathbb{Z}) \longrightarrow SL_2(\mathbb{Z}_{p^{e+1}})$ é sobrejetiva, e como $\mathbb{Z}_{p^{e+1}} = \{\overline{0}, \overline{1}, \ldots, \overline{p^e - 1}, \overline{p^e}, \overline{p^e + 1}, \ldots, \overline{2p^e - 1}, \overline{2p^e}, \overline{2p^e + 1}, \ldots, \overline{p^{e+1} - 1}\}$, o homomorfismo η é sobrejetivo. Vamos calcular $|Ker(\eta)|$.

Dado $\begin{bmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{bmatrix} \in Ker(\eta)$, temos $\begin{bmatrix} \widetilde{a} & \widetilde{b} \\ \widetilde{c} & \widetilde{d} \end{bmatrix} = \begin{bmatrix} \widetilde{1} & \widetilde{0} \\ \widetilde{0} & \widetilde{1} \end{bmatrix}$. Logo $\overline{b} = \overline{c} = 0$, daí devemos ter $\overline{b}, \overline{c} \in \{\overline{0}, \overline{p^e}, \ldots, \overline{(p-1)p^e}\}$. Como as escolhas de $\overline{b}$ não influenciam nas escolhas de $\overline{c}$, e vice-versa, segue que existem p possibilidades para escolhas de cada um deles. Temos também $\tilde{a} = \tilde{d} = \tilde{1}$, ou seja, $\overline{a}, \overline{d} \in \{\overline{1}, \overline{p^e + 1}, \overline{2p^e + 1}, \ldots, \overline{(p-1)p^e + 1}\}$, e temos ainda que $\overline{ad - bc} = \overline{ad} = \overline{1}$ (pois b e c são múltiplos p^e, logo bc é múltiplo de p^{e+1}). Assim $\overline{a}$ e $\overline{d}$ são elementos inversos um do

outro em $\mathbb{Z}_{p^{e+1}}$, e fixado um deles o outro estará determinado. Desse fato segue que existem p possibilidades para a escolha de $\overline{a}$ ou de $\overline{d}$. Concluímos assim que $|Ker(\eta)| = p^3$.

Pelo Teorema dos Homomorfismos e pela hipótese em $|SL_2(\mathbb{Z}_{p^e})|$ temos

$$|SL_2(\mathbb{Z}_{p^{e+1}})| = p^{3(e+1)}\Big(1 - \frac{1}{p^2}\Big),$$

e o resultado segue pelo Princípio da Indução.

(c) Primeiramente escrevemos $N = p_1^{e_1} \dots p_r^{e_r}$ e definimos a aplicação

$$\begin{array}{rcl} \nabla : SL_2(\mathbb{Z}_N) & \longrightarrow & SL_2(\mathbb{Z}_{p_1^{e_1}}) \times \cdots \times SL_2(\mathbb{Z}_{p_r^{e_r}}) \\ \begin{bmatrix} a_N & b_N \\ c_N & d_N \end{bmatrix} & \longmapsto & \left(\begin{bmatrix} a_{(1)} & b_{(1)} \\ c_{(1)} & d_{(1)} \end{bmatrix}, \dots, \begin{bmatrix} a_{(r)} & b_{(r)} \\ c_{(r)} & d_{(r)} \end{bmatrix} \right), \end{array}$$

onde x_N representa a classe de x módulo N e, para $i \in \{1, \dots, r\}$, $x_{(i)}$ representa a classe de x módulo $p_i^{e_i}$. É fácil ver que ∇ está bem definida. Além disso ∇ é um homomorfismo de grupos, considerando o produto direto de grupos. Daí

$$\begin{array}{rcl} Ker(\nabla) & = & \left\{ \begin{bmatrix} a_N & b_N \\ c_N & d_N \end{bmatrix} \in SL_2(\mathbb{Z}_N);\ \begin{bmatrix} a_{(i)} & b_{(i)} \\ c_{(i)} & d_{(i)} \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} mod(p_i^{e_i}),\ i \in \{1, \dots, r\} \right\} \\ & = & \left\{ \begin{bmatrix} a_N & b_N \\ c_N & d_N \end{bmatrix} \in SL_2(\mathbb{Z}_N);\ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} mod(N) \right\}, \end{array}$$

onde a última igualdade segue do Teorema Chinês dos Restos. Logo ∇ é injetiva.

Pelo Teorema Chinês dos Restos, ∇ é também sobrejetiva e logo ∇ é um isomorfismo. Assim, pelos ítens anteriores

$$\begin{array}{rcl} [SL_2(\mathbb{Z}) : \Gamma(N)] = |SL_2(\mathbb{Z}_N)| & = & \left|\Pi_{i=1}^r SL_2(\mathbb{Z}_{p_i^{e_i}})\right| = \Pi_{i=1}^r |SL_2(\mathbb{Z}_{p_i^{e_i}})| \\ & = & N^3 \Pi_{p|N}\Big(1 - \frac{1}{p^2}\Big), \end{array}$$

como queríamos.

(d) A aplicação $f : \Gamma_1(N) \longrightarrow \mathbb{Z}_N$, dada por $f\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \overline{b}$, é claramente um homomorfismo sobrejetivo. Se $f\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \overline{b} = \overline{0}$, então como $\overline{ad - bc} = \overline{ad} = \overline{1}$, segue que $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma(N)$, portanto $Ker(f) = \Gamma(N)$. Do Teorema dos Homomorfismos segue $[\Gamma_1(N) : \Gamma(N)] = |\mathbb{Z}_N| = N$.

Agora, a função $g : \Gamma_0(N) \longrightarrow \mathbb{Z}_N^*$, dada por $g\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \overline{d}$ é um homomorfismo sobrejetivo de núcleo é $\Gamma_1(N)$. Portanto $[\Gamma_0(N) : \Gamma_1(N)] = |\mathbb{Z}_N^*| = \phi(N) = N \cdot \Pi_{p|N}\Big(1 - \frac{1}{p}\Big)$, pelo Teorema dos Homomorfismos.

(e) Pelos ítens (c) e (d) temos

$$[SL_2(\mathbb{Z}) : \Gamma_1(N)] = \frac{[SL_2(\mathbb{Z}) : \Gamma(N)]}{[\Gamma_1(N) : \Gamma(N)]} = N^2 \Pi_{p|N}\Big(1 - \frac{1}{p^2}\Big),$$

e portanto

$$[SL_2(\mathbb{Z}) : \Gamma_0(N)] = \frac{[SL_2(\mathbb{Z}) : \Gamma_1(N)]}{[\Gamma_0(N) : \Gamma_1(N)]} = N \cdot \Pi_{p|N}\Big(1 + \frac{1}{p}\Big).$$

□

Esta Proposição nos permite concluir que se Γ é um subgrupo de congruência de nível N, então $[SL_2(\mathbb{Z}) : \Gamma]$ é finito, já que

$$[SL_2(\mathbb{Z}) : \Gamma(N)] = [SL_2(\mathbb{Z}) : \Gamma][\Gamma : \Gamma(N)].$$

Encerraremos este capítulo dando um exemplo de um subgrupo de congruência, que surge do *problema dos quatro quadrados*. Este problema visa responder a pergunta sobre o número de maneiras diferentes que um dado número inteiro positivo pode ser escrito como soma de quatro quadrados de números inteiros. Vamos rapidamente descrever como tal subgrupo é obtido.

Dados n, k números inteiros positivos, o *número de representações de n por k quadrados* é $r(n,k) = \sharp\{v \in \mathbb{Z}^k;\ n = v_1^2 + \ldots + v_k^2\}$. Definimos a *função geradora de representação* por $\theta_k(\tau) = \sum_{n=0}^{\infty} r(n,k)q^n,\ \tau \in \mathcal{H},\ q = e^{2\pi i \tau}$. Para o caso $k = 4$, a função $\theta_4(\tau)$ é uma forma modular de peso 2 em relação ao subgrupo $\Gamma_0(4)$ ([2], p. 11-12). Em particular, $\theta_4(\tau)$ tem a seguinte propriedade:

$$\theta_4\Big(\frac{a\tau + b}{c\tau + d}\Big) = (c\tau + d)^2 \theta_4(\tau),\ \forall \tau \in \mathcal{H},\ \forall \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(4).$$

A partir de conhecimento de uma base explicita do espaço das formas modulares de peso dois obtém-se a solução para o problema dos quatro quadrados ([2], p. 19)

$$r(n,4) = 8 \sum_{\substack{0<d|n \\ 4\nmid n}} d,\ n \geq 1.$$

Para verificar a propriedade acima mencionada da função $\theta_4(\tau)$, com relação a ação do subgrupo $\Gamma_0(4)$, basta verificar em geradores desse subgrupo. Afirmamos que o grupo Γ_θ definido por $\Gamma_\theta = \big\langle \pm T, \pm S_4 \big\rangle$, onde $T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ e $S_4 = -ST^{-4}S = \begin{bmatrix} 1 & 0 \\ 4 & 1 \end{bmatrix}$ é o próprio grupo $\Gamma_0(4)$, ou seja, $\Gamma_\theta = \Gamma_0(4)$. Como $\pm T, \pm S_4 \in \Gamma_\theta$, é claro que $\Gamma_\theta \subset \Gamma_0(4)$. Consideremos então $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(4)$. Podemos escrever $c = 4c_0, c_0 \in \mathbb{Z}$. Dessa forma $ad - bc = 1$ e em particular $d \neq 0$.

Se $d = 1$ então $a = 1 + bc$, assim

$$M = \begin{bmatrix} 1+bc & b \\ c & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^b \begin{bmatrix} 1 & 0 \\ 4 & 1 \end{bmatrix}^{c_0} \in \Gamma_\theta.$$

Analogamente, se $d = -1$, então $M = (-T)^{-b} \cdot S_4^{-c_0} \in \Gamma_\theta$.

Seja então $|d| > 1$. Como $ad - bc = 1$ temos que $c \neq 0$ e existem inteiros q e r tais que $d = qc + r$, onde $0 < |r| < \dfrac{|c|}{2}$. Daí $MT^{-q} = \begin{bmatrix} a & b-aq \\ c & r \end{bmatrix}$. Como já visto, se $|r| = 1$, então $M \cdot T^{-q} \in \Gamma_\theta$, e portanto $M \in \Gamma_\theta$. Se $|r| > 1$ então existem inteiros q_0 e r_0 tais que $c_0 = q_0 r + r_0$, onde $0 < |r_0| < \dfrac{|r|}{2}$, já que $ad - bc = 1$. Concluímos que para algum inteiro a', temos

$$M \cdot T^{-q} \cdot S_4^{-q_0} = \begin{bmatrix} a' & b-aq \\ 4r_0 & r \end{bmatrix},$$

onde $0 < 4|r_0| < 2|r| < |c|$. Repetindo esse processo um número finito de vezes podemos supor $|r| = 1$, assim obtemos uma matriz em Γ_θ e portanto $M \in \Gamma_\theta$.

Capítulo 2

FUNÇÕES ELÍPTICAS E FORMAS MODULARES

Neste capítulo apresentaremos alguns resultados acerca de dois tipos de funções relacionadas aos reticulados e ao grupo linear especial, vistos no capítulo anterior.

Primeiramente trataremos das funções elípticas, que são aplicações meromorfas em $\mathbb{C}$ e periódicas em um reticulado Ω. Feito isso, trataremos das formas modulares, que por sua vez são aplicações meromorfas definidas no semiplano superior complexo e que têm uma propriedade particular sob a ação de subgrupos de congruência de $\Gamma(1)$.

2.1 Funções Elípticas - Uma Abordagem Geral

Trataremos aqui das funções elípticas em caráter mais geral, apresentando suas propriedades básicas. Essas propriedades servirão para a demonstração de fatos importantes sobre as chamadas curvas elípticas, objetos a serem tratados no capítulo 3. Essas funções são abordadas com mais detalhes no capítulo 3 de [5].

Por toda essa seção, fixaremos a notação $\Omega = [\omega_1, \omega_2]$ para denotar um reticulado em $\mathbb{C}$, com $Im(\frac{\omega_2}{\omega_1}) > 0$. O conjunto $P = \{t_1\omega_1 + t_2\omega_2;\ t_1, t_2 \in [0,1]\}$ é chamado de *paralelogramo fundamental* de Ω. Para quaisquer $a, b \in \mathbb{Z}$, $P_{a,b} = \{(a+t_1)\omega_1 + (b+t_2)\omega_2;\ t_1, t_2 \in [0,1]\}$ também pode ser considerado como um paralelogramo fundamental de Ω.

Definição 2.1.1. *Uma função elíptica (em relação à Ω) é uma função meromorfa $f : \mathbb{C} \longrightarrow \mathbb{C}$ tal que $f(z+\omega) = f(z)$, para todos $z \in \mathbb{C}$ e $\omega \in \Omega$.*

Denotemos por M_Ω o conjunto de todas as funções elípticas em relação à Ω. É fácil ver que M_Ω é um corpo. Desta definição podemos extrair também os fatos a seguir.

Observação 2.1.2. *f é elíptica se, e somente se, f é meromorfa em $\mathbb{C}$ e para todo $z \in \mathbb{C}$, $f(z+\omega_1) = f(z) = f(z+\omega_2)$.*

Observação 2.1.3. *Se f é uma função elíptica inteira (sem pólos), então f é constante. De fato, podemos considerar f como sendo definida apenas no paralelogramo fundamental P, que é um conjunto compacto. Daí $f(P)$ é também um conjunto compacto. O resultado segue então do Teorema de Liouville.*

Desta segunda observação podemos concluir também que se f é uma função elíptica que não possui zeros então ela é constante.

Sejam $\alpha \in \mathbb{C}^*$ e P um paralelogramo fundamental. Consideremos o conjunto

$$P_\alpha = \alpha + P = \{\alpha + z;\ z \in P\} = \{\alpha + t_1\omega_1 + t_2\omega_2;\ t_1, t_2 \in [0,1]\},$$

que também é um paralelogramo fundamental para Ω. As vezes é conveniente considerar $t_1, t_2 \in [0,1)$, o que nos dá um único representante em P_α para cada classe módulo Ω.

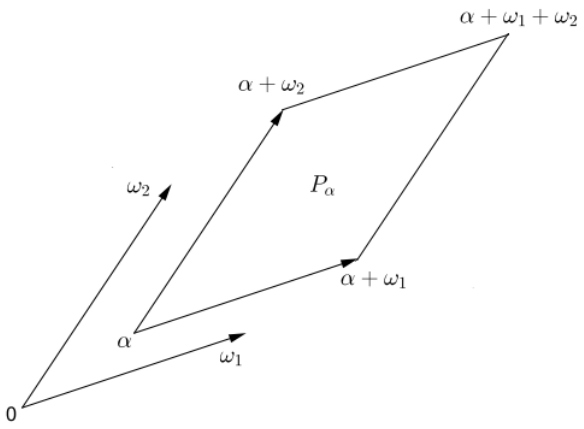

Figura 2.1: Paralelogramo fundamental P_α.

Os teoremas a seguir utilizam ferramentas já bem conhecidas da Análise Complexa.

Teorema 2.1.4. *Sejam f uma função elíptica e P_α um paralelogramo fundamental que não contém pólos de f na fronteira ∂P_α de P_α. Então a soma dos resíduos de f no interior de P_α é zero.*

Demonstração. Sejam $\gamma_1, \gamma_2, \gamma_3$ e γ_4 os caminhos lineares que compõem a fronteira ∂P_α de P_α, como mostrados na figura abaixo. Se existem k pólos de f no interior de P_α, então do Teorema dos Resíduos segue que

$$\frac{1}{2\pi i}\int_{\partial P_\alpha} f(z)dz$$

é a soma dos resíduos de f no interior de P_α.

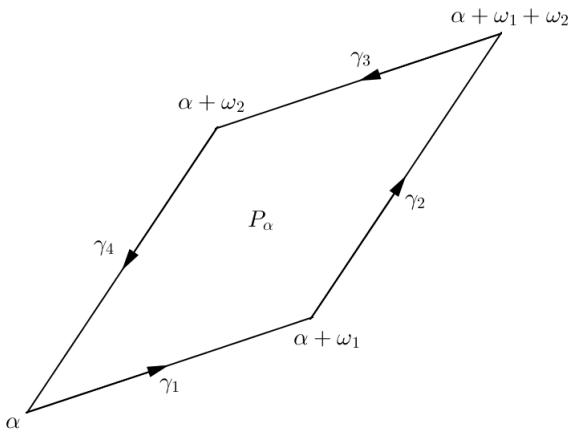

Figura 2.2: Caminhos na fronteira de P_α.

Consideremos as parametrizações:

- $\gamma_1(t) = \alpha + t\omega_1$,
- $\gamma_2(t) = \alpha + \omega_1 + t\omega_2$,
- $\gamma_3(t) = \alpha + (1-t)\omega_1 + \omega_2$,
- $\gamma_4(t) = \alpha + (1-t)\omega_2$,

onde $t \in [0,1]$. Assim, podemos escrever

$$\int_{\partial P_\alpha} f(z)dz = \int_{\gamma_1} f(z)dz + \int_{\gamma_2} f(z)dz + \int_{\gamma_3} f(z)dz + \int_{\gamma_4} f(z)dz.$$

Sendo $\gamma_3^-(t) = \alpha + t\ \omega_1 + \omega_2$ e $\gamma_4^-(t) = \alpha + t\ \omega_2$, $t \in [0,1]$, os caminhos inversos de γ_3 e γ_4, respectivamente, segue da conhecida igualdade $\int_\gamma f(z)dz = -\int_{\gamma^-} f(z)dz$ que

$$\begin{aligned}\int_{\partial P_\alpha} f(z)dz &= \int_0^1 f(\alpha + t\omega_1)\cdot\omega_1\ dt + \int_0^1 f(\alpha + \omega_1 + t\cdot\omega_2)\cdot\omega_2\ dt \\ &- \int_0^1 f(\alpha + t\cdot\omega_1 + \omega_2)\cdot\omega_1\ dt - \int_0^1 f(\alpha + t\cdot\omega_2)\cdot\omega_2\ dt = 0,\end{aligned}$$

pois f é Ω-periódica.

□

Teorema 2.1.5. *Sejam f uma função elíptica e P_α um paralelogramo fundamental que não contém zeros e polos de f na fronteira ∂P_α de P_α. Sejam $m_1, \ldots, m_k$ as ordens dos zeros e dos pólos de f no interior de P_α. Então*

$$\sum_{i=1}^{k} m_i = 0.$$

Demonstração. Como f é uma função elíptica, temos que $\frac{f'(z)}{f(z)} = \frac{f'(z+\omega)}{f(z+\omega)}$, $\forall \omega \in \Omega$ e para todo $z \in \mathbb{C}$ que não seja zero nem pólo de f.

Agora, seja z_i um zero de f, com ordem m_i. Sabemos (da demonstração do Teorema dos Resíduos) que existe uma vizinhança V de z_i tal que $f(z) = (z - z_i)^{m_i} g(z)$, $\forall z \in V$, com g holomorfa em V e $g(z_i) \neq 0$. Daí temos

$$\frac{f'(z)}{f(z)} = \frac{m_i}{z - z_i} + G(z),$$

onde $G(z) = \frac{g'z)}{g(z)}$, G holomorfa em V e $G(z_i) \neq 0$. O mesmo processo pode ser aplicado para cada pólo de f. Dessa forma, vemos que os resíduos da função elíptica f'/f no interior de P_α são exatamente as ordens dos zeros e dos pólos de f nessa região, contados com multiplicidades.

Assim, pelo Teorema anterior segue que

$$0 = \int_{\partial P_\alpha} \frac{f'(z)}{f(z)} dz = \sum_{i=1}^{k} m_i,$$

como queríamos.

□

Segue do Teorema 2.1.5 acima que o número de zeros e o número de polos de f em um paralelogramo fundamental, ambos contados com multiplicidades, coincidem. Isto nos permite definir a *ordem de uma função elíptica* f como sendo o número de zeros (ou de polos) de f em um paralelogramo fundamental P, contados com multiplicidades. É claro que se $u \in \mathbb{C}$, as ordens de f e de $f - u$ são iguais. Em particular, f assume o valor u em um paralelogramo fundamental exatamente o número de vezes igual a ordem de f.

Teorema 2.1.6. *Nas condições do teorema anterior, para os zeros e polos $z_1, \ldots, z_k$ de f com ordens $m_1, \ldots, m_k$, respectivamente, tem-se*

$$\sum_{i=1}^{k} m_i z_i \equiv 0 \ mod(\Omega).$$

Demonstração. Como foi visto na demonstração do Teorema 2.1.5, se z_j é um zero de f de multiplicidade m_j em uma vizinhança V de z_j podemos escrever

$$\frac{f'(z)}{f(z)} = \frac{m_j}{z - z_j} + G(z),$$

onde G é holomorfa em V e $G(z_j) \neq 0$. Daí segue que

$$z\frac{f'(z)}{f(z)} = \frac{z_j m_j}{z - z_j} + m_j + zG(z).$$

Analogamente para o caso em que z_j é um polo de f.

Considerando um paralelogramo fundamental P_α como no Teorema 2.1.5, obtemos

$$\int_{\partial P_\alpha} z\frac{f'(z)}{f(z)}dz = 2\pi i \sum_{j=1}^{k} m_j z_j.$$

Para calcular o termo do lado esquerdo dessa igualdade consideremos inicialmente os caminhos γ_1 e γ_3 do Teorema 2.1.4, observando que este é o caminho $\gamma_1 + \omega_2$ no sentido contrário. Daí, usando a mudança de variável $u = z + \omega_2$ e que f é periódica em Ω, temos

$$\begin{aligned}\int_{\gamma_1} z\frac{f'(z)}{f(z)}dz &= \int_{\gamma_1} (z+\omega_2)\frac{f'(z)}{f(z)}dz - \int_{\gamma_1} \omega_2\frac{f'(z)}{f(z)}dz \\ &= -\int_{\gamma_3} u\frac{f'(u)}{f(u)}du - \int_{\gamma_1} \omega_2\frac{f'(z)}{f(z)}dz.\end{aligned}$$

Portanto

$$\int_{\gamma_1} z\frac{f'(z)}{f(z)}dz + \int_{\gamma_3} z\frac{f'(z)}{f(z)}dz = \omega_2(2\pi i k_2),$$

para algum inteiro k_2 já que $\log f(\alpha + \omega_1) = \log f(\alpha)$.

Procedendo analogamente em relação aos caminhos γ_2 e γ_4, obtemos, para algum $k_1 \in \mathbb{Z}$,

$$\int_{\gamma_2} z\frac{f'(z)}{f(z)}dz + \int_{\gamma_4} z\frac{f'(z)}{f(z)}dz = 2\pi i k_1 \omega_1.$$

Segue dessas considerações que

$$\int_{\partial P_\alpha} z\frac{f'(z)}{f(z)}dz = 2\pi i \sum m_i z_i = 2\pi i(k_1\omega_1 + k_2\omega_2),$$

donde segue o resultado.

□

Os teoremas acima são provados em ([5], p.74-78), e serão de fundamental importância para a demonstração de resultados do capítulo 3. Dois deles se referem à uma função elíptica especial. O primeiro mostra que juntamente com sua derivada, esta função gera todo o corpo M_Ω. Além disso, por meio de tal função obtemos um objeto geométrico em $\mathbb{C} \times \mathbb{C}$ denominado curva elíptica afim. As curvas obtidas dessa forma possuem uma estreita relação com os reticulados complexos.

2.2 Formas Modulares de Peso Inteiro

Como já fizemos na demonstração da Proposição 1.1.1, cada elemento $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma(1)$ pode ser visto como uma transformação linear fracionária, da forma

$$A(\tau) = \frac{a\tau + b}{c\tau + d},\ \tau \in \mathbb{C}.$$

Podemos de forma natural considerar $A(\tau)$ no plano complexo estendido $\overline{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$, $A(\infty) = \frac{a}{c}$ e $A(-\frac{d}{c}) = \infty$ se $c \neq 0$; $A(\infty) = \infty$, se $c = 0$.

Dadas quaisquer duas matrizes $A, B \in \Gamma(1)$, $A(B(\tau)) = (A \cdot B)(\tau)$ e também $(-A)(\tau) = A(\tau)$, $\tau \in \mathcal{H}$. Essa última igualdade nos diz que A e $-A$ determinam uma mesma transformação linear fracionária. Na verdade, temos que

$$PSL_2(\mathbb{R}) = \frac{SL_2(\mathbb{R})}{\{\pm I\}} \simeq Aut(\mathcal{H}),$$

onde $Aut(\mathcal{H})$ é grupo das aplicações conformes em $\mathcal{H}$. A Proposição 1.2.1 nos diz que $Aut(\mathcal{H})$ é gerado pelas transformações $T(\tau) = \tau + 1$ e $S(\tau) = -\frac{1}{\tau}$.

Definiremos um tipo especial de aplicações de $\mathcal{H}$ em $\mathbb{C}$ e depois apresentaremos dois exemplos em particular, fundamentais na sequência deste trabalho. Nossa abordagem aqui se assemelha àquela feita em [2] e em [6].

Definição 2.2.1. *Seja $k \in \mathbb{Z}$. Uma função meromorfa $f : \mathcal{H} \longrightarrow \mathbb{C}$ é fracamente modular de peso k em $\Gamma(1)$ se*

$$f(A(\tau)) = (c\tau + d)^k f(\tau),\ \forall \tau \in \mathcal{H} \text{ e para cada } A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma(1).$$

Observações

- Uma função fracamente modular de peso $k \in \mathbb{Z}$ em $\Gamma(1)$ está bem definida, pois vimos na demonstração da Proposição 1.2.1 que se $\tau \in \mathcal{H}$ então $A(\tau) \in \mathcal{H}$, já que $Im(A(\tau)) = \frac{Im(\tau)}{|c\tau+d|^2} > 0$. E como $\Gamma(1)$ é gerado pelas matrizes T e S, para verificar que f é fracamente modular de peso k em $\Gamma(1)$, basta verificar que $f(T(\tau)) = f(\tau)$ e $f(S(\tau)) = \tau^k f(\tau)$, $\forall \tau \in \mathcal{H}$.

- Se $k = 0$ então isso significa que f é $\Gamma(1)$-invariante, isto é, $f(A(\tau)) = f(\tau)$, $\forall \tau \in \mathcal{H}$ e $\forall A \in \Gamma(1)$.

- Como $-I = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \in \Gamma(1)$, então $(-1)^k f(\tau) = f(-I(\tau)) = f(\tau),\ \forall \tau \in \mathcal{H}$. Segue daí que se k é ímpar, então $f \equiv 0$. Em contextos mais gerais, de subgrupos Γ de $\Gamma(1)$ de índices finito onde $-I \notin \Gamma$, entretanto, existem formas modulares de peso ímpar.

- Como o fator $(c\tau + d)^k$ não possui zeros nem pólos em $\mathcal{H}$, segue que f e $f \circ A$ possuem a mesma quantidade de zeros e de pólos, $\forall A \in \Gamma(1)$.

Uma função fracamente modular de peso inteiro em $\Gamma(1)$ pode ser definida sobre o ponto infinito. Noutras palavras, podemos definir f sobre o conjunto $\mathcal{H}^* = \mathcal{H} \cup \{\infty\}$. É o que faremos abaixo.

Primeiramente, consideremos a mudança de variáveis dada pela aplicação $h : \mathcal{H} \longrightarrow \mathbb{C}$, $h(\tau) = e^{2\pi i \tau} = q$. Definimos um sistema fundamental de vizinhanças do ponto infinito para cada número real $r > 0$,

$$V_r = \{\tau \in \mathcal{H};\ Im(\tau) > r\}.$$

Por meio de h, obtemos um sistema de vizinhanças de zero, da forma $B(0,s)^* = B(0,s)\backslash\{0\}$, onde $B(0,s)$ é a bola aberta de centro em 0 e raio s. Temos que $B(0,s)^* \subset D^*$, onde D é o disco unitário aberto e $D^* = D\backslash\{0\}$. Então, para a aplicação f, definimos $g : D^* \longrightarrow \mathbb{C}$ por $g(q) = f(\log(q)/2\pi i)$. Como a função logaritmo é $2\pi i\mathbb{Z}$-periódica, segue que g é bem definida.

Assim, sendo f uma função fracamente modular de peso k em $\Gamma(1)$, dizemos que f é meromorfa (respectivamente, holomorfa) no ∞ se g é meromorfa (respectivamente, holomorfa) no 0. Em caso afirmativo, f pode ser expressa por uma série de potências na variável q, ou seja

$$f(\tau) = g(q) = \sum_{n \geq n_0}^{\infty} a_n q^n,\ a_n \in \mathbb{C},\ n_0 \in \mathbb{Z},$$

(respectivamente, $n_0 = 0$).

Se $\tau = x + iy$, então $q = e^{-2\pi y} e^{2\pi i x}$, logo q converge para zero se e somente se $Im(\tau)$ converge para ∞. Daí para mostrar que uma função f é holomorfa em ∞ basta mostrar que existe o limite $\lim_{Im(\tau)\to\infty} f(\tau)$, ou apenas que f é limitada se $Im(\tau)$ é suficientemente grande.

É possível também definir um sistema fundamental de vizinhanças próximo à qualquer ponto $\frac{a}{c} \in \mathbb{Q}$, $mdc\{a,c\} = 1$. De fato, como a e c são inteiros primos entre si, existem $b, d \in \mathbb{Z}$ tais que $ad - bc = 1$. Definindo $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, segue que $A(\infty) = \frac{a}{c}$, isto é, $\lim_{Im(\tau)\to\infty} A(\tau) = \frac{a}{c}$. É possível então utilizar a matriz A para transportar uma vizinhança V_r à um disco tangente ao eixo real em $\frac{a}{c}$. Esse disco é um sistema de vizinhaças para $\frac{a}{c}$ ([6], p. 104-105).

Definição 2.2.2. *Dado $k \in \mathbb{Z}$, uma função $f : \mathcal{H} \longrightarrow \mathbb{C}$ é uma forma modular de peso k se f é fracamente modular de peso k e se é holomorfa em $\mathcal{H}^*$. Se $a_0 = 0$ na expansão em série de f descrita acima, então f é uma forma cuspidal de peso k.*

O conjunto das formas modulares de peso k é um espaço vetorial denotado por $\mathcal{M}_k(\Gamma(1))$, que possui dimensão finita devido ao fato de cada forma modular de peso k ser holomorfa em ∞ ([2], p. 4 e p. 87-88). O conjunto $\mathcal{S}_k(\Gamma(1))$ das formas cuspidais de peso k é um subespaço vetorial de $\mathcal{M}_k(\Gamma(1))$. Como o produto de formas modulares de pesos k e l produz uma outra forma modular de peso $k+l$, o conjunto $\mathcal{M}(\Gamma(1)) = \bigoplus_{k\in\mathbb{Z}} \mathcal{M}_k(\Gamma(1))$ de todas as formas modulares de peso inteiro forma um anel graduado, no qual $\mathcal{S}(\Gamma(1)) = \bigoplus_{k\in\mathbb{Z}} \mathcal{S}_k(\Gamma(1))$ é um subanel.

2.2.1 Dois Exemplos Importantes

A Série de Eisenstein

O primeiro exemplo de forma modular em $\Gamma(1)$ é a *série de Eisenstein* $G_k : \mathcal{H} \longrightarrow \mathbb{C}$ ($k > 2$ par) dada por

$$G_k(\tau) = \sum_{(c,d)^*} \frac{1}{(c\tau + d)^k},$$

onde a notação $(c, d)^*$ significa que a soma contabiliza os pares $(c, d) \in (\mathbb{Z} \times \mathbb{Z}) - \{(0, 0)\}$.

Estas séries são importantes pois, como veremos no capítulo 3, aparecerão como coeficientes de polinômios que definirão curvas elípticas. Como G_k é uma função de $\tau \in \mathcal{H}$, tais polinômios dependerão essencialmente de $\tau \in \mathcal{H}$.

Proposição 2.2.3. *Para qualquer número inteiro $k > 2$ par, $G_k \in \mathcal{M}_k(\Gamma(1))$.*

Demonstração. Vamos primeiramente mostrar que G_k é absolutamente convergente.

Para cada $\tau \in \mathcal{H}$ e cada $n \in \mathbb{N}$, considere $L_{\tau,n} = \{a\tau + b;\ a, b \in \mathbb{R},\ max\{|a|, |b|\} = n\}$ e $\Omega_{\tau,n} = \Omega_\tau \cap L_{\tau,n}$. Claramente $\Omega^*_\tau = \cup_{n\in\mathbb{N}} \Omega_{\tau,n}$.

Chamemos de m e M a menor e a maior norma entre os elementos de Ω_τ, respectivamente. Em $\Omega_{\tau,1}$, temos

$$0 < m \leq |a\tau + b| \leq M \Rightarrow \frac{1}{M^k} \leq \frac{1}{|a\tau + b|^k} \leq \frac{1}{m^k},$$

e similarmente, para $\Omega_{\tau,n}$, temos

$$0 < nm \leq |a\tau + b| \leq nM \Rightarrow \frac{1}{(nM)^k} \leq \frac{1}{|a\tau + b|^k} \leq \frac{1}{(nm)^k}.$$

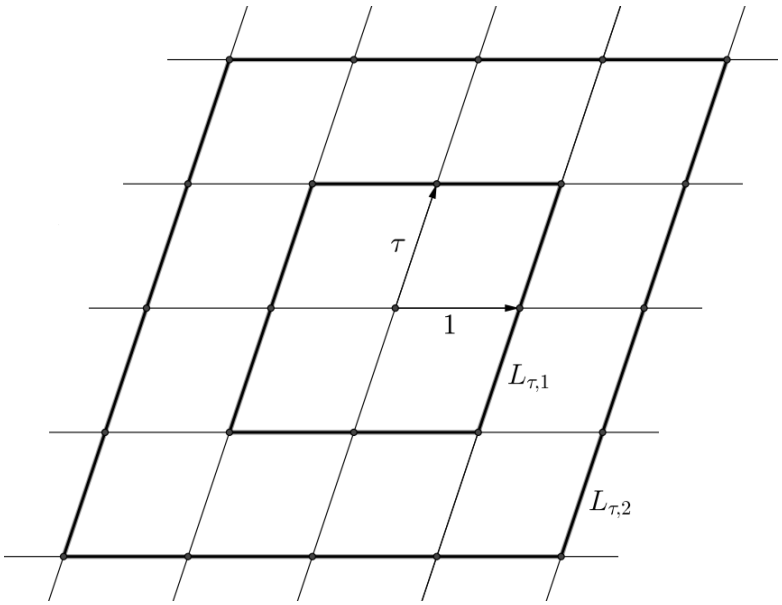

Figura 2.3: Conjuntos $L_{\tau,1}$ e $L_{\tau,2}$.

Chamando de $\Sigma_n = \sum_n \frac{1}{|a\tau+b|^k}$ a soma parcial dos inversos das normas elevadas à k de todos os elementos em $\Omega_{\tau,1}, \ldots, \Omega_{\tau,n}$, $n \in \mathbb{N}$, temos

$$\begin{aligned}
\frac{8}{M^k} + 2\frac{8}{(2M)^k} + \ldots + n\frac{8}{(nM)^k} \leq &\ \Sigma_n \ \leq \frac{8}{m^k} + 2\frac{8}{(2m)^k} + \ldots + n\frac{8}{(nm)^k} \\
\frac{8}{M^k}\Big(1 + \frac{1}{2^{k-1}} + \ldots + \frac{1}{n^{k-1}}\Big) \leq &\ \Sigma_n \ \leq \frac{8}{m^k}\Big(1 + \frac{1}{2^{k-1}} + \ldots + \frac{1}{n^{k-1}}\Big) \\
\frac{8}{M^k}\sum_{i=1}^{n}\frac{1}{i^{k-1}} \leq &\ \Sigma_n \ \leq \frac{8}{m^k}\sum_{i=1}^{n}\frac{1}{i^{k-1}}
\end{aligned}$$

Como n é arbitrariamente escolhido, segue que Σ_n é limitada superiormente por $\frac{8}{m^k}\zeta(k-1)$, onde ζ é a conhecida função zeta de Riemann. Como $k > 2$, segue que Σ_n é convergente, ou seja, G_k é absolutamente convergente.

Agora, dado $\tau_0 \in \mathcal{H}$ fixo, seja $\delta = \frac{1}{2}Im(\tau_0)$ e considere $D(\tau_0) = \{\tau \in \mathcal{H};\ |\tau - \tau_0| \leq \delta\}$. Dados $c, d \in \mathbb{Z}$, $c \neq 0$, temos $|d/c + \tau_0| \geq Im(\tau_0) = 2\delta$, daí para cada $\tau \in D(\tau_0)$ temos

$$|c\tau + d - (c\tau_0 + d)| = |c||\tau - \tau_0| \leq |c|\delta \leq \frac{1}{2}|c\tau_0 + d|,$$

e pela desigualdade triangular

$$|c\tau + d| \geq |c\tau_0 + d| - |c\tau + d - (c\tau_0 + d)| \geq \frac{1}{2}|c\tau_0 + d|.$$

Assim, dados o inteiro par $k > 2$, $\tau \in \mathcal{H}$, $(c, d) \in \mathbb{Z}^2$, $c \neq 0$, segue que

$$|c\tau + d|^{-k} \leq 2^k |c\tau_0 + d|^{-k}.$$

Agora, escreva $G_k(\tau) = \sum_{c\in\mathbb{Z}} f_c(\tau)$, onde $f_c(\tau) = \sum_{d\in\mathbb{Z}} \frac{1}{(c\tau+d)^k}$. Para cada $c \in \mathbb{Z}$, como $D(\tau_0)$ é compacto e cada $(c\tau+d)^{-k}$ pode ser visto como uma função contínua em $\mathcal{H}$, segue da convergência de G_k que f_c é uma função contínua. Dessa forma, pela desigualdade acima e pela convergência de G_k, segue do Teste M de Weierstrass ([5], p. 81) que G_k converge uniformemente em subconjuntos compactos de $\mathcal{H}$. Como cada parcela da somatória é uma função analítica em $\mathcal{H}$, segue que G_k é analítica.

Temos também

$$G_k(\tau+1) = \sum_{(c,d)^*} \frac{1}{(c(\tau+1)+d)^k} = \sum_{(c,d')^*} \frac{1}{(c\tau+d')^k} = G_k(\tau)$$

e

$$\tau^{-k}G_k(-1/\tau) = \tau^{-k}\sum_{(c,d)^*} \frac{1}{\left(c(-\frac{1}{\tau})+d\right)^k} = \tau^{-k}\sum_{(c,d)^*} \frac{\tau^k}{(d\tau-c)^k} = \sum_{(c,d)^*} \frac{1}{(d\tau-c)^k} = G_k(\tau).$$

Assim segue que G_k é fracamente modular de peso k. E como G_k converge uniformemente em compactos de $\mathcal{H}$, $\lim_{Im(\tau)\to\infty} \frac{1}{(c\tau+d)^k} = 0$, se $c \neq 0$, e $\lim_{Im(\tau)\to\infty} \frac{1}{(c\tau+d)^k} = \frac{1}{d^k}$, se $c = 0$, então

$$\lim_{Im(\tau)\to\infty} G_k(\tau) = \lim_{Im(\tau)\to\infty} \sum_{(c,d)^*} \frac{1}{(c\tau+d)^k} = \sum_{d\in\mathbb{Z}} \frac{1}{|d|^k} = 2\zeta(k).$$

Portanto G_k é holomorfa em ∞, donde concluímos que G_k é uma forma modular de peso k.

□

Um outro fato interessante sobre G_k é que sua série de Fourier é

$$G_k(\tau) = 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!}\sum_{n=1}^{\infty} \sigma_{k-1}(n)q^n,$$

onde $\sigma_{k-1}(n) = \sum_{\substack{m|n \\ m>0}} m^{k-1}$ ([2], p. 5). A *série de Eisenstein normalizada* é $E_k : \mathcal{H} \longrightarrow \mathbb{C}$, $E_k(\tau) = \frac{G_k(\tau)}{2\zeta(k)}$. Por fim, $\mathcal{M}(\Gamma(1)) = \mathbb{C}[E_4, E_6]$ e $\mathcal{S}(\Gamma(1)) = \Delta\mathcal{M}(\Gamma(1))$ ([2], p. 88), onde Δ é a função discriminante e será definida abaixo.

O Invariante Modular j

Sejam $g_2, g_3 : \mathcal{H} \longrightarrow \mathbb{C}$ as funções definidas por $g_2(\tau) = 60G_4(\tau)$ e $g_3(\tau) = 140G_6(\tau)$, e seja $\Delta : \mathcal{H} \longrightarrow \mathbb{C}$ a função *discriminante* definida por $\Delta(\tau) = (g_2(\tau))^3 - 27(g_3(\tau))^2$.

Como G_4 e G_6 são formas modulares de peso $k = 4$ e $k = 6$, respectivamente, segue que Δ é uma forma modular de peso $k = 12$, e no desenvolvimento em série de Fourier de Δ (em q)

temos $a_0 = 0$ e $a_1 = (2\pi)^{12}$. Então $\Delta \in \mathcal{S}_{12}(\Gamma(1))$. No capítulo 3 será mostrado que $\Delta(\tau) \neq 0$, $\forall \tau \in \mathcal{H}$, e pela expansão em série (em q), temos que $\tau \to \infty$ implica $\Delta(\tau) \to 0$.

O *invariante modular* $j : \mathcal{H} \longrightarrow \mathbb{C}$ é definido por

$$j(\tau) = 1728\frac{(g_2(\tau))^3}{\Delta(\tau)} \tag{2.1}$$

Como g_2 e Δ são holomorfas em $\mathcal{H}$ e $\Delta(\tau) \neq 0$, $\forall \tau \in \mathcal{H}$, o invariante modular j é uma função holomorfa e de peso $k = 0$ em $\mathcal{H}$, mas pelo que vimos acima não é holomorfa em ∞. Logo j é uma função fracamente modular, mas não é uma forma modular, pois possui um pólo em ∞ de ordem 1 ([2], p. 73). A aplicação j também possui um zero em $\rho = e^{2\pi i/3}$, pois $g_2(S(\rho)) = \rho^4 g_2(\rho)$ e $g_2(S(\rho)) = g_2(\rho)$ e $\rho \neq 1$ e sua série de Fourier em q é dada por $j(\tau) = q^{-1} + 744 + 196884q + \sum_{n=2}^{\infty} a_n q^n$, conforme ([2], p. 73) e ([5], p. 282). Como é provado também em ([2], p. 73), o corpo das funções modulares de peso $k = 0$ em $\mathcal{H}^*$ é $\mathbb{C}(j)$.

Afirmamos agora que j é sobrejetiva. Com efeito, supondo o contrário, deve existir $c \in \mathbb{C}$ tal que função $h : \mathcal{H} \longrightarrow \mathbb{C}$ dada por $h(\tau) = j(\tau) - c$ nunca se anula. Além disso, o único pólo de h é ∞.

Considere o caminho da figura abaixo. A escolha deste caminho e o motivo pelo qual ele é suficiente serão justificados na seção 4.2 (especificamente no Teorema 4.2.1).

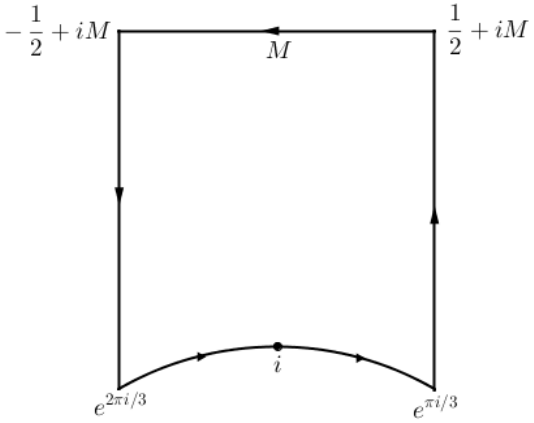

Figura 2.4: Caminho γ.

Pelas propriedades de h referidas acima, segue do Princípio do Argumento que

$$0 = \frac{1}{2\pi i}\int_{\gamma} \frac{j'(\tau)}{j(\tau) - c} d\tau.$$

Por outro lado, considerando a simetria entre os caminhos dados pelas retas verticais e os semicírculos, e a modularidade da função j, segue que $0 = \int_{\gamma'} \frac{j'(\tau)}{j(\tau)-c} d\tau$, onde $\gamma'(t) = \frac{1-2t}{2} + iM$, $t \in [0, 1]$ é o caminho horizontal na figura acima.

Efetuando a mudança $\tau \mapsto q = e^{2\pi i\tau}$, a integral acima torna-se $\int_{c'} \frac{f'(q)}{f(q)-c}dq$, na qual a função $f : D\backslash\{0\} \longrightarrow \mathbb{C}$ é dada por $f(q) = j(\tau) = \frac{1}{q} + \sum_{n=0}^{\infty} a_n q^n$ e c' é o caminho circular em torno de zero obtido após a mudança de variáveis acima. Tomando M suficientemente grande segue do Princípio do Argumento e do fato do caminho c' estar no sentido horário que

$$0 = \frac{1}{2\pi i}\int_{c'} \frac{f'(q)}{f(q)-c}dq = 1,$$

um absurdo.

Uma propriedade importante da função j é que $j(A(\tau)) = j(\tau),\ \forall A \in \Gamma(1)$ e $\forall \tau \in \mathcal{H}$, como facilmente podemos constatar. Isso nos permitirá utilizar a função j como invariante para caracterizarmos os reticulados homotéticos (e também toros complexos e curvas elípticas isomorfas), conforme veremos no capítulo 4.

Formas Modulares em Γ

O conceito de formas modulares pode ser estendido para subgrupos Γ de $\Gamma(1) = SL_2(\mathbb{Z})$. Dados k um inteiro positivo e Γ um subgrupo de $\Gamma(1)$, uma função meromorfa $f : \mathcal{H} \longrightarrow \mathbb{C}$ é dita *fracamente modular de peso k para* Γ se dada $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma$, tem-se

$$f(M(\tau)) = (c\tau + d)^k f(\tau),\ \tau \in \mathcal{H}.$$

O próximo passo rumo à definição de forma modular de peso k para Γ é determinar uma condição para que f seja holomorfa nos chamados *pontos cuspidais de* Γ, que são as classes de cada ponto $\tau \in \overline{\mathcal{H}} = \mathcal{H}^* \cup \mathbb{Q} = \mathcal{H} \cup \{\infty\} \cup \mathbb{Q}$ via ação de Γ e será mencionadas no capítulo 4. A maneira como tal condição é obtida pode ser encontrada em ([2], p. 16-17) e ([6], p. 124-126).

Capítulo 3

TOROS COMPLEXOS E A FUNÇÃO $\wp$ DE WEIERSTRASS

Neste terceiro capítulo trataremos de dois objetos importantes desse trabalho. Na primeira seção trataremos dos chamados toros complexos, que são grupos obtidos considerando o quociente de $\mathbb{C}$ por um reticulado Ω. Nossa abordagem será baseada na terceira seção do capítulo 1 de [2]. Na segunda seção estudaremos a função $\wp$ de Weierstrass, uma função elíptica especial por meio da qual podemos caracterizar todo o corpo M_Ω das funções elípticas em relação a um reticulado Ω. E também podemos obter um objeto geométrico chamado curva elíptica, que será tratado no capítulo seguinte. Maiores detalhes com relação à função $\wp$ podem ser vistos em [5] e em [6].

3.1 Os Toros Complexos

Dado um reticulado $\Omega = [\omega_1, \omega_2]$ em $\mathbb{C}$, considere a seguinte relação: dados $z_1, z_2 \in \mathbb{C}$,

$$z_1 \sim z_2 \iff z_1 - z_2 \in \Omega.$$

É fácil verificar que $\sim$ é uma relação de equivalência. O conjunto $\mathbb{T}_\Omega = \mathbb{C}/\Omega = \{z + \Omega;\ z \in \mathbb{C}\}$ das classes de equivalência pela relação acima é chamado de *Toro Complexo*.

Podemos observar que algebricamente o toro complexo é um grupo abeliano, considerando a soma de classes de equivalência. Já no aspecto geométrico, o toro complexo pode ser identificado com a região do plano complexo limitada um palalelogramo determinado por ω_1 e ω_2, cujos lados opostos são identificados por meio da relação de equivalência mencionada. Identificando

um desses pares, obtemos a partir do paralelogramo um tubo; fazendo o mesmo com o outro par do tubo obtemos uma superfície topologicamente conhecida como *toro*, que dá nome ao conjunto $\mathbb{T}_\Omega$.

O toro complexo como definido acima possui uma estrutura algébrica, mas também possui uma estrutura analítica oriunda do próprio conjunto $\mathbb{C}$. Isso reside no fato de que qualquer disco aberto em torno de um ponto $z+\Omega \in \mathbb{T}_\Omega$ é imagem via a projeção canônica $\rho_\Omega : z \mapsto z+\Omega$ de um conjunto enumerável de discos abertos em $\mathbb{C}$, cujos centros são pontos da forma $z+\omega$, $\omega \in \Omega$. A Figura 3.1 nos mostra isso de maneira esquemática.

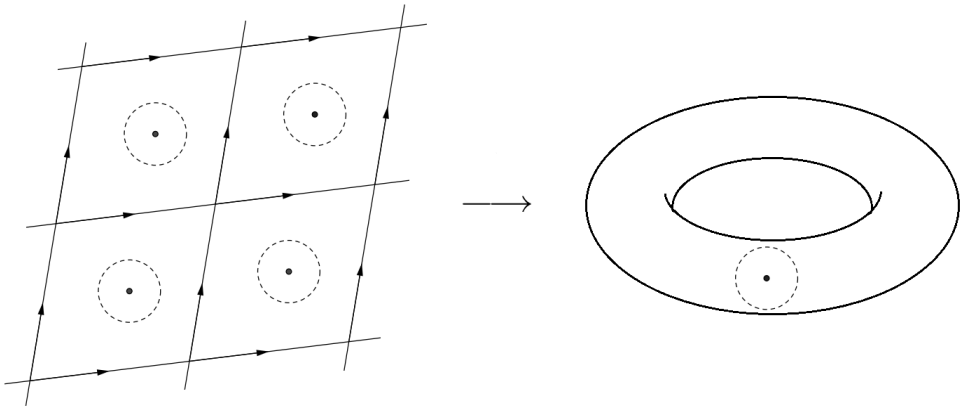

Figura 3.1: Discos abertos em $\mathbb{C}$ e em $\mathbb{T}_\Omega$.

Um toro complexo também possui estrutura analítica de Superfície de Riemann, e é por meio da utilização dessa estrutura que é possível provar os dois próximos resultados, os quais caracterizam completamente os homomorfismos entre toros complexos. Como, porém, não é foco deste trabalho, omitiremos as demonstrações. As mesmas podem ser encontradas em ([2], p. 26) e em ([5], p. 71).

Proposição 3.1.1. *Se $\varphi : \mathbb{T}_\Omega \longrightarrow \mathbb{T}_{\Omega'}$ é uma função holomorfa entre toros complexos, então existem $m, b \in \mathbb{C}$, com $m\Omega \subset \Omega'$, tais que*

$$\varphi(z+\Omega) = mz + b + \Omega'.$$

A aplicação é invertível se, e somente se, $m\Omega = \Omega'$.

Corolário 3.1.2. *Se $\varphi : \mathbb{T}_\Omega \longrightarrow \mathbb{T}_{\Omega'}$, $\varphi(z+\Omega) = mz + b + \Omega'$, com $m\Omega \subset \Omega'$, é uma aplicação holomorfa entre toros complexos, então as afirmações seguintes são equivalentes:*

(a) φ é um homomorfismo de grupos;

(b) Se $b \in \Omega'$, então $\varphi(z + \Omega) = mz + \Omega'$.

(c) $\varphi(0 + \Omega) = 0 + \Omega'$.

Em particular, existe um homomorfismo não-nulo holomorfo de grupos entre toros complexos $\mathbb{T}_\Omega$ e $\mathbb{T}_{\Omega'}$ se, e somente se, existe algum $m \in \mathbb{C}^*$ tal que $m\Omega \subset \Omega'$. Existe um isomorfismo de grupos holomorfo entre toros complexos $\mathbb{T}_\Omega$ e $\mathbb{T}_{\Omega'}$ se, e somente se, existe $m \in \mathbb{C}^*$ tal que $m\Omega = \Omega'$.

Como pode ser facilmente constatado, se $m\Omega = \Omega'$, então o Corolário 3.1.2 garante que o diagrama abaixo é comutativo:

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{m} & \mathbb{C} \\ \downarrow{\scriptstyle \rho_\Omega} & & \downarrow{\scriptstyle \rho_{\Omega'}} \\ \mathbb{T}_\Omega & \xrightarrow{\varphi} & \mathbb{T}_{\Omega'} \end{array}$$

onde $m : \mathbb{C} \longrightarrow \mathbb{C}$ é $m(z) = m \cdot z$ e as aplicações ρ_Ω e $\rho_{\Omega'}$ são as respectivas projeções canônicas.

Exemplo 3.1.3. *Vimos no final da Seção 1.1 que um reticulado $\Omega = [\omega_1, \omega_2]$ é equivalente ao reticulado Ω_ω, $\omega = \frac{\omega_2}{\omega_1}$. Segue então do Corolário 3.1.2 acima que a aplicação $\varphi_w : \mathbb{T}_\Omega \longrightarrow \mathbb{T}_{\Omega_w}$ dada por $\varphi(z + \Omega) = \frac{z}{\omega_1} + \Omega_w$ é um isomorfismo de toros complexos.*

O exemplo acima mostra que podemos separar os toros complexos de acordo com as órbitas da ação de $SL_2(\mathbb{Z})$. Isso ocorrerá, como veremos no próximo capítulo, também para as curvas elípticas.

3.2 A Função $\wp$ de Weierstrass

Na seção 2.1 estudamos as funções elípticas em caráter geral. Ao final daquela seção dissemos que existia uma função elíptica por meio da qual (juntamente com sua derivada complexa) é possível caracterizar o corpo M_Ω das funções elípticas em relação ao reticulado Ω. A função $\wp$ de Weierstrass que estudaremos nessa seção é a função referida. Pelo que vimos na seção anterior e será confirmado nesta seção, a própria definição de função elíptica permite entender cada $f \in M_\Omega$ como uma função cujo domínio é o toro complexo $\mathbb{T}_\Omega$.

Para um reticulado $\Omega = [\omega_1, \omega_2]$, a *função $\wp$ de Weierstrass* é definida por

$$\wp_\Omega(z) = \frac{1}{z^2} + \sum_{\omega \in \Omega^*} \Big(\frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \Big) \tag{2.1}$$

onde $\Omega^* = \Omega - \{0\}$, $z \in \mathbb{C} - \Omega$.

Quando não houver necessidade de mais detalhes, denotaremos $\wp = \wp_\Omega$. Temos que $\wp$ é uma série absolutamente e uniformemente convergente em subconjuntos compactos de $\mathbb{C} - \Omega$. Além disso, $\wp$ é analítica em $\mathbb{C} - \Omega$ e possui pólos de ordem 2 em cada ponto de Ω ([5], seção 3.9). Assim, temos a derivada de $\wp$

$$\wp'(z) = -2\sum_{\omega\in\Omega} \frac{1}{(z-\omega)^3}.$$

Também de acordo com [5], $\wp'$ é absolutamente e uniformemente convergente em subconjuntos compactos de $\mathbb{C}$, e como podemos ver $\wp'$ possui pólos de ordem 3 em cada ponto de Ω.

Observamos inicialmente que $\wp'$ é uma função ímpar e periódica em relação à Ω e que $\wp$ é uma função par. Segue então da periodicidade de $\wp'$ que $\wp(z+\omega_i)-\wp(z) = z_0 \in \mathbb{C},\ \forall z \in \mathbb{C}-\Omega$, com $i \in \{1,2\}$. E tomando $z = -\frac{1}{2}\omega_i$ na equação anterior, como $\wp$ é par temos $z_0 = 0$. Assim a função $\wp$ também é periódica em relação à Ω.

Segue dessas observações que $\wp$ e $\wp'$ pertencem ao corpo M_Ω das funções elípticas em relação à Ω. Especificamente, $\wp \in M_\Omega^+$ e $\wp' \in M_\Omega^-$, onde M_Ω^+ e M_Ω^- denotam as funções elípticas pares e ímpares em Ω, respectivamente.

A fim de demonstrarmos outras propriedades das funções $\wp$ e $\wp'$, definimos a *série de Eisenstein generalizada* por

$$G_k(\Omega) = \sum_{\omega\in\Omega^*} \frac{1}{\omega^k},\ k > 2,\ k \text{ par.}$$

Como cada elemento em Ω é escrito da forma $a\omega_1 + b\omega_2,\ a, b \in \mathbb{Z}$, e a série G_k definida na Seção 2.2 é absolutamente convergente, temos que $G_k(\Omega) = \omega_2^{-k} G_k(\omega)$, onde $\omega = \frac{\omega_1}{\omega_2}$. Temos também que dado $m \in \mathbb{C}^*$, vale $G_k(m\Omega) = m^{-k}G_k(\Omega)$. Quando não houver necessidade de detalhes, denotaremos apenas $G_k(\Omega) = G_k$.

Teorema 3.2.1. *Seja $\wp$ a função de Weierstrass em relação ao reticulado $\Omega = [\omega_1, \omega_2]$. Então*

(a) Para todo z tal que $0 < |z| < inf\left\{|\omega|;\ \omega \in \Omega - \{0\}\right\}$,

$$\wp(z) = \frac{1}{z^2} + \sum_{n=2}^{\infty}(n+1)G_{n+2}z^n,\ n \text{ par.}$$

(b) As funções $\wp$ e $\wp'$ satizfazem a relação

$$(\wp'(z))^2 = 4(\wp(z))^3 - g_2\wp(z) - g_3,$$

onde $g_2 = g_2(\Omega) = 60G_4(\Omega)$ e $g_3 = g_3(\Omega) = 140G_6(\Omega)$.

(c) As funções $x = \wp(z)$ e $y = \wp'(z)$ satisfazem a equação

$$y^2 = 4(x - a_1)(x - a_2)(x - a_3),\ a_i = \wp(\omega_i/2),\ i \in \{1, 2, 3\},$$

onde $\omega_3 = \omega_1 + \omega_2$ e $a_i \neq a_j$, $i \neq j$.

Demonstração.

(a) Observemos que para $|z| < |\omega|$, temos

$$\begin{aligned}\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} &= \frac{1}{\omega^2}\left[\frac{1}{\left(1-\frac{z}{\omega}\right)^2} - 1\right] \\ &= \frac{1}{\omega^2}\sum_{n=1}^{\infty}(n+1)\left(\frac{z}{\omega}\right)^n,\end{aligned}$$

daí,

$$\begin{aligned}\wp(z) &= \frac{1}{z^2} + \sum_{\omega\in\Omega^*}\left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right) \\ &= \frac{1}{z^2} + \sum_{\omega\in\Omega^*}\frac{1}{\omega^2}\sum_{n=1}^{\infty}(n+1)\left(\frac{z}{\omega}\right)^n \\ &= \frac{1}{z^2} + \sum_{n=1}^{\infty}A_n z^n,\ \text{onde } A_n = \sum_{\omega\in\Omega^*}\frac{n+1}{\omega^{n+2}}.\end{aligned}$$

Observe que se n for ímpar então $A_n = 0$, pois para cada $\omega \in \Omega$ tem-se $-\omega \in \Omega$. E como para cada n par temos $A_n = (n+1)G_{n+2}$, segue o resultado.

(b) Considere a função

$$h(z) = (\wp'(z))^2 - 4(\wp(z))^3 + g_2\wp(z) + g_3.$$

Temos, pelo ítem anterior

$$\wp(z) = \frac{1}{z^2} + 3G_4 z^2 + 5G_6 z^4 + \hat{R}(z^6)$$

e

$$\wp'(z) = -\frac{2}{z^3} + 6G_4 z + 20G_6 z^3 + \bar{R}(z^5)$$

onde $\hat{R}(j)$ e $\bar{R}(j)$ significam os "termos de ordem maior ou igual à j".

Daí cálculos diretos mostram que

$$(\wp'(z))^2 = \frac{4}{z^6} + \frac{24G_4}{z^2} - 80G_6 + \hat{R}(z^2)$$

e

$$4(\wp(z))^3 - g_2\wp(z) - g_3 = \frac{4}{z^6} + \frac{24G_4}{z^2} - 80G_6 + \bar{R}(z^2).$$

Como as funções $\wp$ e $\wp'$ são meromorfas e Ω-periódicas, a função $h = \hat{R} - \bar{R}$ é holomorfa, Ω-periódica e é holomorfa. Logo, pelo teorema de Liouville h é constante. E como $\lim_{z\to 0} h(z) = 0$, segue o resultado.

(c) Observamos primeiramente que se $z \in \mathbb{C}$ é tal que $2z \in \Omega$ então temos $\wp'(z) = \wp'(z - 2z) = \wp'(-z) = -\wp'(z)$, e logo $\wp'(z) = 0$. Daí como cada $2z_i \in \Omega$, $z_i = \frac{\omega_i}{2}$, $i \in \{1, 2, 3\}$, temos $\wp'(z_i) = 0$, e como a função $\wp'$ possui ordem 3, segue que esses são os únicos zeros de $\wp'$.

Segue do ítem anterior que cada $a_i = \wp(z_i)$ é raíz do polinômio $P(X) = 4X^3 - g_2X - g_3$ em $\mathbb{C}[X]$. Afirmamos agora que cada a_i é um valor duplo de $\wp$. Fixando $i \in \{1, 2, 3\}$ e definindo $f : \mathbb{C}\backslash\Omega \longrightarrow \mathbb{C}$, $f(z) = \wp(z) - a_i$, segue imediatamente que f é uma função meromorfa, periódica em relação à Ω e possui ordem 2, igual à de $\wp$. Segue-se então que z_i é raíz de f e de f', e isso implica que a_i é um valor duplo de $\wp$.

Temos então $(\wp'(z))^2 = 4(\wp(z) - a_1)(\wp(z) - a_2)(\wp(z) - a_3)$. Se, por exemplo, $a_1 = a_2$, então o fator $(\wp(z) - a_1)^2$ teria ordem 4, o que implicaria que $\wp - a_i$ possuiria 4 zeros, um absurdo.

□

Observação 3.2.2.

(a) O terceiro ítem acima mostra que $\Delta(\Omega) = g_2^3 - 27g_3^2 \neq 0$. De fato, como o polinômio P não possui raízes múltiplas, o discriminante $\mathcal{D}(P) = 16\Delta(\Omega)$ não é nulo. Em particular, considerando o reticulado $\Omega_\tau = [1, \tau]$, temos $\Delta(\Omega_\tau) = \Delta(\tau) \neq 0$, $\forall \tau \in \mathcal{H}$.

(b) O polinômio $f(X, Y) = Y^2 - 4X^3 + g_2X + g_3$ é irredutível em $\mathbb{C}[X, Y]$. Caso contrário, considerando a igualdade $\mathbb{C}[X, Y] = \mathbb{C}[X][Y]$, como o grau de f em relação à variável Y é 2, teríamos $4X^3 - g_2X - g_3 = (r(X))^2$, para algum $r(X) \in \mathbb{C}[X]$, um absurdo.

Fixemos algumas notações. Dado $f \in M_\Omega$, sejam $\mathcal{S}_f$ o conjunto das singularidades de f, e $\mathcal{Z}_f$ e $\mathcal{N}_f$ os conjuntos dos zeros e dos pólos de f, respectivamente. Temos que $\mathcal{S}_f = \mathcal{Z}_f \cup \mathcal{N}_f$, e quando não houver risco de confusões, omitiremos os índices f, como faremos a seguir.

Lema 3.2.3.

(a) Seja $f \in M_\Omega^+$ uma função elíptica par. Se $z_0 \in \mathcal{Z}$, então $z_0^* = \omega_1 + \omega_2 - z_0 \in \mathcal{Z}$. Vale o análogo para $\mathcal{N}$.

(b) Dado $z \in \mathbb{C} - \Omega$, tal que $2z \in \Omega^*$, então $z - z_0 \in \Omega$, para algum $z_0 \in \{\frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2}\}$.

(c) Se $z \in \mathcal{S}$ é tal que $2z \in \Omega$, então z é um zero de f de ordem par.

(d) $\wp(u) = \wp(u') \Leftrightarrow u - u' \in \Omega$.

Demonstração. (a) Evidente, pois pela periodicidade e paridade de f, tem-se $f(z_0^*) = f(z_0)$.

(b) Dado z nas condições do enunciado acima, existem inteiros a e b, não ambos nulos, tais que $2z = a\omega_1 + b\omega_2$. Logo

$$z = \frac{a}{2}\omega_1 + \frac{b}{2}\omega_2.$$

Como $z \notin \Omega$, os inteiros a e b não podem ser simultaneamente pares. Caso eles sejam ambos ímpares, então

$$z - \Big(\frac{\omega_1 + \omega_2}{2}\Big) = \Big(\frac{a-1}{2}\Big)\omega_1 + \Big(\frac{b-1}{2}\Big)\omega_2 \in \Omega.$$

Caso a seja par e b seja ímpar, então

$$z - \frac{\omega_2}{2} = \frac{a}{2}\omega_1 + \Big(\frac{b-1}{2}\Big)\omega_2 \in \Omega.$$

O outro caso é análogo. Isso reforça o fato de que os únicos zeros de $\wp'$ em $\mathbb{T}_\Omega$ são $\frac{\omega_1}{2} + \Omega$, $\frac{\omega_2}{2} + \Omega$ e $\frac{\omega_3}{2} + \Omega$.

(c) Se f é par, então $f^{(k)}(z) = (-1)^k f^{(k)}(-z)$, $k \in \mathbb{N}$ e $z \in \mathbb{C}$. Dessa forma se $z \in \mathcal{Z}$ e $2z \in \Omega$, então

$$f^{(2k+1)}(z) = (-1)^{2k+1} f^{(2k+1)}(-z) = -f^{(2k+1)}(z) \Rightarrow f^{(2k+1)}(z) = 0.$$

Analogamente, se $z \in \mathcal{N}$, então $\left(\frac{1}{f}\right)^{(2k+1)}(z) = 0$.

(d) Caso contrário, a função $f(z) = \wp(z) - \wp(u) = \wp(z) - \wp(u')$ possuiria duas raízes, cada uma de ordem 2, o que é um absurdo, pois a ordem de $\wp$ é 2.

□

Teorema 3.2.4. *O corpo M_Ω das funções elípticas em Ω é gerado pelas funções $\wp$ e $\wp'$.*

Demonstração. É claro que $\mathbb{C}(\wp, \wp') \subset M_\Omega$. Descrevemos a seguir a estratégia que será utilizada para provar a outra inclusão.

Seja $f \in M_\Omega$. Observamos primeiramente que, para todo $z \in \mathbb{C}$,

$$f(z) = \frac{f(z) + f(-z)}{2} + \frac{f(z) - f(-z)}{2\wp'(z)}\wp'(z).$$

Como as funções $\frac{f(z)+f(-z)}{2}$ e $\frac{f(z)-f(-z)}{2\wp'(z)}$ são pares, se provarmos que o conjunto das funções elípticas pares M_Ω^+ é gerado por $\wp$, então teremos que $\{1, \wp'\}$ será um sistema de geradores do espaço vetorial M_Ω sobre $\mathbb{C}(\wp)$. Daí $dim_{\mathbb{C}(\wp)} M_\Omega \leq 2$, e do ítem (b) da Observação 3.2.2, que nos dá $[\mathbb{C}(\wp, \wp') : \mathbb{C}(\wp)] = 2$, teremos $M_\Omega = \mathbb{C}(\wp, \wp')$.

Tomemos então $f \in M_\Omega^+ - \{0\}$. Nossa estratégia aqui será construir uma função $g \in \mathbb{C}(\wp)$ cujos zeros e pólos com as respectivas ordens sejam os mesmos de f. Consideremos então o conjunto $\mathcal{S} = \mathcal{Z} \cup \mathcal{N}$ das singularidades de f, onde $\mathcal{Z} = \{a_1, \ldots, a_n\}$ e $\mathcal{N} = \{b_1, \ldots, b_m\}$ são os conjuntos dos zeros e dos pólos de f, respectivamente.

No Lema anterior, vimos que se $z_k \in \mathcal{S}$, então z_k e z_k^* possuem ordens iguais. Dessa forma, considere $\mathcal{S}^*$ o conjunto das singularidades de f no qual existe apenas um dos elementos $\{z_0, z_0^*\}$ na situação descrita acima. Note que se $z_0 - \frac{\omega_i}{2} \in \Omega$, então $z_0^* - \frac{\omega_i}{2} \in \Omega$, $i \in \{1, 2, 3\}$.

Assim, podemos definir (sem redundâncias) para cada $z_k \in \mathcal{S}^*$,

$$r_k = \begin{cases} ord_{z_k}(f), \text{ se } 2z_k \not\equiv 0 mod(\Omega) \\ ord_{z_k}(f)/2, \text{ se } 2z_k \equiv 0 mod(\Omega) \end{cases}$$

Consideremos então a função

$$g(z) = \frac{\Pi_{i=1}^{n^*}(\wp(z) - \wp(a_i))^{r_i}}{\Pi_{j=1}^{m^*}(\wp(z) - \wp(b_j))^{r_j}} \in \mathbb{C}(\wp),$$

onde $n^* = \#\mathcal{S}^*$ e $m^* = \#\mathcal{N}^*$.

Precisamos agora provar que as ordens das singularidades de f e g coincidem. Em caso afirmativo, aplicaremos a Observação 2.1.3 à função elíptica $f/g \in M_\Omega^+$, e o resultado estará demonstrado.

Com efeito, seja $z_k \in \mathcal{S}$ e suponha primeiramente que $z_k \notin \Omega$. Como z_k é um zero de ordem 2 de $\wp(z) - \wp(z_k)$, então $-z_k$ também é zero dessa função, pois $\wp$ é par. Logo $2z_k \in \Omega$. Reciprocamente, se $2z_k \in \Omega$, então do ítem (c) do Lema 3.2.3 segue que z_k é um zero de ordem 2 de $\wp(z) - \wp(z_k)$. Assim, se tivermos $2z_k \in \Omega$, então as ordens de f e g coincidem. No caso em

que $\wp(z) - \wp(z_k)$ possuir um zero de ordem 1, como a ordem de $\wp$ é 2, temos da paridade de f que z_k^* será o outro zero. Concluímos portanto que f e g possuem as mesmas singularidades, e as ordens das tais coincidem, caso $z_k \notin \Omega$.

Suponhamos agora o caso $z_k \in \Omega$. Da mesma maneira que fizemos na Seção 2.1, considere um paralelogramo fundamental P_α tal que f e g não possuam singularidades em ∂P_α, e no interior de P_α exista apenas um elemento $\omega \in \Omega$. Se f e g possuírem uma singularidade neste ponto ω, com ordens m_f e m_g, respectivamente, então pelo Teorema 2.1.5, temos

$$0 = m_f + (\#\mathcal{Z} - \#\mathcal{N}) = m_g + (\#\mathcal{Z} - \#\mathcal{N}),$$

e pelo que vimos acima isto implica $m_f = m_g$.

Como dissemos acima, segue da Observação 2.1.3 que $f/g = u$, com $u \in \mathbb{C}^*$, portanto $f \in \mathbb{C}(\wp)$, como queríamos.

□

Capítulo 4

CURVAS ELÍPTICAS

A teoria das curvas elípticas é uma das mais belas e versáteis de toda a Matemática, possuindo aplicações em Geometria Diferencial (Superfícies Mínimas), Criptografia, Geometria Algébrica, e foi um ingrediente fundamental na demonstração do Último Teorema de Fermat dada por Andrew Wiles, em 1995.

Neste capítulo veremos como obter as curvas elípticas a partir da função $\wp$ de Weierstrass, por meio da qual será possível obter também as principais propriedades dessas curvas. Feito isso, faremos uma discussão introdutória a respeito das chamadas curvas modulares, que podem ser entendidas como espaços cujos pontos (exceto alguns em especial) representam classes de curvas elípticas isomorfas.

4.1 Curvas Elípticas e Sua Propriedade de Grupo

Antes de iniciarmos nossa abordagem das curvas elípticas daremos a definição do ambiente no qual tais curvas serão definidas. A abordagem feita aqui é baseada no capítulo 1 de [2] e no capítulo 1 de [6].

Considere o espaço $\mathbb{C}^3$ e a relação de equivalência

$$(a,b,c) \sim (a_0,b_0,c_0) \Leftrightarrow \exists t \in \mathbb{C}^*;\ a = ta_0,\ b = tb_0,\ c = tc_0.$$

Chamamos o conjunto $\mathbb{P}^2_{\mathbb{C}} = \frac{\mathbb{C}^3 - \{(0,0,0)\}}{\sim}$ de *Plano Projetivo Complexo*, ou simplesmente *Plano Projetivo*, e é neste ambiente que trabalharemos com os objetos a serem estudados nesta seção. Cada elemento de $\mathbb{P}^2_{\mathbb{C}}$ será escrito na forma $(a : b : c)$.

Em geral, dado $f \in \mathbb{C}[X,Y]\backslash\mathbb{C}$, a *curva algébrica afim* determinada por f é o conjunto dos pontos $(x,y) \in \mathbb{C} \times \mathbb{C}$ tais que $f(x,y) = 0$. Considerando o polinômio $F(X,Y,Z) =$

$Z^d f(X/Z, Y/Z) \in \mathbb{C}[X, Y, Z]$, $d = gr(f)$, a *curva algébrica projetiva* determinada por f é o conjunto dos pontos $(x : y : z) \in \mathbb{P}^2_{\mathbb{C}}$ tais que $F(x, y, z) = 0$. Vimos no ítem (b) do Teorema 3.2.1 que as funções $\wp$ e $\wp'$, definidas em relação a um mesmo reticulado $\Omega = [\omega_1, \omega_2]$, satisfazem a relação $(\wp')^2 = 4\wp^3 - g_2\wp - g_3$. Assim o conjunto

$$\mathcal{C}_\Omega = \{(x : y : z) \in \mathbb{P}^2_{\mathbb{C}};\ zy^2 = 4x^3 - g_2xz^2 - g_3z^3,\ g_2^3 - 27g_3^2 \neq 0\} \tag{1.1}$$

é uma curva algébrica projetiva determinada pelo polinômio $f(X, Y) = Y^2 - 4X^3 + g_2X + g_3 \in \mathbb{C}[X, Y]$, e é chamada de *curva elíptica*.

Segue do ítem (b) do Teorema 3.2.1 que temos uma aplicação $\Phi_\Omega = \Phi : \mathbb{T}_\Omega \longrightarrow \mathcal{C}_\Omega$ definida por

$$\Phi(z + \Omega) = \begin{cases} (\wp(z) : \wp'(z) : 1), & \text{se} \quad z \notin \Omega \\ (0 : 1 : 0), & \text{se} \quad z \in \Omega \end{cases}.$$

Ela permite definir uma estrutura de grupo abeliano na curva elíptica $\mathcal{C}_\Omega$, que descreveremos após a proposição abaixo.

Proposição 4.1.1. *A aplicação Φ é bijetiva.*

Demonstração. Primeiramente temos que Φ está bem definida, pois as funções $\wp$ e $\wp'$ são periódicas em relação à Ω.

Vamos provar que Φ é sobrejetiva. Seja $(x_0 : y_0 : z_0) \in \mathcal{C}_\Omega$. Se $z_0 = 0$ então segue da equação que $x_0 = 0$ e logo $(x_0 : y_0 : z_0) = (0 : 1 : 0) = \Phi(0 + \Omega)$.

Se $z_0 \neq 0$ então $(x_0 : y_0 : z_0) = (x_1 : y_1 : 1)$. A função $f : \mathbb{C}\backslash\Omega \longrightarrow \mathbb{C}$, $f(z) = \wp(z) - x_1$, é par, periódica em relação à Ω e possui ordem 2. Assim existe $\mu \in \mathbb{C}\backslash\Omega$ tal que $f(\pm\mu) = 0$, isto é, $\wp(\pm\mu) = x_1$. Consideremos dois casos.

1) $z_i = \omega_i/2 \in \{-\mu, \mu\}$, para algum $i \in \{1, 2, 3\}$. Segue do Teorema 3.2.1 e da equação de $\mathcal{C}_\Omega$ que $y^2 = (\wp'(z_i))^2 = 0$. Portanto $(x_1 : y_1 : 1) = (\wp(z_i) : 0 : 1) = \Phi(z_i + \Omega)$.

2) $x_1 \neq \wp(z_i)$, $\forall i \in \{1, 2, 3\}$. Segue do Teorema 3.2.1 e da equação de $\mathcal{C}_\Omega$ que $(y_1)^2 = (\wp'(\mu))^2$ e logo $y_1 = \wp'(\mu)$ ou $y_1 = -\wp'(\mu)$, já que $\wp'$ é uma função ímpar. Portanto $(x_1 : y_1 : 1) = (\wp(\mu) : \wp'(\mu) : 1) = \Phi(\mu + \Omega)$ ou $(x_1 : y_1 : 1) = (\wp(\mu) : -\wp'(\mu) : 1) = \Phi(-\mu + \Omega)$.

Vamos agora provar a injetividade de Φ. Como $0 + \Omega$ é o único ponto de $\mathbb{T}_\Omega$ levado por Φ em $(0 : 1 : 0)$, podemos nos restringir ao caso $z \notin \Omega$.

Se $(\wp(z_1) : \wp'(z_1) : 1) = (\wp(z_2) : \wp'(z_2) : 1)$, então $\wp(z_1) = \wp(z_2)$, e o resultado segue do ítem (d) do Lema 3.2.3.

□

A bijetividade da aplicação Φ pode ser usada para definir uma estrutura de grupo abeliano em $\mathcal{C}_\Omega$ a partir da estrutura já existente em $\mathbb{T}_\Omega$.

Dados $\Phi(z_1+\Omega), \Phi(z_2+\Omega) \in \mathcal{C}_\Omega$, definimos a operação $\oplus$ em $\mathcal{C}_\Omega$ pondo

$$\Phi(z_1+\Omega) \oplus \Phi(z_2+\Omega) = \Phi((z_1+z_2)+\Omega).$$

Como $\mathbb{T}_\Omega$ é um grupo abeliano, o par $(\mathcal{C}_\Omega, \oplus)$ é um grupo abeliano claramente isomorfo à $\mathbb{T}_\Omega$. Além disso o elemento neutro do grupo é $\Phi(0+\Omega) = (0:1:0)$. Esta operação pode ser descrita geometricamente.

Sejam $P = (x_P : y_P : 1)$ e $Q = (x_Q : y_Q : 1)$ pontos distintos em $\mathcal{C}_\Omega \backslash \{(0:1:0)\}$. Pela Proposição 4.1.1, existem $z_1+\Omega, z_2+\Omega \in \mathbb{T}_\Omega - \{0+\Omega\}$ tais que $(x_P : y_P : 1) = (\wp(z_1) : \wp'(z_1) : 1)$ e $(x_Q : y_Q : 1) = (\wp(z_2) : \wp'(z_2) : 1)$.

Considere a reta complexa $ax + by + z = 0$ passando por P e Q, e defina a aplicação $f : \mathbb{C}\backslash\Omega \longrightarrow \mathbb{C}$ como $f(z) = a\wp(z) + b\wp'(z) + c$.

Se $b \neq 0$ então a função f possui um pólo de ordem 3 em $0+\Omega$. Então pelo Teorema 2.1.6 deve existir $z_3 + \Omega \in \mathbb{T}_\Omega$ tal que $z_1 + z_2 + \Omega = -z_3 + \Omega$.

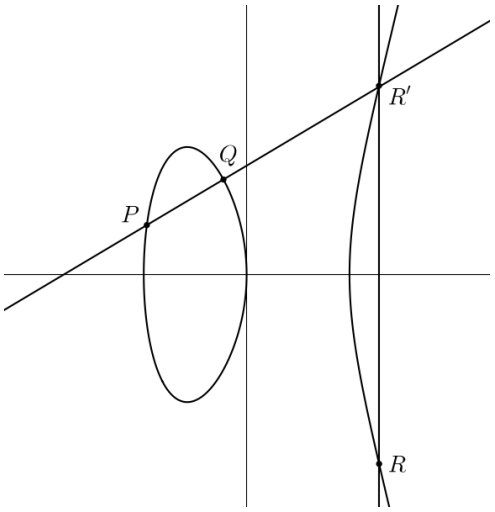

Figura 4.1: Soma $P \oplus Q = R$, no caso $b \neq 0$.

Ou seja, geometricamente, a soma de dois pontos distintos na curva $\mathcal{C}_\Omega$ é o ponto $R = (\wp(z_3) : -\wp'(z_3) : 1)$, simétrico à $R' = (\wp(z_3) : \wp'(z_3) : 1)$, este que é o terceiro ponto na reta contendo P e Q. Ou seja, $P \oplus Q = R$, e a Figura 4.1 mostra esquematicamente este caso.

Se $b = 0$ então nesse caso $a \neq 0$ e a função f possui um pólo de ordem 2 em $0+\Omega$. Também pelo Teorema 2.1.6 temos $z_1 + \Omega = -z_2 + \Omega$. Neste caso, $(\wp(z_1) : \wp'(z_1) : 1) = (\wp(z_2) : -\wp'(z_2) : 1)$, ou seja, os pontos P e Q são simétricos em relação ao eixo da primeira coordenada. Logo,

geometricamente os pontos P e Q pertencem à uma mesma reta vertical. Se $P = Q$ então $P \oplus P$ é descrita de forma análoga tomando a reta tangente à curva $\mathcal{C}_\Omega$ no ponto P.

Considerando a reta complexa passando por P e Q na forma $y = rx + s$, onde $r, s \in \mathbb{C}$, é possível demonstrar ([5], p. 115-119) que se $P \neq Q$, então

$$\begin{aligned} \wp(z_1 + z_2) &= -\wp(z_1) - \wp(z_2) + \frac{1}{4}\left(\frac{\wp'(z_1) - \wp'(z_2)}{\wp(z_1) - \wp(z_2)}\right)^2 \quad \text{e} \\ \wp'(z_1 + z_2) &= \left(\frac{\wp'(z_1) - \wp'(z_2)}{\wp(z_1) - \wp(z_2)}\right)\wp(z_1 + z_2) + s, \end{aligned}$$

e se $P = Q$,

$$\wp(z_1 + z_2) = \wp(2z_1) = -2\wp(z_1) + \frac{1}{4}\left(\frac{\wp''(z_1)}{\wp'(z_1)}\right)^2 \quad \text{e}$$

$$\wp'(z_1 + z_2) = \wp'(2z_1) = \left(\frac{\wp''(z_1)}{\wp'(z_1)}\right)\wp(2z_1) + s.$$

A propriedade de grupo obtida para $\mathcal{C}_\Omega$ não é uma exclusividade para curvas desse tipo. Como pode ser visto em ([6], p. 31-35), dada uma equação $Y^2 = f(X) = aX^3 + bX + c$, $f(X) \in K[X]$, $a \neq 0$ e K um corpo de característica diferente de 2 e 3, o conjunto

$$\mathcal{C}_{f,K} = \{(x : y : z) \in \mathbb{P}^2_K;\ zy^2 = ax^3 + bxz^2 + cz^3,\ -27a^2c^2 - 4ab^3 \neq 0\},$$

também pode ser munido de uma estrutura de grupo abeliano semelhante àquelas das curvas $\mathcal{C}_\Omega$. Definindo $f'(X) = 3aX^2 + b$, podemos definir a soma de dois pontos $P_1 = (x_1 : y_1 : 1)$ e $P_2 = (x_2 : y_2 : 1)$ em $\mathcal{C}_{f,K} \backslash \{(0 : 1 : 0)\}$ como $P_1 \oplus P_2 = P_3 = (x_3 : y_3 : 1)$, onde

$$\begin{aligned} x_3 &= -x_1 - x_2 + \frac{1}{a}\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2, \\ y_3 &= y_2 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_3 - x_2), \end{aligned}$$

se $P_1 \neq P_2$, e

$$\begin{aligned} x_3 &= -2x_1 + \frac{1}{a}\left(\frac{f'(x_1)}{2y_1}\right)^2, \\ y_3 &= y_2 + \left(\frac{f'(x_1)}{2y_1}\right)(x_3 - x_2), \end{aligned}$$

se $P_1 = P_2$.

Observação 4.1.2.

1) Dado o Corolário 3.1.2 e o isomorfismo Φ_Ω entre o toro $\mathbb{T}_\Omega$ e curva elíptica $\mathcal{C}_\Omega$ visto na Proposição 4.1.1, se φ é um isomorfismo entre os toros $\mathbb{T}_\Omega$ e $\mathbb{T}_{\Omega'}$, então a aplicação $f = \Phi_{\Omega'} \circ \varphi \circ \Phi_\Omega^{-1} : \mathcal{C}_\Omega \longrightarrow \mathcal{C}_{\Omega'}$ é um isomorfismo. Logo o diagrama abaixo é comutativo.

$$\begin{array}{ccc} \mathbb{T}_\Omega & \xrightarrow{\varphi} & \mathbb{T}_{\Omega'} \\ {\scriptstyle \Phi_\Omega^{-1}}\uparrow & & \downarrow{\scriptstyle \Phi_{\Omega'}} \\ \mathcal{C}_\Omega & \xrightarrow{f} & \mathcal{C}_{\Omega'} \end{array}$$

2) Dados dois pontos $P_1 = (x_1 : y_1 : 1)$ e $P_2 = (x_2 : y_2 : 1)$ em $\mathcal{C}_\Omega \backslash \{(0:1:0)\}$ com coordenadas racionais, segue das equações acima que $P_3 = P_1 \oplus P_2$ também possui coordenadas racionais. O grupo $\mathcal{C}_\Omega(\mathbb{Q}) = \{(x : y : z) \in \mathcal{C}_\Omega;\ x, y, z \in \mathbb{Q}\}$ é chamado de conjunto dos pontos racionais de $\mathcal{C}_\Omega$.

3) Fazendo a alteração $y \mapsto y/2$ na definição da curva elíptica $\mathcal{C}_\Omega$, obtemos uma curva

$$\mathcal{C} = \{(x : y : z) \in \mathbb{P}^2_{\mathbb{C}};\ zy^2 = x^3 - a_2xz^2 - a_3z^3,\ 4a_2^3 - 27a_3^2 \neq 0\},$$

onde $a_2 = g_2/4$ e $a_3 = g_3/4$. Como vimos acima, este conjunto pode ser munido de uma estrutura de grupo abeliano aditivo e, assim, também pode ser considerado como uma curva elíptica. No capítulo 5 utilizaremos curvas nesse padrão.

O último resultado desta Seção prova um importante fato.

Teorema 4.1.3. *Dada $\mathcal{C} = \{(x : y : z) \in \mathbb{P}^2_{\mathbb{C}};\ zy^2 = 4x^3 - a_2xz^2 - a_3z^3,\ a_2^3 - 27a_3^2 \neq 0\}$ uma curva elíptica, existe um reticulado complexo Ω tal que $\mathcal{C} = \mathcal{C}_\Omega$, isto é, $a_2 = g_2(\Omega)$ e $a_3 = g_3(\Omega)$.*

Demonstração. Como vimos na seção 2.2, a função $j : \mathcal{H} \longrightarrow \mathbb{C}$ é sobrejetiva. Daí existe $\tau_0 \in \mathcal{H}$ tal que $\frac{a_2^3}{a_2^3 - 27a_3^2} = \frac{(g_2(\tau_0))^3}{(g_2(\tau_0))^3 - 27(g_3(\tau_0))^2}$.

Supondo $a_2 \neq 0$ e $a_3 \neq 0$, segue da relação acima que

$$\frac{a_3^2}{(g_3(\tau_0))^2} = \frac{a_2^3}{(g_2(\tau_0))^3}. \tag{1.2}$$

Observe que considerando os reticulados $\Omega_{\tau_0} = [1, \tau_0]$ e $\Omega = \omega\Omega_{\tau_0}$, $\omega \in \mathbb{C}^*$, temos $g_2(\Omega) = \omega^{-4}g_2(\tau_0)$ e $g_3(\Omega) = \omega^{-6}g_3(\tau_0)$. Devemos então encontrar algum $\omega_0 \in \mathbb{C}^*$ tal que $g_j(\Omega) = a_j$, $j \in \{1, 2\}$, isto é, encontrar uma solução $\omega_0 \in \mathbb{C}^*$ para o sistema

$$\begin{cases} a(\tau_0)X^4 - 1 = 0 \\ b(\tau_0)X^6 - 1 = 0 \end{cases},$$

onde $a(\tau_0) = \frac{a_2}{g_2(\tau_0)}$ e $b(\tau_0) = \frac{a_3}{g_3(\tau_0)}$. Se ω é uma solução da primeira equação então $a(\tau_0)^3\omega^{12} = 1$. Daí pela relação 1.2 $b(\tau_0)\omega^6 = \pm 1$, e assim a solução procurada é $\omega_0 = \omega$ ou $\omega_0 = i\omega$. Dessa forma temos $a_2 = \omega_0^{-4} g_2(\tau_0)$ e $a_3 = \omega_0^{-6} g_3(\tau_0)$. Portanto o reticulado procurado é $\Omega = [\omega_1, \omega_2]$, onde $\omega_1 = \omega_0$ e $\omega_2 = \omega_0\tau_0$, e o resultado está provado.

Suponhamos agora que $a_2 = 0$. Temos então que $a_3 \neq 0$ e $g_2(\tau_0) = 0$. Consideremos Ω_{τ_0} e $\Lambda = \omega\Omega_{\tau_0}$, onde $\omega \in \mathbb{C}^*$ é tal que $\omega^{-6} g_3(\Omega_{\tau_0}) = a_3$.

Temos então que $g_2(\Lambda) = \omega^{-4} g_2(\tau_0) = 0 = a_2$ e $g_3(\Lambda) = \omega^{-6} g_3(\tau_0) = a_3$. Por fim, se $a_3 = 0$ então $a_2 \neq 0$ e usando a relação 1.2 obtemos que $g_3(\tau_0) = 0$. Então tomando $\Lambda' = \omega\Omega_{\tau_0}$, com $\omega \in \mathbb{C}^*$ tal que $\omega^{-4} g_2(\tau_0) = a_2$, segue que $g_2(\Lambda') = a_2$ e $g_3(\Lambda') = 0 = a_3$.

□

A Proposição 4.1.1 e o Teorema 4.1.3 acima nos permitem ver que reticulados equivalentes em $\mathbb{C}$, classes de toros complexos isomorfos e curvas elípticas em $\mathbb{P}^2_{\mathbb{C}}$ isomorfas são conceitos equivalentes.

4.2 Curvas Modulares e Espaços de Moduli de Curvas Elípticas

Nesta segunda e última seção vamos estudar uma estrutura que no caso do grupo $\Gamma(1)$ está naturalmente relacionada às curvas elípticas que estamos considerando. Os temas aqui apresentados são tratados de maneira mais detalhada em [4], [5] e [7].

Começamos definindo a relação de equivalência abaixo. Seja Γ um subgrupo de $\Gamma(1)$ e $\sim$ a seguinte relação de equivalência em $\mathcal{H}$:

$$\tau_1 \sim \tau_2, \tau_1, \tau_2 \in \mathcal{H} \Longleftrightarrow \exists M \in \Gamma;\ M(\tau_1) = \tau_2.$$

Para cada $\tau \in \mathcal{H}$, o conjunto $\Gamma\tau$ de todos os elementos $M(\tau)$, $M \in \Gamma$, é chamado de *órbita de τ sob a ação de* Γ, ou simplesmente *órbita de τ*. O conjunto de todas as órbitas de $\mathcal{H}$ sob a ação de Γ é denotado por $Y(\Gamma) = \Gamma\backslash\mathcal{H} = \{\Gamma\tau;\ \tau \in \mathcal{H}\}$. Para os grupos definidos no Capítulo 1, denotamos por $Y(1)$, $Y(N)$, $Y_1(N)$ e $Y_0(N)$ os conjuntos das órbitas de $\mathcal{H}$ sob a ação dos grupos $\Gamma(1)$, $\Gamma(N)$, $\Gamma_1(N)$ e $\Gamma_0(N)$, respectivamente.

Agora considere $\mathcal{F}$ um subconjunto fechado e conexo de $\mathcal{H}$. Dizemos que $\mathcal{F}$ é um *domínio fundamental de* Γ se: *(i)* dado qualquer $\tau \in \mathcal{H}$, existe $M \in \Gamma$ tal que $M(\tau) \in \mathcal{F}$, *(ii)* dados $\tau_1, \tau_2 \in int(\mathcal{F})$ distintos, tem-se $\tau_2 \neq M(\tau_1),\ \forall M \in \Gamma$, e *(iii)* se $\tau_1, \tau_2 \in \partial\mathcal{F}$, então $\tau_1 = \tau_2$

ou existe $M \in \Gamma$ tal que $\tau_2 = M(\tau_1)$. Usaremos a notação $\mathcal{F}(\Gamma)$ para representar o domínio fundamental $\mathcal{F}$ de Γ conexo.

Cabe destacar que $\mathcal{F}(\Gamma)$ não é único, pois dados um subgrupo Γ em $\Gamma(1)$ e $A \in \Gamma$, então $A\mathcal{F}(\Gamma)$ também é um domínio fundamental de Γ.

4.2.1 Domínios Fundamentais de $\Gamma(1)$ e a Curva Modular $X(1)$

Utilizando essas definições demonstraremos o próximo resultado, essencial para entendermos a natureza da relação entre reticulados complexos, toros complexos e curvas elípticas. Nesta seção consideramos o grupo especial linear $\Gamma(1)$ que, pela Proposição 1.2.1, é gerado pelas matrizes $T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ e $S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$

Teorema 4.2.1. *O conjunto* $\mathcal{F}(1) = \left\{\tau \in \mathcal{H};\ |Re(\tau)| \leq 1/2 \text{ e } |\tau| \geq 1\right\}$ *é um domínio fundamental de* $\Gamma(1)$*, e já o denotaremos* $\mathcal{F}(1)$*. Se* $\tau, \tau' \in \mathcal{F}(1)$ *são* $\Gamma(1)$*-equivalentes, então* $Re(\tau) = \pm\frac{1}{2}$*,* $\tau' = \tau \mp \frac{1}{2}$ *ou* $|\tau| = 1$*,* $\tau' = -\frac{1}{\tau}$*. Além disso, se* $\tau \in \mathcal{F}(1)$*, então* $\mathcal{I}(\tau) = \{A \in \Gamma(1);\ A(\tau) = \tau\} = \{\pm I\}$*, exceto nos casos:*

- i*,* $\mathcal{I}(i) = \langle S \rangle$*.*
- $\rho = e^{2\pi i/3}$*,* $\mathcal{I}(\rho) = \langle ST \rangle$*.*
- $-\overline{\rho} = e^{\pi i/3}$*,* $\mathcal{I}(-\overline{\rho}) = \langle TS \rangle$*.*

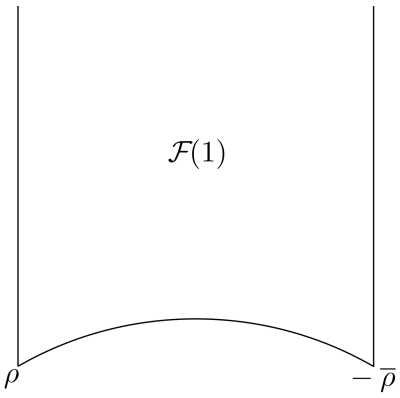

Figura 4.2: Região $\mathcal{F}(1)$.

Demonstração. Ver ([6], p. 100-103) e ([5], p. 244).

□

Como dissemos no comentário anterior ao Teorema acima, para cada $A \in \Gamma(1)$ temos que $A\mathcal{F}(1)$ é um domínio fundamental de $\Gamma(1)$. Logo, a partir das matrizes T e S, obtemos os domínios fundamentais vistos na Figura 4.3 a seguir.

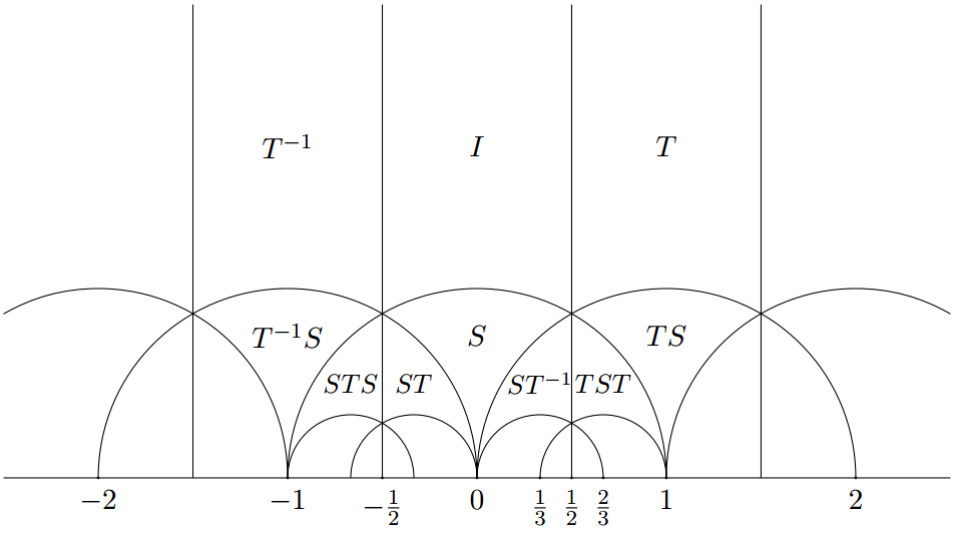

Figura 4.3: Domínios fundamentais de $\Gamma(1)$.

Uma conclusão que obtemos a partir da Proposição 4.1.1 e do Teorema 4.1.3 é que cada classe de reticulados não homotéticos em $\mathbb{C}$ (ou de toros complexos ou de curvas elípticas não isomorfas) pode ser associada bijetivamente ao conjunto $Y(1) = \Gamma(1)\backslash\mathcal{H}$ das órbitas de $\mathcal{H}$ sob a ação de $\Gamma(1)$. Podemos ver então por quê a função j definida no capítulo 2 é chamada de invariante modular. Para cada órbita $\Gamma\tau$ em $Y(1)$, temos $j(\Gamma\tau) = j(\tau)$, logo, cada classe de curvas elípticas isomorfas possui um único valor, que podemos denotar $j(\mathcal{C}_\tau)$. O conjunto $\mathcal{F}(1)$ é chamado de *espaço de parâmetros de curvas elípticas* para $\Gamma(1)$.

Considerando o grupo $\Gamma = \Gamma(1)$ e o sistema fundamental de vizinhanças V_r do ponto infinito (capítulo 2, p. 20), podemos então perguntar qual é o efeito da ação de $\Gamma(1)$ em ∞. A resposta conforme verifica-se a seguir é que a classe do infinito sob a ação de $\Gamma(1)$ é $\Gamma(1)\infty = \mathbb{Q} \cup \{\infty\}$.

De fato, seja $\frac{a}{c} \in \mathbb{Q}$, com a e c números inteiros e $mdc\{a, c\} = 1$. Então, existem $b, d \in \mathbb{Z}$ tais que $ad - bc = 1$, e considerando a matriz $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma(1)$, temos que

$$\tau \to \infty \Rightarrow A(\tau) \to \frac{a}{c};\ \text{e}\ w \to \frac{a}{c} \Rightarrow A^{-1}(w) \to \infty.$$

Para um subgrupo Γ qualquer de $\Gamma(1)$, uma Γ-órbita dos pontos de $\mathbb{Q}$ é chamada *cúspide*, *ponto cuspidal* ou *classe cuspidal* de Γ. Como todos os números racionais estão na $\Gamma(1)$-órbita

de ∞, então $\Gamma(1)$ possui apenas uma cúspide, representada por ∞. Isso não é verdade para subgrupos próprios Γ de $\Gamma(1)$, pois existem outras cúspides além de ∞, representadas por números racionais. O conjunto das órbitas dos elementos de $\overline{\mathcal{H}} = \mathcal{H}^* \cup \mathbb{Q} = \mathcal{H} \cup \{\infty\} \cup \mathbb{Q}$ é denotado por $X(\Gamma) = \Gamma\backslash\overline{H} = Y(\Gamma) \cup \Gamma\backslash(\mathbb{Q} \cup \{\infty\})$ e é chamado de *curva modular*. Tal objeto pode ser tratado como uma superfície de Riemann compacta, conexa, e também pode ser descrito por polinômios com coeficientes em $\mathbb{C}$. Isso pode ser conferido em ([2], capítulo 2) e ([6], p. 104-105).

Conforme pode ser visto em ([2], p. 62), para uma curva modular $X(\Gamma)$ é possível definir o *gênero* $g_{X(\Gamma)} = g_\Gamma$, um invariante topológico que é um número inteiro não negativo e intuitivamente corresponde ao seu número de furos ou buracos. Afirmamos que o gênero $g_{X(1)} = g_1$ de $X(1) = X(\Gamma(1))$ é zero.

De fato, como já vimos acima, a função j é invariante sob a ação de $\Gamma(1)$ e logo pode ser definida em $Y(1)$, ou seja, $j : Y(1) \longrightarrow \mathbb{C}$, $j(\Gamma\tau) = j(\tau)$. Nesse caso, pelo visto na seção 2.2 e pelo Teorema 4.2.1, j é uma bijeção. Como a série de Fourier de j na variável $q = e^{2\pi i\tau}$ é $1/q + \sum_{n=0}^{\infty} a_n q^n$ ([2], p. 73), segue que j possui um único pólo simples em ∞, e definindo $j(\Gamma\infty) = \infty$, temos que j é uma função meromorfa de $X(1)$ em $\overline{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$. Como $\overline{\mathbb{C}}$ é uma superfície homeomorfa à esfera $\mathbb{S}^2$, segue que $g_1 = 0$.

4.2.2 Domínio Fundamental de Γ e o Gênero de $X(\Gamma)$

Nessa subseção vamos resumidamente indicar como, dado um subgrupo de congruência Γ de $\Gamma(1)$, pode-se obter seu domínio fundamental, seu espaço de parâmetros, e como pode ser calculado o gênero g_Γ da curva modular $X(\Gamma)$.

Um critério para obtermos um domínio fundamental qualquer subgrupo de $\Gamma(1)$ de índice finito é dado pela Proposição abaixo.

Proposição 4.2.2. *Seja Γ um subgrupo de $\Gamma(1)$ tal que $[\Gamma(1) : \Gamma] = n < \infty$, e sejam as matrizes $A_1 = I, A_2, \ldots, A_n$ de $\Gamma(1)$ tais que $\Gamma(1) = \cup_{i=1}^{n} A_i\Gamma$. Então*

$$\mathcal{F}(\Gamma) = \bigcup_{i=1}^{n} A_i^{-1}\mathcal{F}(1)$$

é um domínio fundamental de Γ.

Demonstração. Ver ([6], p. 105).

□

De acordo com essa Proposição, para o caso $\Gamma = \Gamma(2)$, um domínio fundamental de $\mathcal{F}(2) = \mathcal{F}(\Gamma(2))$ é mostrado na Figura 4.4 a seguir ([6], p. 105-106).

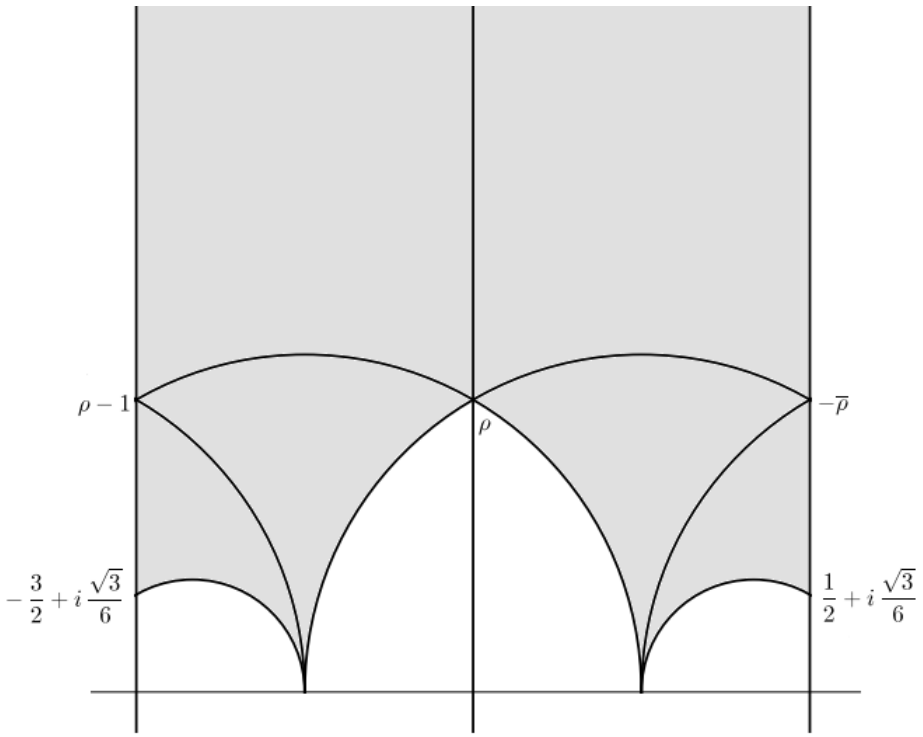

Figura 4.4: Um domínio fundamental de $\Gamma(2)$.

Para $N = 1$ foi relativamente simples obtermos o espaço de parâmetros de curvas para $\Gamma(1)$ e o gênero da curva modular $X(1)$. Para os casos $N > 2$, entretanto, tal empreendimento não é tão óbvio. A maneira de determinar o espaço de parâmetros de curvas para um subgrupo Γ de congruência de $\Gamma(1)$ pode ser vista em detalhes em ([2], seção 1.5).

Para o cálculo do gênero de curvas modulares do tipo $X(N) = \Gamma(N)\backslash\overline{\mathcal{H}}$, em ([4], p. 218-219) é discutida a fórmula

$$g_{X(N)} = 1 + [X(N) : X(1)]\left(\frac{N-6}{12N}\right),$$

na qual

$$[X(N) : X(1)] = \begin{cases} 6 & \text{se} \quad N = 2 \\ \frac{1}{2}N^3\Pi_{p|N}(1 - 1/p^2) & \text{se} \quad N > 2 \end{cases}.$$

É fácil verificar que o gênero de $X(2)$ também é zero. Uma maneira de calcular o gênero das curvas $X_0(N) = \Gamma_0(N)\backslash\overline{\mathcal{H}}$ e $X_1(N) = \Gamma_1(N)\backslash\overline{\mathcal{H}}$ pode ser vista em ([7], p. 38) e em ([2], p. 107-108 e p. 404), na qual se faz uso da projeção canônica $f : X(\Gamma) \longrightarrow X(1)$, $f(\Gamma\tau) = \Gamma(1)\tau$,

e da conhecida *fórmula de Riemann-Hurwitz*

$$2 - 2g_\Gamma \;=\; d_\Gamma(2g_1 - 2) + \sum_{x \in X(\Gamma)} (e_x - 1),$$

onde $d_\Gamma \in \mathbb{Z}^+$ é o *grau* de f e $e_x \in \mathbb{Z}^+$ é o *índice de ramificação de* $x \in X(\Gamma)$, $\Gamma = \Gamma_0(N)$ ou $\Gamma = \Gamma_1(N)$.

Encerraremos este capítulo enunciando uma versão do notável Teorema da Modularidade, que foi um resultado chave para a demonstração do Último Teorema de Fermat ([2], p. 63).

Teorema 4.2.3. *Se $\mathcal{C}$ é uma curva elíptica tal que $j(\mathcal{C}) \in \mathbb{Q}$, então existem $N \in \mathbb{Z}^+$ e uma aplicação holomorfa sobrejetiva $f : X_0(N) \longrightarrow \mathcal{C}$.*

Capítulo 5

O PROBLEMA DOS NÚMEROS CONGRUENTES

Neste capítulo consideraremos o Problema dos Números Congruentes. Trata-se de um problema que apesar de sua formulação simples, os avanços recentes na tentativa de solucioná-lo envolvem conceitos profundos da matemática. Destacaremos aqui como conceitos apresentados nos capítulos anteriores podem ser utilizados para a obtenção de avanços relacionados ao problema.

Nossa abordagem será semelhante àquela feita em [1]. Na seção 1, apresentaremos algumas formas equivalentes do problema dos números congruentes, e como ele se relaciona com as curvas elípticas. Na segunda Seção veremos, de maneira suscinta, o caminho para a demonstração do Teorema de Tunnell, o avanço mais profundo. Finalmente abordaremos como o problema está diretamente relacionado com a famosa conjectura de Birch-Swinnerton-Dyer, esse que é um dos conhecidos Problemas do Milênio.

5.1 Números Congruentes e as Curvas Elípticas

5.1.1 Algumas Caracterizações do Problema

Um número racional $n \in \mathbb{Q}$ é chamado de *número congruente* se existe um triângulo retângulo de lados $a, b, c \in \mathbb{Q}$ e área n, ou seja, $a^2 + b^2 = c^2$ e $ab = 2n$. Nessas condições (a, b, c) é uma *tripla pitagórica*. Uma tripla pitagórica é *primitiva* se for composta de números inteiros positivos primos entre si. Suporemos sempre $0 < a < b$, salvo menção em contrário.

O Problema dos Números Congruentes visa estabelecer um critério que decida se um dado

$n \in \mathbb{Q}$ é congruente ou não, e foi objeto de interesse de matemáticos gregos e árabes ([6], p. 2). Estes últimos estudaram um problema equivalente, como veremos nesta seção. Denotando por $\mathbb{Q}^+$ o grupo multiplicativo dos números racionais positivos e por $\mathbb{Q}^2$ o subgrupo de $\mathbb{Q}^+$ dos números racionais que são quadrados, a questão que os matemáticos árabes buscaram responder era: dado $n \in \mathbb{Q}$, podemos encontrar $t \in \mathbb{Q}$ tal que $t^2 - n, t^2, t^2 + n \in \mathbb{Q}^2$? Esta questão foi estudada por Fibonacci em seu livro *Liber Quadratorum* (1225), no qual chamou um tal número n de "congruente", isto é, n é congruente (do latim "congrum") se existe um $t \in \mathbb{Q}$ tal que $t^2 - n, t^2, t^2 + n$ podem ser "congregados" numa progressão aritmética de razão n em $\mathbb{Q}^2$ ([1], p. 62).

Desde então, muitos matemáticos notáveis se dedicaram a resolução de casos particulares do problema, entre os quais se destacam Fermat e Euler. Em 1640, Fermat provou que 1 não é congruente ([1], p. 60), e no séc. XVIII Euler provou que 7 é congruente ([6], p. 2). E é fácil ver que 5 é congruente considerando a tripla pitagórica $(3/2, 20/3, 41/6)$. De fato, como será visto posteriormente, 5 é o menor dos números congruentes.

Uma observação importante é que o número racional positivo n escrito na forma $n = m^2 n_0$, $m, n_0 \in \mathbb{Q}$, n_0 livre de quadrados é congruente se, e somente se, n_0 é congruente. Em particular, se $n = \frac{k}{l}$, $k, l \in \mathbb{Z}$ primos entre si, então, tomando $m = \frac{1}{l}$, concluímos que n é congruente se, e somente se, o número inteiro kl é congruente. Assim, sem perda de generalidade, podemos reduzir o problema dos números congruentes considerando apenas os números inteiros positivos livres de quadrados.

Uma construção de números congruentes é feita da seguinte maneira: dados $0 < k < l$, consideremos no plano $\mathbb{R}^2$ a reta de declividade k/l passando pelo ponto $(-1, 0)$. A intersecção dessa reta com a circunferência unitária de centro na origem $(0, 0)$ são os pontos $(-1, 0)$ e $(u, v) = \left(\frac{l^2-k^2}{l^2+k^2}, \frac{2kl}{l^2+k^2}\right)$. O ponto (u, v) gera a tripla pitagórica $a = l^2 - k^2$, $b = 2kl$ e $c = l^2 + k^2$. Dessa forma $n = kl(l^2 - k^2)$ é um número congruente. Em particular, tomando $k = 1$ e $l = 2$, concluímos que 6 é um número congruente usando a tripla pitagórica $(3, 4, 5)$. Entretanto, por exemplo, o número congruente 5 não é obtido por meio dessa construção. Mas tomando $l = 5$ e $k = 4$ temos que 180 é um número congruente tomando a tripla $(9, 40, 41)$. Como $180 = 2^2 \cdot 3^2 \cdot 5$ segue daí que 5 é um número congruente com tripla pitagórica $(3/2, 20/3, 41/6)$. Analogamente, 7 é um número congruente considerando $l = 16$ e $k = 9$ e observando que $kl(l^2 - k^2) = 3^2 \cdot 4^2 \cdot 7$.

Um primeiro critério pelo qual podemos dizer se um número n é congruente ou não é dado pela Proposição abaixo, considerando-se progressões aritméticas de três termos que são

quadrados de números racionais.

Proposição 5.1.1. *Seja $n \in \mathbb{Z}^+$ livre de quadrados e seja (a,b,c) uma tripla pitagórica tal que $ab = 2n$. Então existe uma bijeção entre os conjuntos $\mathcal{P}_n = \{q \in \mathbb{Q};\ q, q-n, q+n \in \mathbb{Q}^2\}$ e $\mathcal{T}_n = \{(a,b,c) \in \mathbb{Q}^3;\ a^2+b^2=c^2,\ ab=2n\}$.*

Em particular, n é congruente se e somente se $\mathcal{P}_n$ não é vazio.

Demonstração. Se $a^2+b^2=c^2$ e $ab=2n$, $0<a<b<c$, então temos que $(a \pm b)^2 = c^2 \pm 4n$, logo

$$\left(\frac{a \pm b}{2}\right)^2 = \left(\frac{c}{2}\right)^2 \pm n.$$

Chamando $q = \left(\frac{c}{2}\right)^2$ temos que $q, q-n, q+n \in \mathbb{Q}^2$.

Reciprocamente, dado q tal que $q, q-n, q+n \in \mathbb{Q}^2$, segue que $a = \sqrt{q+n} - \sqrt{q-n}$, $b = \sqrt{q+n} + \sqrt{q-n}$ e $c = 2\sqrt{q}$ são números racionais tais que $0<a<b<c$, $a^2+b^2=c^2$ e $ab=2n$.

□

A partir da Proposição acima obtém-se facilmente uma relação do Problema dos Números Congruentes com certas curvas elípticas. Mais precisamente, multiplicando as duas equações $\left(\frac{a\pm b}{2}\right)^2 = \left(\frac{c}{2}\right)^2 \pm n$, vistas na Proposição acima, obtemos $\left(\frac{a^2-b^2}{4}\right)^2 = \left(\frac{c}{2}\right)^4 - n^2$. Daí, para $u = c/2$ e $v = (a^2-b^2)/4$, temos

$$\begin{aligned} v^2 = u^4 - n^2 &\Rightarrow (uv)^2 = u^6 - u^2n^2 \\ &\Rightarrow y^2 = x^3 - n^2x, \end{aligned}$$

onde $x = u^2$ e $y = uv$. O discriminante do polinômio em x é $-4n^6$ e portanto não é nulo.

Assim, o conjunto $\mathcal{C}_n = \{(x:y:z) \in \mathbb{P}^2_{\mathbb{C}};\ zy^2 = x^3 - n^2xz^2\}$ é uma curva elíptica, com parte afim denotada por $\mathcal{A}_n$. Ou seja, a partir de uma tripla pitagórica podemos obter um ponto (de coordenadas racionais) na curva elíptica $\mathcal{C}_n$. A recíproca deste fato, demonstrada na Proposição a seguir, é verdadeira sob certas condições. Denotaremos $\mathcal{C}_n(\mathbb{Q}) = \{(x:y:z) \in \mathcal{C}_n;\ x,y,z \in \mathbb{Q}\}$ o conjunto dos pontos racionais da curva $\mathcal{C}_n$ e $\mathcal{A}_n(\mathbb{Q})$ sua parte afim.

Uma outra caracterização importante entre os números congruentes e a curva definida pela equação $y^2 = x^3 - n^2x$ é dada pela Proposição abaixo.

Proposição 5.1.2. *Dado inteiro livre de quadrados $n>0$, existe uma bijeção entre os conjuntos $\mathcal{T}_n$ e $\{(x,y) \in \mathcal{A}_n(\mathbb{Q});\ y \neq 0\}$, dada por $(a,b,c) \mapsto \left(\frac{nb}{c-a}, \frac{2n^2}{c-a}\right)$ e $(x,y) \mapsto \left(\frac{x^2-n^2}{y}, \frac{2nx}{y}, \frac{x^2+n^2}{y}\right)$.*

Demonstração. Sejam $(a, b, c) \in \mathcal{T}_n$ e $s = c - a > 0$. Então $b^2 - s^2 = 2as$ e, como $a = 2n/b$, temos $4nb = b^3 - bs^2$, e portanto

$$y^2 = x^3 - n^2x,$$

onde $x = \frac{bn}{s}$ e $y = \frac{2n^2}{s}$. O outro caso é provado por verificação direta. Uma conta simples prova que as aplicações são inversas uma da outra.

□

A correspondência dada acima preserva a positividade. Com efeito, se a, b e c são positivos, então $b^2 = (c - a)(c + a) > 0$, logo $c - a > 0$, e daí $x = \frac{nb}{c-a}$ e $y = \frac{2n^2}{c-a}$ são positivos. Reciprocamente, se $x, y > 0$, então $y^2 = x(x^2 - n^2) > 0$, logo $\frac{x^2-n^2}{y}, \frac{2nx}{y}, \frac{x^2+n^2}{y} > 0$. Observamos ainda que a condição $ab = 2n$ permite que tenhamos a e b ambos negativos, o que não altera a condição $a^2 + b^2 = c^2$, com $c < 0$.

Portanto com apenas uma dada tripla pitagórica (a, b, c) podemos obter, por meio de mudança de sinais na tripla, outros três pontos racionais em $\mathcal{A}_n(\mathbb{Q})$.

5.1.2 A Estrutura do Grupo $\mathcal{C}_n(\mathbb{Q})$

O estudo da estrutura do grupo $\mathcal{C}(\mathbb{Q})$ de uma curva elíptica $\mathcal{C}$ é um importante problema da teoria dos números. O teorema de Mordell abaixo assegura que esse grupo é finitamente gerado. Em sua tese Weil (1922) generalizou esse resultado para curvas elípticas sobre corpos de números e Taniyama (1954) provou o equivalente para variedades abelianas sobre corpos de números.

Teorema 5.1.3 (Mordell)**.** *O grupo $\mathcal{C}(\mathbb{Q})$ de uma curva elíptica sobre $\mathbb{Q}$ é $\mathcal{C}(\mathbb{Q})_{Tor} \oplus \mathbb{Z}^r$, onde $\mathcal{C}(\mathbb{Q})_{Tor}$ é o subgrupo dos elementos de ordem finita.*

Demonstração. Ver ([9], capítulo VIII).

□

Os elementos de ordem 2 do grupo $\mathcal{C}_n(\mathbb{Q})$ são facilmente determinados. Se $P \in \mathcal{C}_n(\mathbb{Q})\backslash\{\mathcal{O}\}$, então $P = (x_P : y_P : 1) = \ominus P = (x_P : -y_P : 1)$, onde o símbolo $\ominus$ denota o inverso de P em $(\mathcal{C}_n, \oplus)$. Então $y_P = 0$, e daí $0 = x_P^3 - n^2x_P = x_P(x_P - n)(x_P + n)$, portanto $P \in \{(\pm n : 0 : 1), (0 : 0 : 1)\}$.

O inteiro r do Teorema de Mordell é denominado o *posto* de $\mathcal{C}(\mathbb{Q})$, e o estudo do grupo $\mathbb{Z}^r$, ao contrário do grupo $\mathcal{C}(\mathbb{Q})$ que é bem conhecido, consiste de um dos principais problemas da teoria. Como veremos, o posto tem papel crucial para o problema dos números congruentes.

Teorema 5.1.4 (Mazur). *O grupo de torção $\mathcal{C}(\mathbb{Q})_{Tor}$ de uma curva elíptica sobre $\mathbb{Q}$ é isomorfo à:*

1) $\mathbb{Z}_N$, $N \in \{1, \ldots, 10\} \cup \{12\}$;

2) $\mathbb{Z}_N \times \mathbb{Z}_{2N}$, *onde* $N \in \{1, 2, 3, 4\}$.

Além disso, cada um desses casos ocorre efetivamente.

Demonstração. Ver ([9], VIII.7). □

Como $\mathcal{C}_n(\mathbb{Q})$ tem um subgrupo isomorfo à $\mathbb{Z}_2 \times \mathbb{Z}_2$, segue do Teorema de Mazur que $\mathcal{C}_n(\mathbb{Q})_{Tor} \simeq \mathbb{Z}_2 \times \mathbb{Z}_{2N}$, com $N \in \{1, 2, 3, 4\}$. O Teorema 5.1.6 abaixo afirma que apenas o caso $N = 1$ é possível.

Sejam $\mathbb{P}^2_{\mathbb{Q}}$ e $\mathbb{P}^2_{\mathbb{F}_p}$ os planos projetivos definidos sobre os corpos $\mathbb{Q}$ e $\mathbb{F}_p$, respectivamente. Dado $(x : y : z) \in \mathbb{P}^2_{\mathbb{Q}}$ qualquer, então existem x_0, y_0, z_0 em $\mathbb{Z}$ tais que $mdc\{x_0, y_0, z_0\} = 1$ e $(x : y : z) = (x_0 : y_0 : z_0)$. Noutras palavras, um ponto em $\mathbb{P}^2_{\mathbb{Q}}$, sempre pode ser representado por uma tripla de inteiros primos entre si.

Assim, podemos definir o homomorfismo $\rho_p : \mathcal{C}_n(\mathbb{Q}) \longrightarrow \mathcal{C}_n(\mathbb{F}_p)$, $\rho_p(x : y : z) = (\overline{x} : \overline{y} : \overline{z})$, denominada *redução módulo p*, onde $\overline{x}$ representa a classe do inteiro x módulo p. Denotaremos sempre a imagem de um ponto $P \in \mathcal{C}_n(\mathbb{Q})$ via ρ_p por $\overline{P} \in \mathcal{C}_n(\mathbb{F}_p)$. Como o discriminante de $\mathcal{C}_n$ é igual a $-4n^6$, temos que $\mathcal{C}_n(\mathbb{F}_p) = \{(x : y : z) \in \mathbb{P}^2_{\mathbb{F}_p};\ zy^2 = x^3 - n^2xz^2\}$ é uma curva elíptica se p não divide $2n$, e neste caso dizemos que ρ_p é uma *boa redução*.

Motivados pelo homomorfismo ρ_p, demonstraremos o resultado abaixo, que será utilizado no Teorema subsequente.

Proposição 5.1.5. *Seja p um número primo tal que $p \nmid 2n$ e $p \equiv 3 mod(4)$. Então $|\mathcal{C}_n(\mathbb{F}_p)| = p + 1$.*

Demonstração. Primeiramente, como $p \nmid 2n$, segue que $(0 : 1 : 0), (0 : 0 : 1)$ e $(\pm n : 0 : 1)$ são quatro pontos distintos em $\mathcal{C}_n(\mathbb{F}_p)$.

Afirmamos que -1 não é um quadrado em $\mathbb{F}_p^*$. De fato, a aplicação $g : \mathbb{F}_p^* \longrightarrow \mathbb{F}_p^*$, $g(x) = x^2$, é um homomorfismo do grupo multiplicativo $\mathbb{F}_p^*$. Como $p > 2$, então $-1 \not\equiv 1 mod(p)$ e logo $Ker(g) = \{\pm 1\}$ tem ordem 2. Pelo Teorema dos Homomorfismos segue que $|g(\mathbb{F}_p^*)| = \frac{p-1}{2}$. Assim, se -1 é um quadrado em $\mathbb{F}_p^*$ então $(-1)^{\frac{p-1}{2}} = 1$ e portanto $p \equiv 1 mod(4)$.

Como $p \equiv 3 mod(4)$, segue que -1 não é um quadrado em $\mathbb{F}_p$, e como o subgrupo dos quadrados de $\mathbb{F}_p^*$ possui índice 2, para cada $x \in \mathbb{F}_p - \{0, \pm n\}$ ou $f(x) = x^3 - n^2x$ ou $f(-x) =$

$-f(x)$ é um quadrado módulo p. Daí temos dois pares em $\mathcal{A}_n(\mathbb{F}_p)$, a saber, $(x, \pm\sqrt{f(x)})$ ou $(-x, \pm\sqrt{f(-x)})$.

Como o número de pares $\{x, -x\}$ é $(p-3)/2$, segue que $|\mathcal{C}_n(\mathbb{F}_p)| = p - 3 + 4 = p + 1$.

□

Por meio desta Proposição e da redução módulo p é possível demonstrar que o grupo de torção da curva elíptica $\mathcal{C}_n(\mathbb{Q})$ contém apenas os pontos $\mathcal{O}$, $(0:0:1)$ e $(\pm n:0:1)$

Teorema 5.1.6. *$\mathcal{C}_n(\mathbb{Q})_{Tor} = \{(0:1:0), (0:0:1), (\pm n:0:1)\}$ é o grupo de torção da curva elíptica $\mathcal{C}_n(\mathbb{Q})$.*

Demonstração. Já sabemos que $\{(0:1:0), (0:0:1), (\pm n:0:1)\} \subset \mathcal{C}_n(\mathbb{Q})_{Tor}$ e que não existe outro ponto de ordem 2. Suponhamos por contradição que $|\mathcal{C}_n(\mathbb{Q})_{Tor}| > 4$, e seja $Q \in \mathcal{C}_n(\mathbb{Q})_{Tor}$ um elemento de ordem $e > 2$. Então segue da segunda parte do Teorema de Mazur que $\mathcal{C}_n(\mathbb{Q})_{Tor} \simeq \mathbb{Z}_2 \times \mathbb{Z}_{2N}$, $N \in \{2, 3, 4\}$. Se e for ímpar então $\mathcal{C}_n(\mathbb{Q})_{Tor} \simeq \mathbb{Z}_2 \times \mathbb{Z}_6$ e $|\langle Q \rangle| = e = 3$. Neste caso seja $G = \langle Q \rangle$. Caso e seja par, então deve existir $P \in \mathcal{C}_n(\mathbb{Q})_{Tor}$ tal que $|\langle P \rangle| = 4$, e pelo menos um elemento R de ordem 2 não pertence ao grupo $\langle P \rangle$. Neste caso seja $G = \langle P, R \rangle$, $|G| = 8$. Para ambos os casos seja $G = \{P_1, \ldots, P_m\}$, $|G| = m \in \{3, 8\}$, com $P_i = (x_i : y_i : z_i)$, $x_i, y_i, z_i \in \mathbb{Z}$ e $mdc\{x_i, y_i, z_i\} = 1$.

Dados $i, j \in \{1, \ldots, m\}$, $i \neq j$, chamemos $P_iP_j = (y_jz_i - y_iz_j, x_jz_i - x_iz_j, x_iy_j - x_jy_i) \in \mathbb{R}^3$, e denotemos por M_{ij} o máximo divisor comum das entradas de P_iP_j.

Consideremos então um primo p tal que $p \nmid 2n$ e $p > M_{ij}$. Em particular $p \nmid M_{ij}$ e logo $\overline{P_i} \neq \overline{P_j}$ e $\rho_p|_G$ é um homomorfismo injetivo. Então o conjunto G é isomorfo a um subgrupo de $\mathcal{C}_n(\mathbb{F}_p)$, e assim m divide $|\mathcal{C}_n(\mathbb{F}_p)|$. Se $p \equiv 3 mod(4)$, segue da Proposição 5.1.5 que $m|(p+1)$. Pelo Teorema de Dirichlet para números primos em progressão aritmética essas relações são válidas para uma infinidade de primos.

Assim, considerando o número primo p da forma $p = 24k + 3$, para k inteiro suficientemente grande, juntamente com a condição $m|(p+1)$, obtemos uma contradição em ambos os casos $m \in \{3, 8\}$.

□

O próximo resultado nos dá um critério importante para averiguar se um número n é ou não congruente.

Teorema 5.1.7. *O inteiro n livre de quadrados é um número congruente se, e somente se, o posto da curva elíptica $\mathcal{C}_n(\mathbb{Q})$ é positivo.*

Demonstração. Se n é um número congruente então pela proposição 5.1.2 existe um ponto $P = (x_P : y_P : 1) \in \mathcal{C}_n(\mathbb{Q})$ com $y_P \neq 0$. Como pelo Teorema anterior os únicos elementos de ordem finita de $\mathcal{C}_n(\mathbb{Q})$ são $(0:1:0), (0:0:1)$ e $(\pm n:0:1)$, segue que P possui ordem infinita. Portanto $r \geq 1$.

Reciprocamente, suponhamos que $P = (x_P : y_P : 1) \in \mathcal{C}_n(\mathbb{Q})$ possui ordem infinita. Então pelo Teorema anterior $y_P \neq 0$, e pela Proposição 5.1.2 o conjunto $\mathcal{T}_n$ das triplas pitagóricas (a, b, c) com $ab = 2n$ não é vazio. Portanto n é um número congruente.

□

Para uma curva elíptica $\mathcal{C}(\mathbb{Q})$ os possíveis grupos de torção estão determinados pelo Teorema de Mazur e, no caso da curva $\mathcal{C}_n(\mathbb{Q})$, pelo Teorema 5.1.6. Entretanto, mesmo para a curva $\mathcal{C}_n(\mathbb{Q})$ a determinação de seu posto é um problema cuja solução não é conhecida, e está relacionada a conjectura de Birch e Swinnerton-Dyer, um dos famosos Problemas do Milênio. Falaremos mais dela dessa questão na próxima seção.

5.2 O Critério de Tunnell

Seja $n > 0$ um número inteiro livre de quadrados. A *função L de Hasse-Weil* da curva elíptica $\mathcal{C}$ é

$$L(\mathcal{C}; s) = \Pi_p \frac{1}{1 - 2a_{n,p}p^{-s} + p^{1-2s}},$$

na qual $s \in \mathbb{C}$, $Re(s) > 3/2$, p é um inteiro primo positivo e $a_{n,p} = p + 1 - |\mathcal{C}(\mathbb{F}_p)|$. Para a curva $\mathcal{C}_n$ essa função possui um prolongamento analítico em todo o plano complexo e satisfaz uma equação funcional ([6], p. 84).

Conjectura 1 (Birch e Swinnerton-Dyer)**.** *Seja $\mathcal{C}$ uma curva elíptica. Então $L(\mathcal{C}; 1) = 0$ se, e somente se, $\mathcal{C}$ possui infinitos pontos racionais.*

A chamada versão "forte" da conjectura afirma que a ordem de zero de $L(\mathcal{C}; s)$ em 1 é igual ao posto r da curva elíptica, ou seja,

$$L(\mathcal{C}; s) = a_0(s-1)^r + (\text{termos de ordem maior}),\ a_0 \neq 0,$$

se, e somente se, $r \geq 1$.

Existem boas evidências tanto para a afirmação quanto para a negação da Conjectura. Uma evidência contraria a ela é discutida em ([6], p. 91). A principal evidência favorável surgiu em

1977, quando John Coates e Andrew Wiles provaram o resultado abaixo para uma certa classe de curvas elípticas, dentre as quais se incluem as curvas do tipo $\mathcal{C}_n$ ([6], p. 92).

Teorema 5.2.1 (Coates-Wiles)**.** *Seja $\mathcal{C}$ uma curva elíptica. Se o posto de $\mathcal{C}(\mathbb{Q})$ é positivo, então $L(\mathcal{C};1)=0$.*

De maneira equivalente, pelo Teorema 5.1.7, se n (livre de quadrados) é um número congruente, então $L(\mathcal{C}_n;1)=0$. Por outro lado, se a Conjectura de Birch e Swinnerton-Dyer for verdadeira, também pelo Teorema 5.1.7 segue que n é congruente.

Usando o chamado método de Heegner, Gross e Zagier provaram que se $n \equiv 5,6,7 mod(8)$, então n é congruente se $L(\mathcal{C}_n;s)$ tem um zero simples em $s=1$ ([6], p. 93). Além disso, para $n<10^6$, Elkies prova nesse caso que n é um número congruente sem nenhuma restrição ([3]). Finalmente, Monsky em 1990 provou que, entre outros, todos esses inteiros são números congruentes ([8], p. 66).

Encerramos esse capítulo mostrando o Critério de Tunnell. Como veremos, por meio dele podemos provar que 1, 2 e 3 não são números congruentes. Uma extensa lista de números congruentes pode ser encontrada em ([10]), na qual constam os números inteiros 5, 6, 7, 13 e 14.

Teorema 5.2.2 (Tunnell, ([6], p. 217))**.** *Existem formas modulares f e g de peso $3/2$ definidas por ($q=e^{2\pi i\tau}$, $\tau\in\mathcal{H}$):*

$$\begin{aligned} f(q)=\sum_{n=1}^{\infty}a_nq^n &= \sum_{x,y,z\in\mathbb{Z}}q^{2x^2+y^2+32z^2}-\frac{1}{2}\sum_{x,y,z\in\mathbb{Z}}q^{2x^2+y^2+8z^2} \\ g(q)=\sum_{n=1}^{\infty}b_nq^n &= \sum_{x,y,z\in\mathbb{Z}}q^{4x^2+y^2+32z^2}-\frac{1}{2}\sum_{x,y,z\in\mathbb{Z}}q^{4x^2+y^2+8z^2} \end{aligned}$$

e para cada $n\in\mathbb{Z}^+$ livre de quadrados, temos

$$L(\mathcal{C}_n;1)=\begin{cases} \frac{\beta}{4\sqrt{n}}a_n^2, & se \quad n \text{ é ímpar} \\ \frac{\beta}{2\sqrt{n}}(b_{n/2})^2, & se \quad n \text{ é par} \end{cases},$$

onde $\beta=\int_1^{\infty}\frac{1}{\sqrt{x^3-x}}dx$. Em particular, $L(\mathcal{C}_n;1)=0$ se, e somente se, $a_n=0$ se é n ímpar, ou $b_{n/2}=0$ se n é par.

Teorema 5.2.3 (Critério de Tunnell)**.** *Sejam $n \in \mathbb{Z}^+$ livre de quadrados e*

$$\begin{aligned} D_n(X,Y,Z) &= 2X^2 + Y^2 + 8Z^2 - n, \\ F_n(X,Y,Z) &= D_n(X,Y,Z) + 24Z^2, \\ G_n(X,Y,Z) &= 2(4X^2 + Y^2 + 8Z^2) - n, \\ H_n(X,Y,Z) &= G_n(X,Y,Z) + 48Z^2. \end{aligned}$$

Para cada $F \in \mathbb{Z}[X,Y,Z]$ seja $N(F) = \#\{(x,y,z) \in \mathbb{Z}^3;\ F(x,y,z) = 0\}$. Se n é um número congruente então $N(D_n) = 2N(F_n)$ se n é ímpar, e $N(G_n) = 2N(H_n)$ se n é par.

Se a Conjectura de Birch-Swinnerton-Dyer é verdadeira e valem essas igualdades, então n é um número congruente.

Demonstração. Se n é um número congruente, então segue do Teorema 5.1.7 e do Teorema de Coates-Wiles que $L(\mathcal{C}_n; 1) = 0$. Assim, pelo Teorema anterior, $a_n = 0$, se n é ímpar, e $b_{n/2} = 0$, se n é par. Considerando os coeficientes dos termos de ordem n das formas f e g dadas anteriormente, concluímos daí que $0 = N(F_n) - \frac{1}{2}N(D_n)$, ou $0 = N(H_n) - \frac{1}{2}N(G_n)$.

Reciprocamente, se são válidas essas igualdades então $a_n = 0$ se n é ímpar, ou $b_{n/2} = 0$, se n é par. Pelo Teorema anterior concluímos que $L(\mathcal{C}_n; 1) = 0$. Nesse caso, se a Conjectura de Birch-Swinnerton-Dyer é assumida verdadeira então o posto de $\mathcal{C}_n(\mathbb{Q})$ é positivo, e portanto, pelo Teorema 5.1.7, n é um número congruente.

□

Considerando o Critério de Tunnell (que pressupõe verdadeira a Conjectura de Birch e Swinnerton-Dyer), o Teorema de Coates-Wiles e o Teorema 5.1.7, temos

$$\begin{aligned} n \text{ congruente} &\iff \mathcal{C}_n(\mathbb{Q}) \simeq \mathcal{C}_n(\mathbb{Q})_{Tor} \oplus \mathbb{Z}^r, r > 0 \\ &\iff L(\mathcal{C}_n; 1) = 0 \\ &\iff a_n = 0 \ (n \text{ ímpar}) \text{ ou } b_{n/2} = 0 \ (n \text{ par}). \end{aligned}$$

Exemplo 5.2.4. *Pelo Critério de Tunnell, os números* 1, 2 *e* 3 *não são congruentes. De fato, $N(D_1) = 2 = N(F_1)$, $N(G_2) = 2 = N(H_2)$ e $N(D_3) = 4 = N(F_3)$. Temos ainda $N(G_{14}) = 0 = N(H_{14})$ e $N(D_{13}) = 8$ $N(F_{13}) = 4$, portanto* 13 *e* 14 *são números congruentes pelo Critério de Tunnell.*

Existe ainda um caso mais geral do problema dos números congruentes, que pode ser assim enunciado: dado um ângulo θ, $0 < \theta \leq \pi/2$, um número inteiro positivo n é chamado de

θ-congruente se existe uma tripla racional (a, b, c) tal que

$$a^2 + b^2 - 2ab\cos(\theta) = c^2,\ ab.\text{sen}(\theta) = 2n.$$

O problema que estudamos nesse trabalho corresponde ao caso $\theta = \pi/2$.

Referências Bibliográficas

[1] CONRAD, Keith. The Congruent Number Problem. Disponível em http://www.math.uconn.edu/~kconrad/blurbs/ugradnumthy/congnumber.pdf. Acesso em 05/09/2014

[2] DIAMOND, Fred; SHURMAN, Jerry. **A First Course In Modular Forms**. New York: Springer-Verlag, 2005. (Coleção Graduate Texts In Mathematics; 228).

[3] ELKIES, Noam D. Disponível em http://www.math.harvard.edu/~elkies/compnt.html. Acesso em 26/09/2015.

[4] HUSEMÖLLER, Dale. **Elliptic Curves**. 2. ed. New York: Springer-Verlag, 2004. (Coleção Graduate Texts In Mathematics; 111).

[5] JONES, Gareth A.; SINGERMAN, David. **Complex Functions, An Algebraic And Geometric Viewpoint**. Cambridge: Cambridge University Press, 1987.

[6] KOBLITZ, Neal. **Introduction to Elliptic Curves and Modular Forms**. 2. ed. Virginia: Springer-Verlag, 1993. (Coleção Graduate Texts In Mathematics; 97).

[7] MILNE, James S. **Modular Functions and Modular Forms - Elliptic Modular Curves**. Disponível em http://www.jmilne.org/math/

[8] MONSKY, Paul. Mock Heegner Points And Congruent Numbers. In: **Mathematische Zeitschrift**. Göttingen: Springer Berlin Heidelberg, 1990. p. 45-68.

[9] SILVERMAN, Joseph H. **The Arithmetic Of Elliptic Curves**. 2. ed. New York: Springer-Verlag, 2009. (Coleção Graduate Texts In Mathematics, 106).

[10] THE ON-LINE ENCYCLOPEDIA of Integer Sequences. Disponível em http://oeis.org/A003273/list. Acesso em 18/05/2015.