Elipses não são curvas elípticas!
Nível U
Eduardo Tengan

Ao contrário da crença popular, elipses não são curvas elípticas. O propósito deste artigo é desmistificar tal crença.

1 Aritmética das Cônicas

Considere a singela equação diofantina

$$2x^2 + 3y^2 = 5z^2 \tag{1}$$

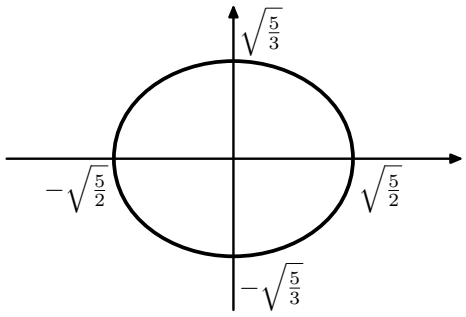
É claro que $(x, y, z) = (0, 0, 0)$ é uma solução (dita **trivial**), mas esta não é uma solução particularmente interessante (afinal, ela é a solução trivial!). Por outro lado, se (x, y, x) não é uma solução trivial, então $z \neq 0$ e dividindo (1) por $5z^2$ obtemos

$$\frac{(x/z)^2}{5/2} + \frac{(y/z)^2}{5/3} = 1$$

e assim para encontrar as soluções não triviais de (1) basta determinar as soluções **racionais** de

$$\frac{x^2}{5/2} + \frac{y^2}{5/3} = 1 \tag{2}$$

que é a equação de uma elipse com eixos $2\sqrt{5/2}$ e $2\sqrt{5/3}$:



Vejam, uma elipse!

Em outras palavras, resolver (1) é equivalente a encontrar todos os **pontos racionais** (i.e. pontos com ambas as coordenadas racionais) da elipse acima.

É fácil encontrar um destes pontos racionais, por exemplo $(x, y) = (1, 1)$. Mas como encontrar todos? A ideia é utilizar a *geometria* da figura acima, fazendo uma espécie de "projeção estereográfica" desta cônica (como é no plano, talvez o nome "projeção monográfica" fosse mais adequado...)

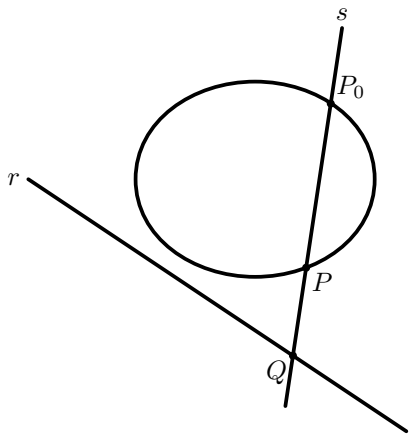
Começamos trançando uma reta r paralela à reta tangente à elipse no ponto $P_0 = (1, 1)$. Derivando (2) em relação à x, obtemos $\frac{2x}{5/2} + \frac{2yy'}{5/3} = 0$ e assim $y' = -2/3$ para $(x, y) = (1, 1)$. Portanto podemos tomar (por exemplo)

$$y = -\frac{2}{3}x - 2 \qquad \text{(reta } r\text{)}$$

Agora, para um ponto $P \neq P_0$ da elipse, seja s a reta que liga P a $P_0 = (1, 1)$; como esta reta não é paralela a r, temos que r e s determinam um ponto Q, como na figura a seguir.

Vamos mostrar que a associação $P \mapsto Q$ define uma bijeção entre os pontos racionais da elipse, excetuando o ponto P_0, e os pontos racionais da reta r.

Em primeiro lugar, se P é um ponto racional da elipse então a equação da reta s, que liga dois pontos racionais P e P_0, possui coeficientes racionais. Logo Q será um ponto racional, sendo a intersecção de duas retas r e s cujas equações têm coeficientes racionais.



Traçando retas

Reciprocamente, suponha que $Q = (a, b)$ é um ponto racional de r. Então a equação da reta s, determinada pelos pontos racionais P_0 e Q, terá coeficientes racionais:

$$y - 1 = \frac{b-1}{a-1} \cdot (x - 1) \qquad \text{reta } s$$

Como a equação da elipse também tem coeficientes racionais, a intersecção $P \neq P_0$ de s com a elipse será um ponto racional. Vejamos o porquê. Isolando y na equação de s e substituindo em (2) obtemos uma equação quadrática com coeficientes racionais

$$\frac{2}{5}x^2 + \frac{3}{5}\Big(1 + \frac{b-1}{a-1} \cdot (x-1)\Big)^2 - 1 = 0 \tag{3}$$

Sabemos que a abscissa $x = 1$ de P_0 é uma das raízes, logo a outra raiz (que é a abscissa de P) é racional também pelas relações de Girard. Como P pertence à reta s cuja equação tem coeficientes racionais, a ordenada de P também será racional, ou seja, P será um ponto racional!

Vamos encontrar uma fórmula explicita para P em função de $Q = (a, b)$. Em (3), temos que o coeficiente líder é $\frac{2}{5} + \frac{3}{5}(\frac{b-1}{a-1})^2$ e o termo independente é $-1 + \frac{3}{5}(1 - \frac{b-1}{a-1})^2$. Desta forma, como $x = 1$ é uma raiz, a outra será dada por

$$\frac{-1 + \frac{3}{5}(1 - \frac{b-1}{a-1})^2}{\frac{2}{5} + \frac{3}{5}(\frac{b-1}{a-1})^2} = \frac{10a^2 + 90a + 21}{10a^2 + 24a + 87}$$

após algumas contas, utilizando o fato que $b = -\frac{2}{3}a - 2$ (afinal, lembre-se de que $Q \in r$!). Utilizando a equação de s, temos portanto que a ordenada de P é

$$1 + \frac{b-1}{a-1} \cdot \Big(\frac{10a^2 + 90a + 21}{10a^2 + 24a + 87} - 1\Big) = \frac{10a^2 - 20a - 111}{10a^2 + 24a + 87}$$

Assim, encontramos todas as soluções racionais de (2)! Em particular, temos infinitas soluções, que são dadas por singelas expressões

$$(x, y) = \Big(\frac{10a^2 + 90a + 21}{10a^2 + 24a + 87}, \frac{10a^2 - 20a - 111}{10a^2 + 24a + 87}\Big)$$

para $a \in \mathbb{Q}$, juntamente com $(x, y) = (-1, -1)$. Ou, como o limite para $a \to \infty$ na expressão acima é justamente o ponto $(-1, -1)$ (isto é, P_0 corresponde ao "ponto no infinito" de r, intersecção de r com a reta s tangente à elipse no ponto P_0), podemos sucintamente escrever $a \in \mathbb{Q} \cup \{\infty\}$.

O procedimento acima funciona em geral para qualquer cônica, desde que ela possua pelo menos um ponto racional que possamos utilizar como "ponto de apoio". Mas como decidir se tal ponto existe? Um teorema devido a Haße e Minkowski diz que se uma equação "homogeneizada" como (1) não possui soluções inteiras além da trivial, então isto é detectável analisando-se esta equação módulo uma potência de primo p^k conveniente ou via desigualdades, e além disso basta considerar 2 e os primos que dividem os coeficientes desta equação. Mais precisamente,

Teorema 1.1 (Haße e Minkowski) *Seja uma forma quadrática*

$$Q(x_1, \ldots, x_n) = \sum_{1 \leq i \leq j \leq n} a_{ij} x_i x_j$$

com coeficientes $a_{ij} \in \mathbb{Q}$. Então a equação $Q(x_1, \ldots, x_n) = 0$ tem solução não trivial se, e somente se, ela admite solução não trivial sobre $\mathbb{R}$ e sobre $\mathbb{Q}_p$ para todo primo p. Aqui $\mathbb{Q}_p$ denota o corpo dos p-ádicos.

Assim, o problema de encontrar pontos racionais em tais cônicas é completamente resolvido!

Para maiores detalhes, eu sugiro a leitura do excelente livro "A course in Arithmetic" de um dos maiores matemáticos da atualidade, J.-P. Serre.

2 Curvas Elípticas como Curvas Projetivas Planas

Na seção anterior, vimos como a "projeção monográfica" permite estabelecer uma bijeção entre os pontos racionais de uma cônica e os pontos racionais de uma reta acrescida de um "ponto no infinito", ou seja, uma **reta projetiva**. Nesta seção, novamente será conveniente trabalharmos no mundo projetivo, então faremos um breve resumo dos conceitos que utilizaremos.

Dado um corpo k, o **espaço projetivo** $\mathbb{P}_k^n$ de dimensão n sobre k é definido como o conjunto de todas as direções no espaço afim k^{n+1} de dimensão $n+1$. Em outras palavras, um ponto em $\mathbb{P}_k^n$ pode ser representado como um vetor **não nulo** $(a_0, a_1, \ldots, a_n) \in k^{n+1}$; dois vetores $(a_0, a_1, \ldots, a_n)$ e $(b_0, b_1, \ldots, b_n)$ definem o mesmo ponto se eles são homotéticos, isto é, existe um $\lambda \in k$ não nulo tal que $a_i = \lambda b_i$ para $i = 0, 1, \ldots, n$. Representamos o ponto definido pelo vetor $(a_0, a_1, \ldots, a_n)$ através da sugestiva notação $(a_0 : a_1 : \ldots : a_n)$.

Por exemplo, temos que a reta projetiva pode ser decomposta como

$$\mathbb{P}_k^1 = \{(1 : a_1) \mid a_1 \in k\} \cup \{(0 : 1)\}$$

pois se $a_0 \neq 0$ então $(a_0 : a_1) = (1 : \frac{a_1}{a_0})$ e se $a_0 = 0$ então $(0 : a_1) = (0 : 1)$. Assim, a reta projetiva consiste de uma "reta afim", composta pelos pontos da forma $(1 : a_1)$, e mais um "ponto no infinito" $(0 : 1)$. Da mesma forma, temos que o plano projetivo

$$\mathbb{P}_k^1 = \{(1 : a_1 : a_2) \mid (a_1, a_2) \in k^2\} \cup \{(0 : a_1 : a_2) \mid a_1, a_2 \in k, \text{ não ambos nulos}\}$$

é a união de um "plano afim" (primeiro termo, já que $(1 : a_1 : a_2) = (1 : a_1' : a_2') \iff a_1 = a_1'$ e $a_2 = a_2'$) e uma reta projetiva no "infinito" (segundo termo). Note que a escolha de "reta no infinito" é completamente arbitrária, pois poderíamos tomar uma outra decomposição, por exemplo

$$\mathbb{P}_k^1 = \{(a_0 : a_1 : 1) \mid (a_0, a_1) \in k^2\} \cup \{(a_0 : a_1 : 0) \mid a_0, a_1 \in k, \text{ não ambos nulos}\}$$

e agora os pontos com $a_2 = 0$ formam a "reta no infinito".

Agora falaremos um pouco sobre curvas algébricas planas. No plano afim k^2, temos que qualquer polinômio $p(x, y) \in k[x, y]$ define uma curva

$$C = \{(a, b) \in k^2 \mid p(a, b) = 0\}$$

(que pode eventualmente degenerar em um ponto, em todo o plano, ou mesmo no conjunto vazio, mas não vamos nos preocupar com estes detalhes agora). Porém, no mundo projetivo só podemos considerar polinômios **homogêneos**, isto é, polinômios cujos monômios têm todos o mesmo grau. De fato, se $p(x_0, x_1, x_2) \in k[x_0, x_1, x_2]$ é homogêneo de grau d então temos que

$$p(a_0, a_1, a_2) = 0 \Rightarrow p(\lambda a_0, \lambda a_1, \lambda a_2) = \lambda^d p(a_0, a_1, a_2) = 0$$

Assim, faz sentido dizer quando um polinômio homogêneo $p(x_0, x_1, x_2)$ se anula em uma classe de vetores homotéticos e podemos considerar a curva projetiva definida por $p(x_0, x_1, x_2)$:

$$C = \{(a_0 : a_1 : a_2) \in \mathbb{P}_k^2 \mid p(a_0, a_1, a_2) = 0\}$$

Por exemplo temos que $x_0 = 0$ é uma equação da "reta no infinito" descrita acima. Temos que para qualquer $(a, b, c) \neq (0, 0, 0)$ a equação $ax_0 + bx_1 + cx_2 = 0$ define uma reta projetiva em $\mathbb{P}^2_k$; esta reta é a união de uma reta afim de equação $a + bx + cy = 0$ ($x_0 \neq 0$) e de um "ponto no infinito" $(0 : -c : b)$, intersecção das retas $ax_0 + bx_1 + cx_2 = 0$ e $x_0 = 0$.

Em geral, duas retas distintas

$$\begin{cases} ax_0 + bx_1 + cx_2 = 0 \\ dx_0 + ex_1 + fx_2 = 0 \end{cases}$$

possuem exatamente um ponto de intersecção, pois a solução do sistema linear homogêneo acima é 1 dimensional (não pode ser 2 dimensional, pois neste caso as retas seriam coincidentes), logo define exatamente um ponto em $\mathbb{P}^2_k$ (ou seja, uma direção em k^3).

Agora estamos prontos para dar a (primeira) definição de curva elíptica:

Definição 2.1 Seja k um corpo, de característica diferente de 2 e 3 para simplificar (isto é, $2 \neq 0$ e $3 \neq 0$ em k). Uma curva projetiva plana definida por uma equação da forma

$$y^2z = x^3 + axz^2 + bz^3, \qquad a, b \in k,$$

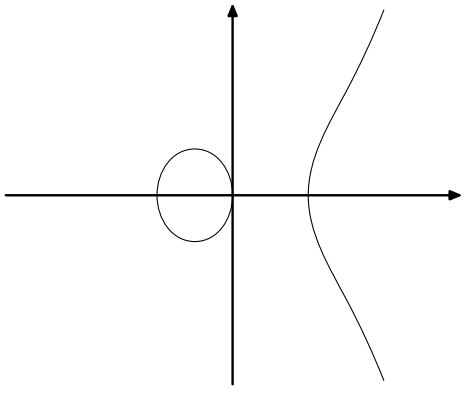
é denominada de **curva elíptica** sobre k.

Observe que a curva acima é a união da curva afim de equação ($z \neq 0$)

$$y^2 = x^3 + ax + b \qquad (*)$$

e de um único "ponto no infinito" $O = (0 : 1 : 0)$, intersecção da curva projetiva acima com a "reta no infinito" $z = 0$. Por este motivo, muitas vezes, ao fazermos as contas, trabalhamos com a equação afim $(*)$, que é mais simples, retornando ao modelo projetivo conforme necessário.

Vejamos uma curva elíptica real, por exemplo $y^2 = x^3 - x$. Note que na figura as duas pontas do ramo da direita se encontram no "ponto do infinito" $O = (0 : 1 : 0)$, que é o ponto de intersecção da "reta no infinito" com qualquer reta "vertical" $x - cz = 0$. Em outras palavras, O é o ponto de concorrência de todas as retas verticais.



Veja! Uma curva elíptica!

3 A Lei da Corda-Tangente

Vamos tentar imitar o procedimento da primeira seção para encontrar os pontos racionais de uma curva elíptica sobre $\mathbb{Q}$. A primeira dificuldade com a qual nos deparamos é que enquanto em geral uma reta intercepta uma cônica em 2 pontos, ela intercepta um curva elíptica em 3 pontos! Observe por exemplo o eixo das abscissas na figura anterior.

Por outro lado, se tivermos **dois** pontos racionais P e Q em uma curva elíptica, então podemos encontrar um novo ponto racional R, intersecção da curva elíptica com a reta r que liga P e Q. Para ver que este ponto é racional, observe que a reta que passa por P e Q tem equação

$$y - y_P = \frac{y_P - y_Q}{x_P - x_Q} \cdot (x - x_P)$$

cujos coeficientes são racionais. As abscissas dos pontos de intersecção desta reta com a curva elíptica $(*)$ são as soluções de

$$\left(y_P + \frac{y_P - y_Q}{x_P - x_Q} \cdot (x - x_P)\right)^2 = x^3 + ax + b$$

que também é uma equação com coeficientes racionais. Como duas de suas raízes x_P e x_Q são racionais, a terceira raiz x_R também será racional pelas relações de Girard. Assim obtemos

$$x_R = -x_P - x_Q + \left(\frac{y_P - y_Q}{x_P - x_Q}\right)^2 \qquad \text{e} \qquad y_R = y_P + \frac{y_P - y_Q}{x_P - x_Q} \cdot (x_R - x_P)$$

Mas o que fazer se conhecemos apenas um ponto racional? Aí tomamos $x_P = x_Q$, ou seja, tomamos a reta tangente a este ponto! Basta substituir o coeficiente angular $\frac{y_P - y_Q}{x_P - x_Q}$ por $\frac{3x_P^2 + a}{2y_P}$ nas fórmulas acima. Por exemplo, considere a curva elíptica

$$y^2 = x^3 + 17$$

Ela possui um ponto racional $P = Q = (-1, 4)$. Fazendo as contas acima encontramos o insuspeito terceiro ponto racional $R = (\frac{137}{64}, \frac{2651}{512})$. Simples, não?

Observe que qualquer curva elíptica sempre possui um ponto racional, a saber, o "ponto no infinito" $O = (0 : 1 : 0)$! Será que podemos obter novos pontos racionais a partir de O? Para responder esta questão, observe que a curva $(*)$ é tangente à "reta no infinito" $z = 0$ em O: de fato, trabalhando no plano afim $y \neq 0$ que contém O, temos que a curva elíptica tem equação

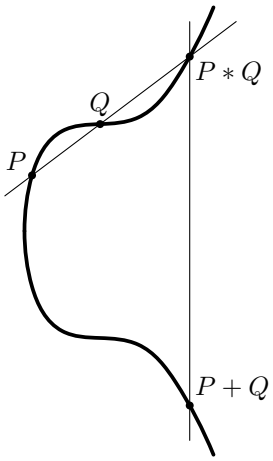
$$z = x^3 + axz^2 + bz^3$$

e assim a única intersecção com $z = 0$ é o ponto O, ou seja, O é um ponto de *inflexão* da curva. Logo aplicando o procedimento acima com $P = Q = O$ obtemos novamente o ponto O! De certa forma O age como uma espécie de "elemento neutro" para a operação acima. Podemos ser mais precisos.

Dados dois pontos racionais P e Q de uma curva elíptica, denote por $P * Q$ o ponto R que é o terceiro ponto de intersecção da curva elíptica com a reta que passa por P e Q. Definimos a soma de P e Q como sendo

$$P + Q \stackrel{\text{def}}{=} (P * Q) * O$$

Note que $(P * Q) * O$ nada mais é que o simétrico de $P * Q$ com relação ao eixo x pois a reta que passa por O e $P * Q$ é nada mais é do que a reta "vertical" que passa por $P * Q$.



A lei da corda-tangente

Esta regra, que associa a P e Q o ponto racional $P + Q$ é popularmente conhecida como **lei da corda-tangente**.

Teorema 3.1 *A lei da corda-tangente define um grupo abeliano sobre os pontos racionais de uma curva elíptica. Em outras palavras, temos*

1. *(Associatividade)* $(P+Q)+R = P+(Q+R)$ *para quaisquer três pontos racionais* P, Q *e* R;
2. *(Elemento Neutro)* $P+O = O+P = P$ *para qualquer ponto racional* P;
3. *(Inverso) para qualquer ponto racional* P, *existe um outro ponto racional* $-P$ *tal que* $P+(-P) = (-P)+P = O$;
4. *(Comutatividade)* $P+Q = Q+P$ *para quaisquer dois pontos racionais* P *e* Q.

Prova A associatividade é a propriedade mais difícil de ser verificada e sua prova será postergada até a próxima seção. A comutatividade é clara, pois $P*Q = Q*P$. Agora seja $P = (x_P, y_P)$ um ponto racional da curva. Então $P*O = (x_P, -y_P)$ é o simétrico de P com relação ao eixo x. Analogamente, temos $(x_P, -y_P)*O = (x_P, y_P) = P$, o que mostra que O é o elemento neutro deste grupo. Da mesma forma, é fácil ver que $-P = (x_P, -y_P)$, o simétrico de P com relação ao eixo x. □

Note que $P*Q = -(P+Q)$, logo $P+Q+P*Q = O$. Assim, a lei da corda tangente pode ser assim enunciada: **três pontos têm soma zero se, e somente se, eles estão alinhados**.

Temos agora algumas questões. Como decidir se a curva elíptica tem *algum* ponto racional além do ponto no infinito O? Como encontrá-lo explicitamente? Finalmente, o procedimento acima gera todos os pontos racionais da curva elíptica?

Aqui a situação não é tão simples assim. O problema de decidir a existência de pontos racionais está em aberto. Felizmente sabe-se que o procedimento acima realmente gera todos os pontos racionais a partir de um certo conjunto finito de pontos. Este é o famoso

Teorema 3.2 (Mordell-Weil) *O grupo de uma curva elíptica é finitamente gerado.*

A prova deste teorema requer algumas ferramentas de Teoria Algébrica dos Números, sobre a qual falarei em alguma outra semana olímpica, então vocês terão que esperar até lá ou ler o excelente livro do Silverman, "Arithmetic of Elliptic Curves". Há provas elementares mas elas são complicadas e então eu acho mais fácil aprender as ferramentas mais avançadas, que são úteis em outros contextos também. Infelizmente a demonstração é não construtiva e não permite achar os geradores deste grupo, mas existe um algoritmo conjectural (não muito simples de descrever) para encontrar estes geradores: a questão é saber se ele pára ou não. Até hoje, em todas as curvas elípticas testadas, ele sempre parou...

4 Curvas Elípticas como Rosquinhas

Considere o seguinte **reticulado** Λ gerado por dois números complexos ω_1 e ω_2 linearmente independentes sobre $\mathbb{R}$:

$$\Lambda = \{n_1\omega_1 + n_2\omega_2 \in \mathbb{C} \mid n_1, n_2 \in \mathbb{Z}\}$$

Identificando dois números complexos z e w se $z \equiv w \pmod{\Lambda}$, isto é, se $z - w \in \Lambda$, obtemos que todo número complexo é equivalente a exatamente um elemento do **paralelogramo fundamental**

$$P = \{r_1\omega_1 + r_2\omega_2 \in \mathbb{C} \mid r_1, r_2 \in \mathbb{R}, 0 \le r_1, r_2 < 1\}$$

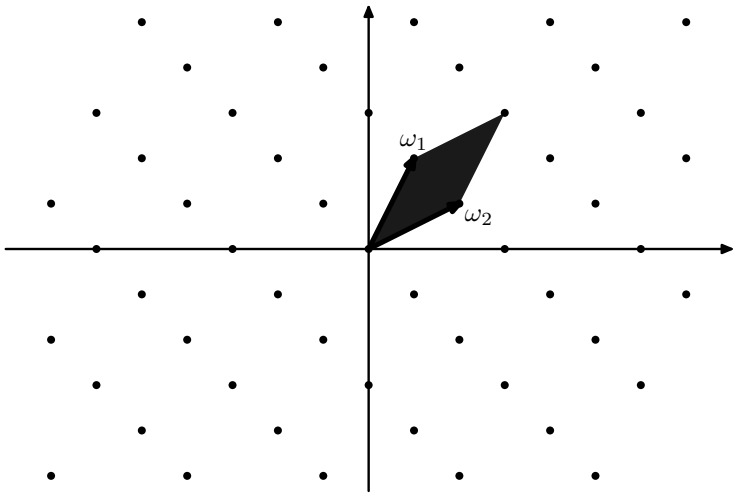
como mostra a figura a seguir.

Como os lados opostos (do fecho) deste paralelogramo estão identificados, temos um quociente $\mathbb{C}/\Lambda$ que topologicamente é uma **rosquinha** como diria Homer Simpson ou, em termos mais científicos, um **toro**. Este toro é a **curva elíptica complexa definida pelo reticulado** Λ. Esta rosquinha vem, de fábrica, equipada com uma estrutura de grupo abeliano: dados dois pontos $P, Q \in \mathbb{C}/\Lambda$ representados por números complexos $z, w \in \mathbb{C}$, a soma $P+Q \in \mathbb{C}/\Lambda$ é o ponto correspondente ao número complexo $z+w$ (em outras palavras, a estrutura de grupo abeliano é o quociente do grupo aditivo de $\mathbb{C}$ módulo o subgrupo Λ).

Mas o que rosquinhas têm a ver com a definição anterior de curva elíptica como curva projetiva plana? Para responder a esta questão, vamos estudar as funções meromórficas em $\mathbb{C}/\Lambda$, ou seja, as funções meromórficas $f\colon \mathbb{C} \to \{\infty\}$ que são invariantes por translações por elementos em Λ. Tais funções são popularmente conhecidas como **funções duplamente periódicas** pois elas possuem dois períodos:

$$f(z+\omega_1) = f(z) \qquad \text{e} \qquad f(z+\omega_2) = f(z)$$

para todo $z \in \mathbb{C}$.



O reticulado Λ e seu paralelogramo fundamental

Teorema 4.1 *Seja f uma função duplamente periódica com relação ao reticulado Λ.*

1. *Se f é holomorfa então f é constante.*
2. *Seja P o paralelogramo fundamental de Λ.*
   - *i. contando multiplicidades, o número de zeros e polos de f em P são iguais;*
   - *ii. a soma dos resíduos de f em P é 0.*
   - *iii. a soma dos zeros menos a soma dos polos em P (multiplicidades contadas) é igual a 0 módulo Λ.*

PROVA 1. Se f é holomorfa, então ela é contínua e portanto atinge um máximo no fecho de P, que é um conjunto compacto. Assim, f é limitada em todo o plano complexo. Pelo teorema de Liouville f é constante.

2. Transladando P por uma constante, podemos assumir que nenhum zero ou polo de $f(z)$ ou $f'(z)$ está no bordo ∂P de P. Assim, a diferença entre o número de zeros e polos de f em P é igual a

$$\frac{1}{2\pi i}\int_{\partial P}\frac{f'(z)}{f(z)}\,dz = 0,$$

já que $f'(z)/f(z)$ é duplamente periódica e portanto as integrais em lados opostos do paralelogramo P se cancelam. A prova dos demais itens é análoga, utilizando os integrandos $f(z)$ e $\frac{zf'(z)}{f(z)}$. □

Vamos exibir funções duplamente periódicas (não constantes) explicitamente. Pelo teorema acima, tal função deve ter pelo menos um polo, mas não pode ter apenas um polo simples pois a soma dos resíduos é 0. A próxima coisa mais simples a se tentar é um polo duplo em cada $\omega \in \Lambda$, algo como $\sum_{\omega\in\Lambda}(z-\omega)^{-2}$. Infelizmente esta soma não converge, mas uma pequena modificação resolve este problema:

Definição 4.2 Seja Λ um reticulado em $\mathbb{C}$ e $\Lambda' = \Lambda - \{0\}$. A **função $\wp$ de Weierstraß** com relação a Λ é definida como

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega\in\Lambda'}\left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right)$$

Vamos mostrar que $\wp(z)$ é realmente duplamente periódica, mas antes vamos nos livrar das questões de convergência. Para $n \geq 3$, defina

$$G_n \stackrel{\text{def}}{=} \sum_{\omega\in\Lambda'}\frac{1}{\omega^n}$$

que é absolutamente convergente (observe que $G_n = 0$ se n é ímpar). De fato, quebramos a soma em "camadas de cebola" (quadrada, é claro), onde a k-ésima camada é formada pelos pontos de Λ' sobre os lados do paralelogramo de vértices $k(\omega_1+\omega_2)$, $k(\omega_1-\omega_2)$, $k(-\omega_1+\omega_2)$ e $k(-\omega_1-\omega_2)$. Seja $d > 0$ a

distância entre a origem e o paralelogramo da primeira camada. Temos $8k$ pontos na k-ésima camada, logo

$$|G_n| \leq \sum_{k\geq 1} \frac{8k}{(kd)^n} = \frac{8}{d^n} \sum_{k\geq 1} \frac{1}{k^{n-1}} = \frac{8}{d^n} \cdot \zeta(n-1) < \infty$$

pois $n \geq 3$.

Agora suponha que $|z| \leq R$. Para $|\omega|$ suficientemente grande, temos

$$\left| \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right| = \left| \frac{z(2\omega - z)}{\omega^2 (z-\omega)^2} \right| \leq \frac{c}{|\omega|^3}$$

para alguma constante c. Pelas estimativas anteriores, a soma em $\wp(z)$ converge absolutamente no disco $|z| \leq R$, logo $\wp(z)$ é meromorfa. Ela possui polos duplos apenas em Λ. Para mostrar que $\wp(z)$ é duplamente periódica, é mais fácil trabalhar com a derivada

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

que é claramente duplamente periódica. Seja $f(z) = \wp(z+\omega_1) - \wp(z)$. Como $\wp'(z)$ é duplamente periódica, $f'(z) = 0$, logo $f(z)$ é constante. Mas $\wp(z)$ é uma função par, logo $f(-\omega_1/2) = 0$ e assim $f(z) = 0$. Analogamente $\wp(z+\omega_2) = \wp(z)$, o que completa a prova.

Teorema 4.3 *A função $\wp$ satisfaz a equação diferencial*

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

onde

$$g_2 = 60G_4 = 60 \sum_{\omega \in \Lambda'} \frac{1}{\omega^4} \qquad e \qquad g_3 = 140G_6 = 140 \sum_{\omega \in \Lambda'} \frac{1}{\omega^6}$$

Prova Vamos determinar a expansão em série de Taylor de $\wp(z)$ e $\wp'(z)$ em torno do 0. Para $|z| > |\omega|$, temos $(z-\omega)^{-1} = -\frac{1}{\omega}\sum_{n\geq 0}(z/\omega)^n$. Derivando,

$$-\frac{1}{(z-\omega)^2} = -\frac{1}{\omega} \sum_{n\geq 0} n \left(\frac{z}{\omega}\right)^{n-1} \frac{1}{\omega} \iff \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \sum_{n\geq 1} \frac{(n+1)z^n}{\omega^{n+2}}$$

Assim,

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda'} \sum_{n\geq 1} \frac{(n+1)z^n}{\omega^{n+2}} = \frac{1}{z^2} + \sum_{n\geq 1} (2n+1) G_{2n+2} \cdot z^{2n}$$

pois $G_{2n+1} = 0$. Portanto

$$\begin{aligned}
&\wp'(z)^2 - 4\wp(z)^3 + 60G_4\wp(z) + 140G_6 \\
&\quad = \Big(-\frac{2}{z^2} + \sum_{n\geq 1} 2n(2n+1)G_{2n+2}z^{2n-1}\Big)^2 - 4 \cdot \Big(\frac{1}{z^2} + \sum_{n\geq 1}(2n+1)G_{2n+2}z^{2n}\Big)^3 \\
&\qquad\quad + 60G_4 \cdot \Big(\frac{1}{z^2} + \sum_{n\geq 1}(2n+1)G_{2n+2}z^{2n}\Big) + 140G_6 \\
&\quad = \Big(\frac{4}{z^6} - \frac{24G_4}{z^2} - 80G_6 + (36G_4 - 168G_8)z^2 + \cdots\Big) \\
&\qquad\quad - 4 \cdot \Big(\frac{1}{z^6} + \frac{9G_4}{z^2} + 15G_6 + (21G_8 + 27G_4^2)z^2 + \cdots\Big) \\
&\qquad\quad + 60 \cdot \Big(\frac{1}{z^2} + 3G_4 z^2 + \cdots\Big) + 140G_6 \\
&\quad = (108G_4^2 - 252G_8)z^2 + \cdots
\end{aligned}$$

que uma função holomorfa duplamente periódica, logo é constante. Como esta função é 0 para $z = 0$, esta constante deve ser 0, o que completa a prova. □

Observe que o teorema anterior assevera que para qualquer $z \in \mathbb{C}$ o ponto $(\wp(z), \wp'(z))$ de $\mathbb{C}^2$ é um ponto da curva elíptica E de equação $y^2 = 4x^3 - g_2 \cdot x - g_3$! (o coeficiente 4 não é importante, podemos nos livrar dele fazendo $y \leftarrow 2y$ por exemplo). Podemos até incluir o "ponto no infinito" fazendo-o corresponder a $z = 0$. Assim, obtemos um mapa

$$\begin{aligned} \mathbb{C}/\Lambda &\to E \\ z &\mapsto (z^3\wp(z) : z^3\wp'(z) : z^3) \end{aligned}$$

De fato, as figuras das seções anteriores mostram um "corte" de um toro em $\mathbb{C}^2 = \mathbb{R}^4$ por um plano $\mathbb{R}^2$. Note por exemplo, que a primeira figura é um corte transversal, definido dois "círculos" (lembre-se de incluir o ponto do infinito na segunda componente conexa!).

Agora vamos mostrar que este mapa é uma bijeção e que a soma natural $\mathbb{C}/\Lambda$ corresponde à soma dada pela lei da corda-tangente em E. Em outras palavras, o mapa acima é um isomorfismo de grupos abelianos! Com esta identificação, completaremos a demonstração da associatividade da lei da corda-tangente, pois a operação em $\mathbb{C}/\Lambda$ é obviamente associativa!

Teorema 4.4 (Curvas Elípticas como Rosquinhas)

1. *O mapa acima é uma bijeção.*
2. *Sejam P_1, P_2 e P_3 três pontos da curva elíptica $y^2 = 4x^3 + g_2x - g_3$ correspondentes a três pontos $z_1, z_2, z_3 \in \mathbb{C}$. Temos que P_1, P_2 e P_3 estão alinhados se, e somente se, $z_1 + z_2 + z_3 \equiv 0 \pmod{\Lambda}$.*

Prova 1. Vamos mostrar primeiro a injetividade no caso afim, deixando para o leitor as modificações no caso projetivo. Suponha que $(\wp(z), \wp'(z)) = (\wp(w), \wp'(w))$. Considere $\wp(z) - \wp(w)$ como uma função em z. No paralelogramo fundamental, esta função tem um único polo de ordem 2, logo ela tem também exatamente 2 zeros, que são claramente $\pm w$ a menos que $w \equiv -w \pmod{\Lambda}$. Mas neste caso $\wp'(w) = 0$ (veja exercício 7), logo w é um zero duplo. Logo temos em qualquer caso que $\wp(z) = \wp(w) \Rightarrow z \equiv \pm w \pmod{\Lambda}$. Como $\wp'(z) = \wp'(w)$ por hipótese, se $z \equiv -w \pmod{\Lambda}$ então $\wp'(w) = 0$ e novamente $w \equiv -w \pmod{\Lambda}$. Assim, $z \equiv w \pmod{\Lambda}$, como queríamos demonstrar.

Agora, a sobrejetividade. Seja (a, b) um ponto de E. Então, no paralelogramo fundamental, $\wp(z) - a$ tem um polo duplo e portanto dois zeros, z_0 e $-z_0$ (se $z_0 \equiv -z_0 \pmod{\Lambda}$, então como acima z_0 é um zero duplo). Como $(\wp(z_0), \wp'(z_0))$ e $(\wp(-z_0), \wp'(-z_0))$ são ambos pontos em E com a mesma coordenada $x = a$, um deles deve ser igual a (a, b).

2. Seja $y = mx + c$ a equação de uma reta e $P_1 = (\wp(z_1), \wp'(z_1))$, $P_2 = (\wp(z_2), \wp'(z_2))$ e $P_3 = (\wp(z_3), \wp'(z_3))$ os três pontos de intersecção com a curva elíptica E. No paralelogramo fundamental, a função $\wp'(z) - m\wp(z) - c$ tem um único polo triplo na origem, assim seus três zeros somam 0 módulo Λ pelo teorema anterior. Mas estes três zeros são exatamente z_1, z_2 e z_3, o que termina a prova. □

Como último resultado, observamos que devido ao teorema seguinte, cuja demonstração pode ser encontrada no livro do Silverman, *toda* curva elíptica sobre $\mathbb{C}$ não singular (isto é, tal que o discriminante $\Delta = a^3 - 27b^2$ do polinômio cúbico $x^3 + ax + b$ é não zero, o que significa que $x^3 + ax + b$ não possui raízes múltiplas) pode ser realizada como um toro complexo para algum reticulado conveniente.

Teorema 4.5 (Uniformização) *Sejam $a, b \in \mathbb{C}$ tais que $\Delta = a^3 - 27b^2 \neq 0$. Então existe um único reticulado Λ tal que $g_2(\Lambda) = a$ e $g_3(\Lambda) = b$.*

5 Exercícios

01. Encontre todos os pontos racionais das seguintes cônicas.

(a) $x^2 + 2y^2 = 3$ (b) $x^2 - y^2 = 1$
(c) $x^2 + xy + y^2 = 2$ (d) $13x^2 - xy - y^2 = 1$
(e) $x^2 + y^2 + 2xy + x - y = 20$ (f) $3x^2 - 7y^2 = 1$

02. (OBM) Considere o ponto racional $P = (3, 8)$ na curva elíptica $y^2 = x^3 - 43x + 166$. Calcule $2001P$.

03. (Fórmula de adição) Prove:

$$\wp(z + w) = \frac{1}{4} \cdot \left(\frac{\wp'(z) - \wp'(w)}{\wp(z) - \wp(w)} \right)^2 - \wp(z) - \wp(w)$$

onde $\frac{\wp'(z) - \wp'(w)}{\wp(z) - \wp(w)}$ deve ser interpretado como $\frac{\wp''(z)}{\wp'(z)}$ para $z = w$.

04. Mostre que para uma curva elíptica sobre $\mathbb{C}$ temos $E[n] \cong \mathbb{Z}/(n) \times \mathbb{Z}/(n)$. onde $E[n]$ é o conjunto de pontos P tais que $nP = O$.

05. Mostre que uma curva elíptica possui no máximo 9 pontos de inflexão.

06. Mostre que qualquer função duplamente periódica par é uma função racional em $\wp(z)$. Conclua que qualquer função duplamente periódica é uma função racional em $\wp(z)$ e $\wp'(z)$.
Dica: Para f par, sejam $\pm a_1, \ldots, \pm a_n$ e $\pm b_1, \ldots, \pm b_n$ as listas de zeros e polos de f (multiplicidades contadas, é claro). Mostre que

$$f(z) \cdot \prod_{1 \leq i \leq n} \frac{\wp(z) - \wp(b_i)}{\wp(z) - \wp(a_i)}$$

é homolorfa e portanto constante.

07. Mostre que os zeros de $\wp'(z)$ em P são os pontos de ordem 2 em E, ou seja, $\frac{\omega_1}{2}$, $\frac{\omega_2}{2}$ e $\frac{\omega_1+\omega_2}{2}$. Conclua que

$$\begin{aligned}\wp'(z)^2 &= 4\wp(z)^3 - g_2\wp(z) - g_3 \\ &= 4\big(\wp(z) - \wp\big(\frac{\omega_1}{2}\big)\big)\big(\wp(z) - \wp\big(\frac{\omega_1}{2}\big)\big)\big(\wp(z) - \wp\big(\frac{\omega_1+\omega_2}{2}\big)\big)\end{aligned}$$

08. Dada uma curva elíptica definida sobre $\mathbb{Q}$, mostre que as coordenadas dos pontos complexos de ordem n são números algébricos.
Dica: utilize o fato de que um número em $\mathbb{C}$ é algébrico se, e somente se, sua órbita por qualquer automorfismo de $\mathbb{C}$ é finita.

6 Bibliografia

Algumas sugestões de livros para quem quer aprender mais:

1. Apostol, Tom M.; "Modular functions and Dirichlet series in number theory", Springer-Verlag.
2. Diamond, Fred and Shurman, Jerry; "A first course in Modular Forms", Springer-Verlag.
3. Husemöller, Dale; "Elliptic Curves", Springer-Verlag.
4. Serre, Jean Pierre; "A Course in Arithmetic", Springer-Verlag.
5. Silverman, Joseph H; "The arithmetic of elliptic curves", Springer-Verlag.