

O NÚMERO DE PONTOS INTEIROS NUMA CIRCUNFERÊNCIA

CARLOS FLORENTINO

” When I was a student, abelian functions were, as an effect of the Jacobian tradition, considered the uncontested summit of mathematics, and each of us was ambitious to make progress in this field. And now? The younger generation hardly knows abelian functions.”

Felix Klein, *Development of Mathematics in the 19th Century*, 1928.

1. PRELÚDIO

As funções geralmente designadas por funções abelianas,¹ constituem a generalização mais natural e mais abrangente das funções trigonométricas, que todos conhecemos e usamos frequentemente. Historicamente, estas funções apareceram associadas ao estudo de primitivas da forma

$$(1) \quad \int \frac{dx}{\sqrt{p(x)}}$$

onde $p(x)$ é um polinómio de grau maior que 2 (estes integrais são chamados hiperelípticos). Se o grau de $p(x)$ fosse 2 e assumindo, para simplificar, que estamos a lidar com funções de variável complexa, concluiríamos facilmente que (no caso geral) esta primitiva é uma função composta da função $\arcsin(t)$. Poderíamos dizer, um tanto ou quanto vagamente, que a função inversa de um integral hiperelíptico é uma função abeliana (há no entanto, outros exemplos de funções abelianas).

Mas a analogia não termina aqui, e tem múltiplas facetas em várias áreas da matemática e aplicações. Por exemplo, se alguém nos perguntasse qual a utilidade das funções trigonométricas para a geometria, uma das possíveis respostas é a seguinte: elas servem para parametrizar uma circunferência (e claro, outras cónicas). Concretamente, se a nossa circunferência for $x^2 + y^2 = 1$, todos sabemos que ela é a imagem da aplicação

$$\begin{aligned} \phi: \mathbb{R}/\mathbb{Z} &\rightarrow \mathbb{R}^2 \\ t &\mapsto (\cos 2\pi t, \sin 2\pi t). \end{aligned}$$

Aqui, escrevemos o domínio como \mathbb{R}/\mathbb{Z} , uma vez que é claro que a função ϕ não depende da parte inteira do parâmetro real t , tomando valores idênticos em t e em $t+n$, para todo inteiro n . De forma análoga, as funções abelianas resolvem o mesmo

¹Em homenagem a N. H. Abel, matemático norueguês, 1820-1847.

tipo de problema geométrico, parametrizando neste caso as chamadas variedades abelianas, que são certas deformações da variedade e grupo abeliano $\mathbb{C}^n/\mathbb{Z}^{2n}$.

Num outro contexto, o das equações diferenciais, em particular quando procuramos soluções explícitas para equações que surgem em modelos concretos de física ou engenharia, as funções abelianas são muitas vezes utilizadas, sendo de realçar o seu uso nos chamados *sistemas integráveis*.

Tomando como exemplo o pêndulo simples, sobejamente tratado em vários livros, vemos que a evolução da coordenada angular do pêndulo $\theta(t)$ é descrita pela equação

$$\frac{d^2\theta}{dt^2} = -\frac{g}{L} \sin \theta,$$

sendo L o comprimento do pêndulo e g a constante gravítica (ver por exemplo [A]). Esta equação pode escrever-se na forma $\frac{dI}{dt} = 0$, sendo

$$I = \frac{L}{2g} \left(\frac{d\theta}{dt} \right)^2 - \cos(\theta)$$

uma constante do movimento. Fazendo a substituição $x = \sin(\frac{\theta}{2})$, a equação acima escreve-se como $\frac{dx}{dt} = \pm \sqrt{p(x)}$, onde $p(x) = \frac{g}{2L}(I + 1 - 2x^2)(1 - x^2)$ é um polinómio de grau 4, e portanto,

$$t = \int_0^{\sin(\frac{\theta}{2})} \frac{dx}{\sqrt{p(x)}},$$

de onde se conclui que $\sin(\frac{\theta}{2})$ é uma função abeliana, dado ser a função inversa de um integral hiperelíptico como em (1).

Também na teoria de números as funções abelianas têm jogado um papel de relevo, em particular nos chamados problemas Diofantinos, como aquele que iremos abordar neste artigo.

Mas afinal, como se definem as funções abelianas e quais as suas propriedades? Não pretendemos responder aqui com generalidade a esta questão, sendo o nosso objectivo ilustrar apenas uma interessante aplicação de quatro destas funções, as chamadas funções theta de Jacobi², na resolução de um problema aritmético/geométrico de enunciado elementar, e que se prende com a contagem do número de pontos inteiros numa circunferência.

Como seria de esperar, a literatura sobre funções abelianas é enorme. O leitor interessado pode consultar as várias obras clássicas dedicadas ao assunto que estão referidas no também clássico livro de Whittaker e Watson [WW]. Para abordagens mais recentes, veja-se por exemplo [L], e para tratamentos com ênfase nos aspectos geométricos, podem ser consultados os livros [M],[MM], entre outros.

²Carl G. J. Jacobi, matemático alemão, 1804-1851

2. APRESENTAÇÃO DO PROBLEMA

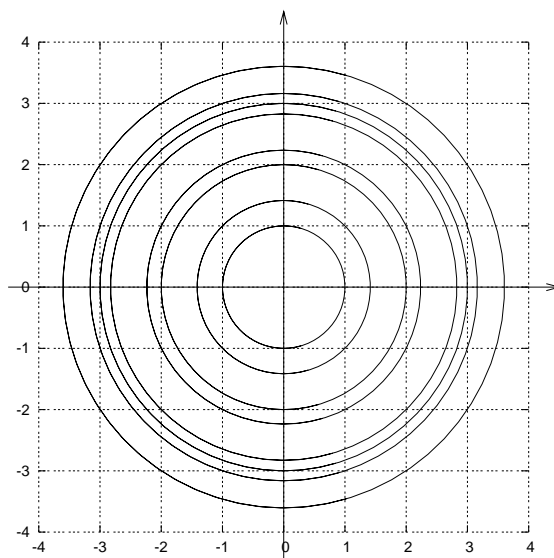
Para começar, consideremos o plano \mathbb{R}^2 e a circunferência de raio $r > 0$ centrada na origem

$$C(r) := \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = r^2\}.$$

Uma questão natural é saber se existe algum ponto desta circunferência cujas coordenadas x e y sejam números inteiros. Vamos chamar a um tal ponto, um ponto inteiro de $C(r)$.

Bastam alguns exemplos para nos convenceremos de que existem circunferências contendo pontos inteiros e outras circunferências onde não existe nenhum ponto inteiro. Por exemplo, sendo $r = \frac{1}{2}$, $C(\frac{1}{2})$ não contém nenhum ponto inteiro, mas $C(\sqrt{2})$ contém os quatro pontos $(\pm 1, \pm 1)$. De facto, se $C(r)$ contem algum ponto inteiro (x, y) , então $x^2 + y^2 = r^2 \in \mathbb{Z}$, logo r deve ser necessariamente a raiz quadrada de um inteiro positivo. Mas esta simples condição não é suficiente, dado que, por exemplo, $C(\sqrt{2})$ tem pontos inteiros como vimos, mas $C(\sqrt{3})$ não tem, facto que se verifica facilmente.

Alem da questão da existência podemos-nos perguntar também, para um dado $r > 0$, quantos pontos inteiros tem $C(r)$. A simetria do problema diz-nos que este número deverá ser um múltiplo de 4. Exceptuando estas simples observações, não parece ser fácil avançar na resolução do problema. A figura abaixo mostra as circunferências de raios $r \leq \sqrt{13}$ que têm pontos inteiros.



Entretanto, é útil notar um outro ponto de vista na abordagem desta questão. Seja N um número inteiro positivo e façamos $r = \sqrt{N}$. O nosso problema geométrico é então equivalente ao seguinte problema de teoria dos números. De quantas maneiras diferentes (se existe alguma) se pode escrever N como a soma de dois quadrados

perfeitos? Isto é, quantas são as soluções inteiras da equação algébrica

$$(2) \quad x^2 + y^2 = N, \quad \text{com } x, y \in \mathbb{Z} \quad ?$$

Descrita desta forma, a nossa questão insere-se na categoria dos chamados problemas Diofantinos³, em que é dada uma equação polinomial em várias variáveis, e se pretende encontrar as suas soluções inteiras. O mais famoso destes problemas é, sem dúvida, o último teorema de Fermat que foi demonstrado recentemente por A. Wiles e R. Taylor [WT] e que esteve em aberto durante mais de 350 anos⁴. Este teorema afirma não haver soluções inteiras da equação algébrica:

$$x^n + y^n = z^n, \quad \text{com } x, y, z, n \in \mathbb{Z}, \quad n \geq 3,$$

à excepção das soluções triviais com $xyz = 0$.

A nossa equação Diofantina, sendo claramente mais simples que a de Fermat, pois é do segundo grau, foi também objecto de estudo de alguns matemáticos célebres. Pitágoras⁵ abordou o caso em que N é um quadrado perfeito, isto é, o caso em que o raio da circunferência é inteiro, $r \in \mathbb{Z}$. Por essa razão, os ternos $(x, y, r) \in \mathbb{Z}^3$, tais que $x^2 + y^2 = r^2$ são chamados triplos pitagóricos. Note-se que este é o caso da equação de Fermat com $n = 2$. Além dos triplos pitagóricos triviais da forma $(\pm r, 0, r)$ ou $(0, \pm r, r)$ com $r \in \mathbb{N}$, temos uma infinidade de triplos pitagóricos não triviais, por exemplo $(3, 4, 5)$ e $(5, 12, 13)$. Mais concretamente, é bem sabido que dados dois inteiros não negativos m, n , o triplo

$$(m^2 - n^2, 2mn, m^2 + n^2)$$

é um triplo pitagórico, e que todo o triplo pitagórico é desta forma, à parte casos trivialmente obtidos a partir destes.

O próprio Fermat estudou a equação (2), usando métodos de teoria de números, tendo sido o primeiro a dar um critério necessário e suficiente para a existência de soluções, e que pode ser enunciado da seguinte forma. Seja $N = p_1^{n_1} \dots p_k^{n_k}$ a decomposição de N em números primos. Então N é a soma de dois quadrados (de inteiros) se e só se, para todo o primo p_j na decomposição acima, congruente com 3 módulo 4, n_j é par. Em particular, concluímos que, se N é um primo ímpar, a equação Diofantina (2) tem soluções inteiras se e só se N for congruente com 1 módulo 4.

³Em homenagem a Diofanto de Alexandria (aprox. 200-284 da nossa era).

⁴Pierre de Fermat (1601-1665) escreveu a sua famosa conjectura na margem de uma tradução de um livro de Diofanto por volta de 1630.

⁵Pitágoras de Samos (aprox. 569-475 AC).

Finalmente, em 1829, a questão do número de soluções da equação (2) foi completamente resolvida para qualquer inteiro positivo N de forma espectacular por Jacobi usando a teoria das funções abelianas, em particular as funções theta, que ele próprio definiu e estudou [J]. O nosso objectivo agora será o de enunciar e demonstrar a solução obtida por Jacobi.

3. ENUNCIADO DO RESULTADO PRINCIPAL

Começemos pelo enunciado, que é verdadeiramente elementar. Sendo $k \in \{0, 1, 2, 3\}$, denotemos por $d_k(N)$ o número de divisores de N (em que se incluem 1 e o próprio N) que são congruentes com k módulo 4. Temos então o seguinte enunciado.

Theorem 1. (Jacobi, [J]) *Dado um inteiro positivo N , o número de soluções inteiras, $\rho(N)$, da equação (2), ou o número de pontos inteiros na circunferência de raio \sqrt{N} centrada na origem, é igual a*

$$\rho(N) = 4[d_1(N) - d_3(N)].$$

Convém de imediato assegurar que, de acordo com esta fórmula, $\rho(N)$ é um número não negativo. Com efeito, não é difícil verificar, o que é deixado ao cuidado do leitor, que se tem sempre $d_1(N) \geq d_3(N)$ para qualquer $N \in \mathbb{N}$. Note-se também que, como o produto de dois números congruentes com 3 módulo 4 é congruente com 1 módulo 4, este resultado implica o critério de existência de Fermat enunciado acima.

Vejamus uma consequência interessante desta fórmula. Como sabemos, a área de um círculo de raio r é πr^2 . Por outro lado, para N um inteiro suficientemente grande, o número de pontos inteiros no interior da circunferência $C(\sqrt{N})$ de raio \sqrt{N} , é aproximadamente igual à área do círculo correspondente,

$$\sum_{n=1}^N \rho(n) \sim \pi N.$$

Assim se prova a seguinte igualdade

$$\frac{\pi}{4} = \frac{1}{4} \lim_{N \rightarrow \infty} \frac{\sum_{n=1}^N \rho(n)}{N} = \lim_{N \rightarrow \infty} \frac{\sum_{n=1}^N (d_1(n) - d_3(n))}{N},$$

que nos dá uma fórmula curiosa para o cálculo aproximado de π .

Passemos então à demonstração do teorema. A demonstração de Jacobi baseia-se num engenhoso e criativo uso de algumas técnicas da teoria das funções analíticas no plano complexo. Assim, assumiremos de agora em diante alguns conceitos desta teoria, que fazem usualmente parte do programa de um curso básico em análise

complexa, como o de função meromorfa, ordem de pólos e zeros, e o de resíduo num pólo.

É importante referir que existem na literatura várias demonstrações mais “elementares” deste resultado, no sentido em que não usam funções abelianas, ou outro tipo de “análise”, usando apenas a manipulação algébrica de séries e produtos [H]. No entanto, os argumentos da demonstração original que aqui seguiremos são, na minha opinião, interessantes precisamente por usarem as funções theta de Jacobi, que deram origem a muita investigação em matemática, ainda hoje activa, servindo este teorema como modesto exemplo das suas inúmeras aplicações.

4. AS QUATRO FUNÇÕES THETA DE JACOBI

Começemos por introduzir as quatro funções theta de Jacobi, que são funções de duas variáveis complexas $(z, \tau) \in \mathbb{C} \times \mathbb{H}$, onde \mathbb{H} designa o semiplano superior $\mathbb{H} \equiv \{w \in \mathbb{C} : \text{Im } w > 0\}$

$$\begin{aligned}\vartheta_1(z, \tau) &= i \sum_{k \in \mathbb{Z}} (-1)^k p^{2k-1} q^{(k-1/2)^2} \\ \vartheta_2(z, \tau) &= \sum_{k \in \mathbb{Z}} p^{2k-1} q^{(k-1/2)^2} \\ \vartheta_3(z, \tau) &= \sum_{k \in \mathbb{Z}} p^{2k} q^{k^2} \\ \vartheta_4(z, \tau) &= \sum_{k \in \mathbb{Z}} (-1)^k p^{2k} q^{k^2}.\end{aligned}$$

Nestas séries, fizemos as seguintes abreviaturas:

$$p = e^{\pi iz}, \quad q = e^{\pi i \tau}.$$

Estas funções são holomorfas em $z \in \mathbb{C}$ e em $\tau \in \mathbb{H}$, pois as séries que as definem são uniformemente convergentes em subconjuntos compactos do seu domínio, uma vez que a condição $\text{Im } \tau > 0$ equivale a $|q| < 1$, o que basta para assegurar a convergência. Estas quatro funções possuem muitas propriedades interessantes, das quais salientamos as seguintes que serão utilizadas na demonstração. Para simplificar a notação, escreveremos $\vartheta_k(z) \equiv \vartheta_k(z, \tau)$ esperando que tal não cause confusão.

Proposition 1. *As quatro funções theta verificam as seguintes propriedades:*

- (1) $\vartheta_3(0) = \vartheta_4\left(\frac{1}{2}\right)$; $\vartheta_2(0) = \vartheta_1\left(\frac{1}{2}\right)$;
- (2) $\vartheta_j(z) = \vartheta_j(z+2)$, $\forall j = 1, 2, 3, 4$, $\forall z \in \mathbb{C}$;
- (3) ϑ_1 é ímpar e tem um zero de ordem 1 na origem, e as outras são pares;
- (4) $\vartheta_1(z+n+m\tau) = (-1)^{m+n} p^{-2m} q^{-m^2} \vartheta_1(z)$, $\forall n, m \in \mathbb{Z}$;
- (5) $\vartheta_4(z+n+m\tau) = (-1)^m p^{-2m} q^{-m^2} \vartheta_4(z)$, $\forall n, m \in \mathbb{Z}$.

Todas estas propriedades são de verificação elementar pelo que demonstraremos simplesmente a última, como ilustração do método usado. Notando que a substituição de z por $z + n + m\tau$, equivale à substituição de p por $(-1)^n pq^m$ (mantendo q), vemos que

$$\begin{aligned} \vartheta_4(z + n + m\tau) &= \sum_{k \in \mathbb{Z}} (-1)^k (-1)^{2kn} p^{2k} q^{2km} q^{k^2} \\ &= \sum_{k \in \mathbb{Z}} (-1)^k p^{2k} q^{2km+k^2} \\ &= \sum_{k \in \mathbb{Z}} (-1)^{k-m} p^{2k-2m} q^{2km-2m+k^2-2km+m^2} \\ &= (-1)^{-m} p^{-2m} q^{-m^2} \sum_{k \in \mathbb{Z}} (-1)^k p^{2k} q^{k^2} = (-1)^m p^{-2m} q^{-m^2} \vartheta_4(z). \end{aligned}$$

Iremos usar também a seguinte importante propriedade destas funções theta.

Proposition 2. *As quatro funções theta verificam a seguinte “equação do calor”*

$$4\pi i \frac{\partial u}{\partial \tau} = \frac{\partial^2 u}{\partial z^2}.$$

Esta proposição é de verificação elementar, podendo-se calcular directamente as derivadas das funções theta, depois de escritas em termos de z e τ , ou usando as relações $\frac{\partial}{\partial \tau} = \pi i q \frac{\partial}{\partial q}$ e $\frac{\partial}{\partial z} = \pi i p \frac{\partial}{\partial p}$. A sua demonstração pode assim ser recomendada ao leitor.

5. RELAÇÃO COM OS PONTOS INTEIROS EM $C(\sqrt{N})$

Certamente o leitor estará a questionar-se sobre o interesse destas funções para a determinação do número de pontos inteiros numa circunferência. A relação é ao mesmo tempo surpreendente e elegante. Notando que com $z = 0$, vem $p = 1$, escrevamos $\vartheta_3(0)^2$ em função de q :

$$(3) \quad \vartheta_3(0)^2 = \left(\sum_{k \in \mathbb{Z}} q^{k^2} \right)^2 = \sum_{k_1 \in \mathbb{Z}} \sum_{k_2 \in \mathbb{Z}} q^{k_1^2+k_2^2} = 1 + \sum_{N \geq 1} \rho(N) q^N.$$

Vemos assim que $\vartheta_3(0)^2$ é a *função geradora* de todos os números $\rho(N)$, no sentido em que, para $N \geq 1$,

$$\rho(N) \text{ é o coeficiente de } q^N \text{ da série de potências que representa } \vartheta_3(0)^2 !!$$

Sendo assim, podemos dizer que a consideração de $\vartheta_3(0)$ (como função de q ou τ) equivale à consideração de todos os números $\rho(N)$, simultaneamente. Para obtermos a formula pretendida para $\rho(N)$, vamos então calcular $\vartheta_3(0)^2$ de outra forma, a qual torna claro, nesta abordagem, a necessidade de se utilizar simultaneamente as quatro funções theta.

Proposition 3. *As quatro funções theta no ponto $z = 0$ (vistas como funções de q) estão relacionadas pela equação*

$$\vartheta_1'(0) = \pi \vartheta_2(0) \vartheta_3(0) \vartheta_4(0).$$

Aqui e doravante, a notação f' significa a derivada parcial de f em relação a z .

6. CONCLUSÃO DO ARGUMENTO

Assumindo, por agora, a proposição 3, e usando a propriedade (i) da proposição 1, temos, no ponto $z = 0$,

$$(4) \quad \vartheta_3(0)^2 = \frac{1}{\pi} \frac{\vartheta_1'(0) \vartheta_3(0)}{\vartheta_2(0) \vartheta_4(0)} = \frac{1}{\pi} \frac{\vartheta_1'(0) \vartheta_4\left(\frac{1}{2}\right)}{\vartheta_4(0) \vartheta_1\left(\frac{1}{2}\right)} = \frac{1}{\pi} F\left(\frac{1}{2}\right).$$

onde $F(z)$ designa a seguinte função

$$F(z) = \frac{\vartheta_1'(0) \vartheta_4(z)}{\vartheta_4(0) \vartheta_1(z)}.$$

Facilmente se verifica ser $F(z)$ uma função meromorfa cujos pólos são todos simples e estão localizados nos pontos $z = n + m\tau$, $n, m \in \mathbb{Z}$ (estes são os zeros simples de $\vartheta_1(z)$ de acordo com a proposição 1(iii e iv)). Note-se que F é uma função elíptica⁶ pois $F(z) = F(z + 2) = F(z + \tau)$, o que é um simples exercício usando a proposição 1. Para continuar a análise desta função calculemos os seus resíduos nos pontos $z = n + m\tau$. Nestes pontos, ϑ_1 tem um zero simples e ϑ_4 não se anula, logo o resíduo de $F(z)$ pode ser calculado de acordo com a fórmula usual, usando uma vez mais a proposição 1

$$(5) \quad \text{Res}_{z=n+m\tau} F = \frac{\vartheta_1'(0) \vartheta_4(n + m\tau)}{\vartheta_4(0) \vartheta_1'(n + m\tau)} = \frac{\vartheta_1'(0)}{\vartheta_4(0)} \frac{(-1)^m p^{-2m} q^{-m^2} \vartheta_4(0)}{(-1)^{m+n} p^{-2m} q^{-m^2} \vartheta_1(0)} = (-1)^n.$$

Podemos agora demonstrar o seguinte resultado, que representa a decomposição de $F(z)$ numa série do tipo geralmente designado por séries de Lambert; este tipo de decomposição pode ser visto como o análogo, para funções elípticas, da decomposição de uma função racional em fracções simples.

Proposition 4. *A função $F(z)$ tem a seguinte representação*

$$(6) \quad F(z) = \pi i \sum_{m \in \mathbb{Z}} \left(\frac{1}{1 + q^m p} - \frac{1}{1 - q^m p} \right)$$

Demonstração. Deixando a questão da convergência da série para o leitor (usar uma vez mais o facto de que $|q| < 1$), vemos que ela representa uma função meromorfa

⁶Uma função diz-se elíptica se for meromorfa em \mathbb{C} e admitir dois períodos linearmente independentes sobre \mathbb{R} .

que tem apenas pólos simples nos pontos onde

$$q^m p = \pm 1 \iff e^{\pi i m \tau + \pi i z} = \pm 1 \iff z = n - m\tau, \quad n, m \in \mathbb{Z}.$$

É fácil ver que a série representa uma função elíptica com períodos 2 e τ , e também podemos verificar que os resíduos da série coincidem com os da função F . De facto,

$$\text{Res}_{z=n-m\tau} \left(\frac{\pi i}{1 \pm q^m p} \right) = \pi i \lim_{z \rightarrow n-m\tau} \frac{z - n + m\tau}{1 \pm e^{\pi i m \tau + \pi i z}} = \frac{1}{\pm e^{\pi i n}} = \pm (-1)^n,$$

o que coincide com (5) pois para cada ponto da forma $z = n - m\tau$, $n, m \in \mathbb{Z}$, apenas uma das fracções da série (6) tem aí um pólo simples. Assim, como a função F e a série são ambas funções elípticas relativas ao mesmo reticulado (i.e, com os mesmos períodos) e têm os mesmos pólos com as mesmas ordens então o seu quociente é uma função elíptica e holomorfa, logo constante; por outro lado, como os resíduos coincidem, este quociente é 1. \square

Estamos agora em condições de terminar o argumento de Jacobi. Fazendo $z = \frac{1}{2}$, isto é, $p = i$, na fórmula (6) e substituindo em (4), obtemos

$$\begin{aligned} 1 + \sum_{N \geq 0} \rho(N) q^N &= \vartheta_3(0)^2 = \frac{1}{\pi} F\left(\frac{1}{2}\right) = 2 \sum_{m \in \mathbb{Z}} \frac{q^m}{1 + q^{2m}} = 1 + 4 \sum_{m \geq 1} \frac{q^m}{1 + q^{2m}} = \\ &= 1 + 4 \sum_{m \geq 1} q^m \frac{1 - q^{2m}}{1 - q^{4m}} = 1 + 4 \sum_{m \geq 1} (q^m - q^{3m}) \sum_{l \geq 0} q^{4ml} = \\ &= 1 + 4 \sum_{m \geq 1} \sum_{l \geq 0} q^{m(4l+1)} - 4 \sum_{m \geq 1} \sum_{l \geq 0} q^{m(4l+3)} = \\ &= 1 + 4 \sum_{N \geq 1} d_1(N) q^N - 4 \sum_{N \geq 1} d_3(N) q^N, \end{aligned}$$

tal como se pretende mostrar. Assim, para terminar a demonstração do teorema de Jacobi, falta apenas mostrar a proposição 3.

7. DEMONSTRAÇÃO DA PROPOSIÇÃO 3

Vamos finalmente mostrar a fórmula que relaciona as quatro funções theta em $z = 0$. Para obtê-la, vamos usar a proposição 2, nomeadamente, o facto de que todas as funções ϑ verificam a equação do calor

$$4\pi i \frac{\partial u}{\partial \tau} = \frac{\partial^2 u}{\partial z^2}.$$

Considere-se então a função

$$g(z) = \frac{2\vartheta_1(z) \vartheta_2(z) \vartheta_3(z) \vartheta_4(z)}{\vartheta_1(2z) \vartheta_2(0) \vartheta_3(0) \vartheta_4(0)}.$$

Usando técnicas semelhantes às que usámos na demonstração da proposição 1.(v), é fácil ver que $g(z)$ é periódica em relação ao reticulado $\mathbb{Z} \oplus \tau\mathbb{Z}$ e que não tem pólos. Dado que uma função inteira e duplamente periódica é constante e que

$$\lim_{z \rightarrow 0} g(z) = \lim_{z \rightarrow 0} \frac{2\vartheta_1'(0)}{2\vartheta_1'(0)} = 1,$$

provámos então a seguinte fórmula de duplicação:

$$\vartheta_1(2z) = \frac{2\vartheta_1(z)\vartheta_2(z)\vartheta_3(z)\vartheta_4(z)}{\vartheta_2(0)\vartheta_3(0)\vartheta_4(0)}.$$

Tirando o logaritmo e derivando em relação a z obtemos

$$\frac{2\vartheta_1'(2z)}{\vartheta_1(2z)} = \frac{\vartheta_1'(z)}{\vartheta_1(z)} + \frac{\vartheta_2'(z)}{\vartheta_2(z)} + \frac{\vartheta_3'(z)}{\vartheta_3(z)} + \frac{\vartheta_4'(z)}{\vartheta_4(z)}.$$

Derivando uma vez mais em relação a z e pondo $z = 0$, obtemos

$$\frac{\vartheta_1'''(0)}{\vartheta_1(0)} = \frac{\vartheta_2''(0)}{\vartheta_2(0)} + \frac{\vartheta_3''(0)}{\vartheta_3(0)} + \frac{\vartheta_4''(0)}{\vartheta_4(0)}.$$

Para obter esta expressão, usámos o facto de que $\vartheta_2'(0) = \vartheta_3'(0) = \vartheta_4'(0) = 0$ e que ϑ_1 é ímpar com um zero simples na origem. Esta propriedade de ϑ_1 implica que a expansão de Laurent de ϑ_1'/ϑ_1 em torno da origem é dada por

$$\frac{\vartheta_1'(z)}{\vartheta_1(z)} = \frac{1}{z} + \frac{2\vartheta_1'''(0)}{3\vartheta_1'(0)} + O(z^3),$$

de onde segue, após alguns cálculos, a expressão acima.

Finalmente, usando a equação do calor, transformamos as segundas derivadas em relação a z em derivadas em ordem a τ :

$$\frac{\partial}{\partial \tau} \frac{\vartheta_1'(0)}{\vartheta_1(0)} = \frac{\partial}{\partial \tau} \frac{\vartheta_2(0)}{\vartheta_2(0)} + \frac{\partial}{\partial \tau} \frac{\vartheta_3(0)}{\vartheta_3(0)} + \frac{\partial}{\partial \tau} \frac{\vartheta_4(0)}{\vartheta_4(0)},$$

o que é equivalente a

$$\frac{\partial}{\partial \tau} \left[\log \left(\frac{\vartheta_2(0)\vartheta_3(0)\vartheta_4(0)}{\vartheta_1'(0)} \right) \right] \Big|_{z=0} = 0.$$

Isto significa que a expressão $\vartheta_2(0)\vartheta_3(0)\vartheta_4(0)\vartheta_1'(0)^{-1}$, à partida uma função de τ , é, no entanto, constante para todo $\tau \in \mathbb{H}$. Para concluir, falta verificar que esta constante é π , o que segue das expansões das funções ϑ com $z = 0$ (isto é $p = 1$) quando τ se aproxima de $i\infty$ (isto é, $q = e^{\pi i\tau} \rightarrow 0$). Neste limite, calculando os

termos de menor ordem de ϑ_k na potência de q , obtemos

$$\begin{aligned}\vartheta_1'(0) &= 2\pi q^{1/4} + O(q^{9/4}) \\ \vartheta_2(0) &= 2q^{1/4} + O(q^{9/4}) \\ \vartheta_3(0) &= 1 + O(q) \\ \vartheta_4(0) &= 1 + O(q),\end{aligned}$$

de onde segue a fórmula de Jacobi.

8. ALGUMAS GENERALIZAÇÕES

Finalmente, vamos escrever umas linhas sobre as relações deste problema com outras matérias, e sobre a generalização destas técnicas a outros contextos.

8.1. Pontos inteiros em esferas de maior dimensão. A relação (3) da função $\vartheta_3(0)^2$ com pontos inteiros de circunferências no plano, generaliza-se imediatamente a outras dimensões. Assim temos

$$(7) \quad \vartheta_3(0)^d = \left(\sum_{k \in \mathbb{Z}} q^{k^2} \right)^d = \sum_{k_1 \in \mathbb{Z}} \dots \sum_{k_d \in \mathbb{Z}} q^{k_1^2 + \dots + k_d^2} = 1 + \sum_{N \geq 1} \rho_d(N) q^N,$$

onde $\rho_d(N)$ designa o número de representações do inteiro $N \geq 1$ como soma de d quadrados (ou, equivalentemente, o número de pontos inteiros na esfera $(d-1)$ -dimensional em \mathbb{R}^d de raio \sqrt{N}). Por outro lado, temos também, como consequência das proposições 1 e 3, para $d = 2k$ par

$$\vartheta_3(0)^{2k} = \left(\frac{1}{\pi} F\left(\frac{1}{2}\right) \right)^k$$

onde $F(z) = \frac{\vartheta_1'(0) \vartheta_4(z)}{\vartheta_4(0) \vartheta_1(z)}$ é a função elíptica já usada anteriormente.

Assim, a expansão em série de Taylor de $F\left(\frac{1}{2}\right)^k$ (na variável $q = e^{\pi i \tau}$) dar-nos-á uma outra representação de $\vartheta_3(0)^{2k}$, que podemos comparar com (7). Esta abordagem é, no entanto, apenas bem sucedida para d par e para $d \leq 8$, porque só nestes casos obtemos séries semelhantes às séries de Lambert usadas anteriormente. Mais precisamente, só nestes casos podem os coeficientes das séries obtidas ser expressos em termos de funções aritméticas conhecidas, como é o caso das funções $d_j(n)$, que usámos no caso $d = 2$. Como exemplo, indicamos aqui o resultado obtido para $d = 2k = 4$, em que a série que se obtém é (veja-se, por exemplo [MM],[G])

$$F\left(\frac{1}{2}\right)^2 = \pi^2 - 32\pi^2 \sum_{m \geq 1} \frac{mq^{4m}}{1 - q^{4m}} + 8\pi^2 \sum_{m \geq 1} \frac{nq^n}{1 - q^n}.$$

Daqui resulta então

$$\begin{aligned}
 \vartheta_3(0)^4 &= \frac{1}{\pi^2} F\left(\frac{1}{2}\right)^2 = 1 - 32 \sum_{m \geq 1} \frac{mq^{4m}}{1 - q^{4m}} + 8 \sum_{m \geq 1} \frac{nq^n}{1 - q^n} = \\
 &= 1 - 32 \sum_{m \geq 1} \sum_{k \geq 0} q^{4m(k+1)} + 8 \sum_{n \geq 1} \sum_{l \geq 0} q^{n(l+1)} = \\
 &= 1 - 8 \sum_{d|N, d \equiv 0 \pmod{4}} d q^N + 8 \sum_{d|N} d q^N.
 \end{aligned}$$

Assim demonstrou Jacobi outro resultado extraordinário.

Theorem 2. *Dado um inteiro positivo N , o número de soluções inteiras da equação $x_1^2 + x_2^2 + x_3^2 + x_4^2 = N$ é igual a oito vezes a soma dos divisores de N que não são congruentes com 0 módulo 4.*

Note-se que esta fórmula implica que todos os inteiros positivos se podem escrever como soma de 4 (ou mais, evidentemente) quadrados, facto este que já era bem conhecido de Lagrange⁷ (e suspeita-se que seria do conhecimento da antiga Babilónia!).

8.2. Outras formas quadráticas. Podemos considerar o problema análogo, substituindo a circunferência por uma elipse ou outra cónica. Este problema equivale à determinação dos possíveis valores e multiplicidades das formas quadráticas binárias (em duas variáveis)

$$(8) \quad q(x, y) = ax^2 + bxy + cy^2,$$

com a, b e c inteiros. Para este tipo de equações, um estudo detalhado do ponto de vista aritmético foi levado a cabo por Gauss⁸ que, entre outras coisas, notou que existem classes de cónicas para as quais o problema é semelhante. Mais precisamente, diz-se que duas formas quadráticas q_1 e q_2 são numericamente equivalentes se os inteiros que representam são os mesmos (i.e, $q_1(\mathbb{Z}^2) = q_2(\mathbb{Z}^2)$). Há ainda outra definição de equivalência para a qual é útil representarmos as formas quadráticas na forma matricial, de modo a que a equação (8) se escreve como $q(\mathbf{x}) = \mathbf{x}^t Q \mathbf{x}$, onde

$$Q = \begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{bmatrix}$$

(\mathbf{x} é o vector (x, y) e t designa a transposição). Assim, dizemos que q_1 e q_2 são algebricamente equivalentes se existe uma matriz unimodular (de determinante igual

⁷J.-L. Lagrange, matemático franco-italiano, 1736-1813.

⁸C. F. Gauss, matemático alemão, 1777-1855.

a 1) com entradas inteiras M , tal que as matrizes de q_1 e q_2 verificam

$$M^t Q_1 M = Q_2.$$

A descoberta de Gauss é que estas duas noções são precisamente idênticas. Assim, por exemplo, os inteiros representados pela forma $q_1(x, y) = 5x^2 - 6xy + 2y^2$, são precisamente os mesmos que os representados por $q_2(x, y) = x^2 + y^2$, pois estas formas são algebricamente equivalentes.

8.3. Relação com funções zeta. Outro desenvolvimento interessante a partir deste círculo de problemas, é a relação das fórmulas obtidas para o número de pontos inteiros numa curva com a chamada função zeta de Riemann⁹

$$\zeta(s) = \sum_{n \in \mathbb{N}} \frac{1}{n^s} = 1 + 2^{-s} + 3^{-s} + \dots$$

Como é bem sabido, esta simples função está por detrás de um dos problemas mais famosos da actualidade matemática ainda por resolver, a *hipótese de Riemann*, segundo a qual os zeros (não triviais) da (continuação analítica para $\mathbb{C} \setminus \{1\}$) da função $\zeta(s)$ estarão localizados na recta $Re(s) = \frac{1}{2}$.

Há muitas outras generalizações naturais da função zeta de Riemann, entre as quais as funções zeta das variedades algébricas, e as chamadas funções L . Como exemplo, para a cónica dada por $q(x, y) = 0$, onde q é uma forma quadrática da forma (8), define-se

$$Z_q(s) = \sum'_{m, n \in \mathbb{Z}} \frac{1}{q(m, n)^s}$$

onde o acento no somatório significa que somamos os termos com $(m, n) \neq (0, 0)$.

Se p for a forma quadrática que considerámos em detalhe, $p(x, y) = x^2 + y^2$, temos

$$Z_p(s) = \sum'_{m, n \in \mathbb{Z}} \frac{1}{p(m, n)^s} = \rho(1) + \rho(2)2^{-s} + \rho(3)3^{-s} + \dots$$

onde $\rho(N)$ é a função que estudámos acima - o número de representações de N como soma de 2 quadrados.

Como exemplo de função L , consideremos as funções L de Dirichlet,

$$L(\chi, s) := \sum_{n \in \mathbb{N}} \chi(n)n^{-s},$$

onde $\chi(n)$ é um chamado carácter de Dirichlet, que é, por definição uma função multiplicativa, $\chi(mn) = \chi(m)\chi(n)$, periódica, $\chi(n + N) = \chi(n)$, para um certo período N , e que verifica $\chi(n) = 0$ se n e N têm um divisor comum não trivial. Por

⁹B. Riemann, matemático alemão, 1826-66.

exemplo, com período $N = 1$, temos apenas o carácter trivial $\chi \equiv 1$, e com período $N = 4$ temos mais possibilidades, uma das quais é

$$\chi_4(n) = \begin{cases} (-1)^{(n-1)/2}, & n \text{ ímpar} \\ 0, & n \text{ par.} \end{cases}$$

Neste caso, temos

$$L(\chi_4, s) = 1 - 3^{-s} + 5^{-s} - 7^{-s} + \dots .$$

Podemos então mostrar-se que, no caso da forma quadrática mais simples $p(x, y) = x^2 + y^2$, é válida a seguinte fórmula

$$(9) \quad Z_p(s) = 4\zeta(s)L(\chi_4, s) !$$

Esta extraordinária relação entre funções zeta pode ser demonstrada usando propriedades aritméticas dos inteiros Gaussianos $\mathbb{Z}[\sqrt{-1}]$, que não podemos explicar aqui (existem outras fórmulas do género associadas a outras formas quadráticas e a outros anéis, [C]), mas podemos notar que se a assumirmos como válida, obtemos de forma automática a fórmula de Jacobi para o número de pontos inteiros numa circunferência. De facto, (9) equivale a

$$\rho(1) + \rho(2)2^{-s} + \rho(3)3^{-s} + \dots = 4(1 + 2^{-s} + 3^{-s} + \dots)(1 - 3^{-s} + 5^{-s} - 7^{-s} + \dots)$$

de onde podemos inferir,

$$\rho(N) = 4 \sum_{N=jk, k \text{ ímpar}} (-1)^{(k-1)/2} = 4(d_1(N) - d_3(N)) .$$

8.4. Funções não abelianas. Uma vez que falámos de funções abelianas, podemos naturalmente questionar-nos sobre a existência de uma classe de funções mais vasta, ainda com propriedades interessantes, que inclua as abelianas como caso particular. Este foi o tema do artigo seminal de A. Weil [W], que esboçou uma possível generalização das funções abelianas no contexto da geometria algébrica, definindo para esse efeito uma classe de variedades que são generalizações naturais das variedades abelianas (que, como mencionámos acima, são parametrizadas por funções abelianas). Estas variedades são denominadas *espaços moduli de fibrados vectoriais sobre uma curva algébrica* e incluem algumas (não todas!) variedades abelianas como caso particular.

Esta generalização deu origem a muita investigação importante em matemática nos últimos anos, especialmente após se terem reconhecido importantes relações destes assuntos com a Física-Matemática. Em particular, provou-se que estes espaços moduli são espaços de fase de certas teorias de gauge [AB], e que as funções não abelianas correspondentes podem ser vistas, por um lado, como estados quânticos

dessas teorias, e por outro, como os *blocos conformes* associados a teorias de campo conforme [V]. No entanto, apesar de já terem desempenhado um papel importante na geometria algébrica, diferencial e simpléctica, não é claro que estas funções não abelianas desempenhem um papel importante noutras áreas da matemática, como acontece com as abelianas. Em particular, não se conhece nenhuma aplicação destas funções à teoria dos números, mas quem sabe?... O leitor interessado poderá encontrar referências úteis e problemas em aberto no artigo [B].

Acknowledgement. Gostaria de agradecer as muitas conversas estimulantes que tenho mantido ao longo dos anos com os meus colegas e amigos J. Mourão, J. P. Nunes, o apoio e a motivação dos meus professores J. Campos Ferreira, P. Almeida, R. Picken e L. Takhtajan, e o carinho especial da Helena e do Miguel.

REFERÊNCIAS

- [A] V. Arnold, *Mathematical Methods of Classical Mechanics*, Springer-Verlag, 1989.
- [AB] M. Atiyah, R. Bott, *The Yang-Mills equations on a Riemann surface*, Philos. Trans. Roy. Soc. London Ser. A **308** (1983) 523-615.
- [B] A. Beauville, *Vector bundles and generalized theta functions: recent results and open problems*, in *Current Topics in Complex Algebraic Geometry*, MSRI Publications 28, 17-33; Cambridge University Press, 1995. math:alg-geom/9404001.
- [C] P. Cartier, *An introduction to zeta functions*, in *From Number Theory to Physics*, M. Waldschmidt et al, Eds, Springer-Verlag, 1992.
- [G] E. Grosswald, *Representations of Integers as Sums of Squares*, Springer-Verlag, 1985.
- [H] M. D. Hirschhorn, *A simple proof of Jacobi's two-square theorem*, Am. Math. Mon. **92** (1985) 579-80; *A simple proof of Jacobi's four-square theorem*, Proc. AMS **101** (1987) 436-8.
- [J] C. G. J. Jacobi, *Fundamenta Nova Theoriae Functionarum Ellipticarum*, Borntträger, Königsberg, 1829. Reimpresso em, *Gesammelte Werke*, Reimer, Berlin, 1881-91.
- [L] D. Lawden, *Elliptic Functions and Applications*, Springer-Verlag, 1989.
- [MM] H. McKean, V. Moll, *Elliptic Curves: Function Theory, Geometry, Arithmetic*, Cambridge University Press, 1997.
- [M] D. Mumford, *Tata Lectures on Theta I, II, III*, Progress in mathematics, vols. 28, 43, 115, Birkhauser, 1983, 1984, 1991.
- [V] E. Verlinde, *Fusion rules and modular transformations in 2d conformal field theory*, Nucl. Phys. **B300** (1988) 360-376.
- [W] A. Weil, *Généralisation des fonctions abéliennes*, J. Math. pur. appl. (9) **17** (1938) 47-87.
- [WW] E. Whittaker and G. Watson, *A Course of Modern Analysis: An Introduction to the General Theory of Infinite Processes and of Analytic Functions; with an Account of the Principal Transcendental Functions*, 4th Ed, Cambridge University Press, 1967.
- [WT] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Ann. Math. (2) **141**, No.3, 443-551 (1995); A. Wiles and R. Taylor, *Ring-theoretic properties of certain Hecke algebras*, Ann. Math. (2) **141**, No.3, 553-572 (1995).