Um Número Quase Inteiro

Eduardo Rocha Walchek*

Instituto de Ciências Matemáticas e de Computação
Universidade de São Paulo
eduardo.walchek@usp.br

Resumo

Basta uma calculadora para verificar que o número

$$e^{\pi\sqrt{163}} = 262\,537\,412\,640\,768\,743,9999999999992500...$$

é muito próximo a um número inteiro. Apesar de isto parecer ser mera coincidência, mostraremos neste artigo que este fato está, na verdade, ligado a profundos resultados de curvas elípticas complexas e da Teoria Algébrica dos Números.

1. Qual é o seu número favorito?

Muitas pessoas têm um número ao qual devotam um apreço especial, seja porque associam a ele recordações ou superstições, ou ainda, de um ponto de vista mais matemático, reconhecem algumas de suas propriedades como notáveis. A preferência mais comum é por números inteiros, visto que, na linguagem corrente, "número" é muitas vezes metônimo de "número inteiro". Mesmo assim, há quem escolha a razão áurea ϕ, a constante de Euler e, o célebre π ou i, a unidade imaginária.

Não foi apenas uma vez que, após dizer a alguém que estudo Matemática, a infame pergunta que titula esta introdução me foi proposta. Mesmo assim, nunca havia pensado seriamente em uma resposta para essa questão. Porém, meu primeiro contato com a Teoria Algébrica dos Números me levou a eleger o meu número preferido: $e^{\pi\sqrt{163}}$. A sua reação ao ler este número talvez tenha sido a mesma mistura de frustração, desconfiança e curiosidade com que minha resposta normalmente é recebida. Espero, com este artigo, mostrar o que vejo de tão especial em tal número (ou, pelo menos, mostrar que *há* algo especial com ele, afinal de contas), embora esta seja apenas uma desculpa para propor-lhe um singelo convite à Teoria dos Números.

2. Brevíssima Introdução às Curvas Elípticas Complexas

Por mais irônico que pareça, não só de números vive a Teoria dos Números! Nesta seção, introduziremos as curvas elípticas complexas, que, apesar de à primeira vista não parecerem diretamente relacionadas com o estudo de números, são ferramentas fundamentais para esta área. Para manter esta introdução concisa, omitiremos os detalhes menos pertinentes, mas o leitor não ficará desamparado com as referências que lhe indicaremos.

Todos estamos acostumados com o plano afim $\mathbb{C}^2$, apesar de não podermos visualizá-lo. Ali, observamos uma bijeção entre (inclinações de) retas passando pela origem e pares de pontos

*Agradeço ao professor e xará Eduardo Tengan por me apresentar à Teoria Algébrica dos Números e, em particular, a este curioso número. Agradeço também aos editores e revisores por seu tempo e paciência.

opostos na esfera unitária $\{z \in \mathbb{C}^2; |z| = 1\}$. Já ouviu falar na expressão "retas paralelas se encontram no infinito"? É claro que esta frase não faz sentido no plano afim, mas podemos acrescentar alguns pontos ao nosso espaço para torná-la verdadeira: suponha que, "no infinito", haja uma esfera envolvendo $\mathbb{C}^2$, em que cada ponto dela é a intersecção de todas as retas paralelas com certa inclinação fixada. Como as retas se estendem para ambas as direções, pontos opostos estão associados à mesma família de paralelas e são, portanto, o mesmo ponto! Esta "esfera de raio infinito com antípodas identificadas" é o **plano projetivo**, nosso ambiente de trabalho.

Definição 1. Considere a seguinte relação de equivalência sobre $\mathbb{C}^3 - \{(0,0,0)\}$:

$$(a_1, a_2, a_3) \sim (b_1, b_2, b_3) \iff (a_1, a_2, a_3) = (\lambda b_1, \lambda b_2, \lambda b_3) \quad \text{para algum } \lambda \in \mathbb{C}^\times.$$

O **plano projetivo** sobre $\mathbb{C}$ é definido por $\mathbb{P}^2_{\mathbb{C}} = \mathbb{C}^3 - \{(0,0,0)\}/\sim$, isto é, o conjunto das classes de equivalência de $\sim$. Denotamos a classe de (a_1, a_2, a_3) por $(a_1 : a_2 : a_3)$.[1]

O nosso familiar plano $\mathbb{C}^2$ (ao qual nos referiremos como **parte afim** do plano projetivo) é o conjunto dos pontos da forma $(a_1 : a_2 : 1) = (a_1, a_2)$, enquanto que os pontos da forma $(a_1 : 1 : 0)$ e $(1 : a_2 : 0)$ são os pontos acrescentados no infinito.

Definição 2. Uma **curva elíptica (complexa)** é um conjunto da forma

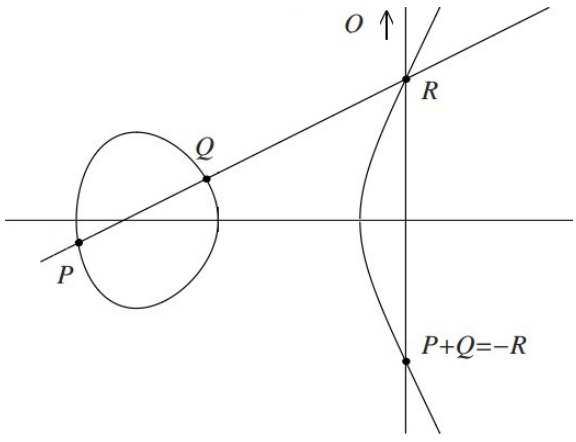
$$E = \{(x : y : z) \in \mathbb{P}^2_{\mathbb{C}};\ y^2 z = 4x^3 - axz^2 - bz^3\},$$

onde $a, b \in \mathbb{C}$ satisfazem $a^3 - 27b^2 \neq 0$. Note que $O \doteq (0 : 1 : 0)$ é o único ponto de E no infinito.

O motivo pelo qual estamos interessados neste objeto é sua estrutura de grupo abeliano, isto é, podemos somar pontos obtendo outros pontos da curva, e esta soma possui propriedades que todos gostamos: associatividade, comutatividade, existência de elemento neutro (que será o O) e de opostos aditivos. Explicitamente, a regra da soma é obtida a partir da máxima ([Was08], p. 12)

Se P, Q e R são colineares, então $P + Q + R = O$.

Mas isto não nos explica diretamente como somar dois pontos! Numa tentativa de entender a regra da soma, troquemos $\mathbb{C}$ por $\mathbb{R}$ (para que possamos desenhar a curva) e, lembrando que os pontos no infinito são intersecções de retas paralelas, pensamos O como um ponto "no topo" de qualquer reta vertical, como na figura ao lado. Para somar dois pontos P e Q, tome a reta que passa por eles[2], que intersecta a curva em outro ponto R. Pela máxima anterior, $R = -(P + Q)$. Se tomamos a vertical passando por R, este ponto será colinear com O e um outro ponto de E que, para que a soma destes seja O, deverá ser $-R = P + Q$.



Agora que conhecemos os objetos, vejamos como eles interagem entre si:

[1] Exercício: tente se convencer de que a "intuição" apresentada acima coincide com esta definição formal!
[2] Se $P = Q$, tome a reta tangente a E em P.

Definição 3. Uma **isogenia** é um mapa polinomial[3] entre curvas elípticas que também é um morfismo de grupos. Uma isogenia inversível por outra isogenia é um **isomorfismo**.

A uma curva elíptica E, associamos um número, chamado ***j*-invariante** de E, dado por

$$j(E) = 1728\frac{a^3}{a^3 - 27b^2} \in \mathbb{C}.$$

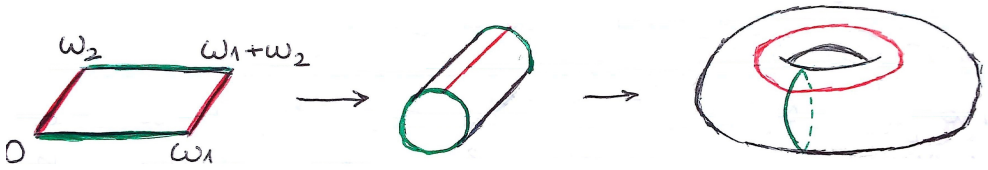
O j-invariante é invariante por isomorfismos (daí o nome!):

Proposição 4. Duas curvas elípticas E e E' são isomorfas se, e somente se, $j(E) = j(E')$.

Esboço da prova. A prova se baseia no fato de um isomorfismo $E' \to E$ atuar na parte afim como $(x, y) \mapsto (u^2x, u^3y)$, com $u \in \mathbb{C}^\times$ ([Sil86], p. 45). Disto, a implicação direta é imediata. Para a recíproca, note que $j(E) = j(E') \implies a^3(b')^2 = (a')^3b^2$. Se $a \neq 0$, tome $u = (a'/a)^{1/4}$. Se não, tome $u = (b'/b)^{1/6}$, pois a condição $a^3 - 27b^2 \neq 0$ garante que a e b não podem ser ambos nulos. □

Como veremos a seguir, o j-invariante de uma curva elíptica E é fortemente influenciado pelo anel $\mathrm{End}(E)$ dos **endomorfismos** de E (que são as isogenias $\phi\colon E \to E$) e esta correlação será fundamental para os propósitos deste artigo. Porém, se já é tão complicado visualizar neste objeto tão abstrato o que é a soma de dois pontos, quanto mais o que é um endomorfismo! Felizmente, *curvas elípticas complexas têm a forma de toros*, e isto facilita imensamente nossa compreensão de seus endomorfismos.

Definição 5. Sejam $\omega_1, \omega_2 \in \mathbb{C}$ linearmente independentes sobre $\mathbb{R}$. O **reticulado** gerado por ω_1 e ω_2 é o subgrupo discreto de $\mathbb{C}$ dado por $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$. O quociente[4] do plano complexo por este reticulado dá origem ao **toro complexo** $\mathbb{C}/\Lambda$:



Sendo um quociente de grupos, $\mathbb{C}/\Lambda$ herda a estrutura de grupo de $\mathbb{C}$. Além disso, os toros são Superfícies de Riemann: *grosso modo*, para cada ponto, podemos tomar uma vizinhança homeomorfa a uma vizinhança de um ponto de $\mathbb{C}$, de modo que, se duas vizinhanças do toro que se intersectam são mandadas em vizinhanças "distantes" em $\mathbb{C}$, ainda assim podemos passar de uma a outra suavemente, isto é, por meio de transformações bi-holomorfas.[5] De fato, basta escolher em torno de cada ponto um aberto suficientemente pequeno que não contenha pontos Λ-equivalentes e ele vai ser idêntico a um aberto em $\mathbb{C}$ (literalmente!). A transição entre duas cartas é feita por meio de translações. Assim, podemos até mesmo falar entre funções holomorfas entre toros: transportamos a função localmente para o nível das cartas e passamos a falar em holomorficidade de funções complexas.

[3] Isto é, na parte afim, uma isogenia atua como $(x, y) \mapsto (p_1(x, y), p_2(x, y))$, com $p_1, p_2 \in \mathbb{C}[x, y]$. Note que ser morfismo de grupos implica que o O de uma curva elíptica é levado no O da outra.

[4] Quocientes servem para identificar pontos: observe que Λ "particiona" $\mathbb{C}$ em paralelogramos idênticos, que diferem entre si por translações dadas por elementos de Λ. No quociente, identificamos todos os pontos que estão na mesma posição relativa em seus respectivos paralelogramos. Como o lado de cima de um paralelogramo é o lado de baixo de outro, temos que colar o lado de cima com o lado de baixo, e o mesmo vale para os outros lados, como mostrado na figura.

[5] A estes homeomorfismos (ou, abusando da nomenclatura, às vizinhanças complexas de chegada) chamamos cartas, e ao conjunto deles, atlas. É como se uma Superfície de Riemann fosse um planeta, para o qual dispomos de um atlas geográfico: todas as partes do planeta estão representadas em alguma carta e duas cartas que cobrem uma mesma região precisam ser coerentes (aliás, esta é a motivação dos nomes destes objetos!).

Teorema 6 (Uniformização)**.** Dada uma curva elíptica E, existe um único (a menos de isomorfismo) toro $\mathbb{C}/\Lambda$ isomorfo a ela como grupo. Reciprocamente, dado um toro $\mathbb{C}/\Lambda$, existe uma única (a menos de isomorfismos) curva elíptica E isomorfa a ele como grupo ([Was08], p. 270).

Na prática, curvas elípticas e toros são a mesma coisa! A noção de isogenia de curvas elípticas se transfere para o mundo dos toros como:

Definição 7. Uma **isogenia** é uma função holomorfa entre toros que também é um morfismo de grupos. Uma isogenia inversível por outra isogenia é um **isomorfismo**.

Na verdade, podemos ir além, observando, em vez dos toros, seus reticulados:

Proposição 8. Dados dois toros $\mathbb{C}/\Lambda$ e $\mathbb{C}/\Lambda'$, existe uma isogenia $\phi\colon \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ se, e somente se, $\alpha\Lambda \subseteq \Lambda'$, para algum $\alpha \in \mathbb{C}^\times$. Além disso, estes toros são isomorfos se, e somente se, $\alpha\Lambda = \Lambda'$, para algum $\alpha \in \mathbb{C}^\times$ ([DS05], p. 26).

Em particular, aplicando a homotetia $\frac{1}{\omega_2}$ ao reticulado $\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$, toda curva elíptica é isomorfa a um toro "normalizado" da forma $\mathbb{C}/\Lambda_\tau$, onde $\Lambda_\tau = \mathbb{Z}\tau \oplus \mathbb{Z}$.

Logo, para falar em endomorfismos de toros (e, portanto, em endomorfismos de curvas elípticas), basta falar em homotetias de reticulados. Com isto, fica fácil ver, por exemplo, que os mapas de multiplicação por inteiro

$$[N]\colon E \to E, \quad [N](P) = \begin{cases} \underbrace{P + \cdots + P}_{N \text{ vezes}} & N \geqslant 0 \\ -(\underbrace{P + \cdots + P}_{|N| \text{ vezes}}) & N < 0 \end{cases} \qquad \text{com } N \in \mathbb{Z}$$

são sempre endomorfismos para qualquer E, pois correspondem a homotetias de multiplicação por inteiro no nível dos reticulados. Em geral, estes são os únicos endomorfismos de que uma curva elíptica dispõe. Uma curva elíptica que possui mais endomorfismos além destes é dita possuir **multiplicação complexa** (pois assim chamamos estes endomorfismos extras). Por exemplo, o reticulado (e portanto a curva elíptica associada[6]) $\mathbb{Z}i \oplus \mathbb{Z}$ tem uma multiplicação complexa por i (que atua como uma rotação de 90 graus), e o reticulado $\mathbb{Z}e^{\pi i/3} \oplus \mathbb{Z}$ tem uma multiplicação complexa por $2e^{\pi i/3}$ (que atua como uma ampliação seguida de uma rotação de 60 graus).[7]

Ainda assim, a existência de multiplicação complexa é bastante restritiva, como veremos na seção seguinte.

3. Um pouco de Teoria Algébrica dos Números

Seja K um corpo que contém $\mathbb{Q}$. Um elemento de K é chamado **inteiro algébrico** se é raiz de um polinômio mônico com coeficientes em $\mathbb{Z}$. O conjunto dos inteiros algébricos de K é um subanel, que denotaremos $\mathcal{O}_K$. Para o corpo[8] $K = \mathbb{Q}(\sqrt{-d})$, com $d \in \mathbb{N}$ livre de quadrados[9], este subanel é explicitamente dado por:

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{-d}] & \text{, se } d \equiv 1,\ 2 \mod 4 \\ \mathbb{Z}\left[\dfrac{1+\sqrt{-d}}{2}\right] & \text{, se } d \equiv 3 \mod 4 \end{cases}$$

[6] A unicidade que está implícita aqui se dá, como frisado anteriormente, por isomorfismo.

[7] Desenhe!

[8] Este é um caso particular de um **corpo quadrático**, isto é, um corpo da forma $\mathbb{Q}(\alpha)$, onde $\alpha \notin \mathbb{Q}$ satisfaz um polinômio quadrático com coeficientes em $\mathbb{Q}$.

[9] Isto é, se um primo p divide d, p^2 não divide d

Proposição 9. Se $E \cong \mathbb{C}/\Lambda_\tau$ é uma curva elíptica com multiplicação complexa, o corpo $\mathbb{Q}(\tau)$ é quadrático e $\mathrm{End}(E)$ é um subanel de $\mathcal{O}_{\mathbb{Q}(\tau)}$.

Prova. Seja $\mathcal{H} \cong \mathrm{End}(E)$ o conjunto das homotetias de Λ_τ, visto como subanel de $\mathbb{Q}(\tau)$. Um $\alpha \in \mathcal{H}$ leva os geradores do reticulado 1 e τ em outros pontos de Λ_τ, isto é, existem $a, b, c, d \in \mathbb{Z}$ tais que

$$\begin{cases} \alpha = a\tau + b \\ \alpha\tau = c\tau + d \end{cases} \implies \alpha^2 - (b+c)\alpha + bc - ad = 0 \qquad (*)$$

Disto já segue que $\mathrm{End}(E)$ é um subanel dos inteiros algébricos. Como E tem multiplicação complexa, existe uma homotetia α que não é simplesmente uma multiplicação por inteiro. Neste caso, $a \neq 0$. Das equações acima, $a\tau^2 + (b-c)\tau - d = 0$, ou seja, $\mathbb{Q}(\tau)$ é um corpo quadrático. □

Podemos afirmar[10] ainda mais sobre o anel de endomorfismos de uma curva elíptica com multiplicação complexa: com a notação anterior, também pode-se mostrar que $\mathrm{End}(E)$ é uma **ordem** de $\mathbb{Q}(\tau)$, isto é, que existem $\alpha_1, \ldots, \alpha_n \in \mathbb{Q}(\tau)$ tais que $\mathrm{End}(E) = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n \oplus \mathbb{Z}$.

Definição 10. Um subconjunto $\mathfrak{f} \subseteq K$ é um **ideal fracionário** de $\mathcal{O}_K$ se existem um ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ e $b \in \mathcal{O}_K$ não nulo tais que que $\mathfrak{f} = \dfrac{1}{b} \cdot \mathfrak{a}$. A relação entre ideais fracionários não-nulos

$$\mathfrak{f} \sim \mathfrak{g} \iff \mathfrak{f} = \mathfrak{g} \cdot (a) \quad \text{para algum } a \in K^\times$$

é de equivalência e o conjunto de suas classes, munido da operação $\overline{\mathfrak{f}} \cdot \overline{\mathfrak{g}} = \overline{\mathfrak{f} \cdot \mathfrak{g}}$, é um grupo $\mathrm{Cl}(\mathcal{O}_K)$, chamado **grupo de classe** de K, e sua ordem é o **número de classe** de K.

Lema 11. Seja A um anel e denote por $\mathrm{Ell}(A)$ o conjunto das curvas elípticas E (a menos de isomorfismo) tais que $\mathrm{End}(E) \cong A$. Então, $|\mathrm{Ell}(\mathcal{O}_K)| \leqslant |\mathrm{Cl}(\mathcal{O}_K)|$.

A demonstração deste lema é demasiadamente técnica, mas se resume em provar que $\mathrm{Cl}(\mathcal{O}_K)$ age transitivamente sobre $\mathrm{Ell}(\mathcal{O}_K)$ ([Sil94], p. 99). Deste lema, segue um resultado poderoso acerca do j-invariante de determinadas curvas elípticas:

Teorema 12. Se E é um curva elíptica tal que $\mathrm{End}(E) \cong \mathcal{O}_K$, para algum corpo K de número de classe 1, então $j(E)$ é racional.

Prova. Note que um automorfismo de $\mathbb{C}$ age sobre uma curva elíptica E simplesmente agindo sobre seus coeficientes a e b. É evidente que $\mathrm{End}(E) \cong \mathrm{End}(\sigma \cdot E) \cong \mathcal{O}_K$ e, pela definição de j, também vemos que $\sigma \cdot j(E) = j(\sigma \cdot E)$. Pelo lema, $\mathrm{Ell}(\mathcal{O}_K)$ é unitário, isto é, $\sigma \cdot E$ e E devem ser isomorfas, de onde $j(E) = j(\sigma \cdot E) = \sigma \cdot j(E)$, para todo automorfismo σ. Logo,[11] $j(E) \in \mathbb{Q}$. □

Um teorema ainda mais poderoso e, de certa forma, complementar ao anterior, é:

Teorema 13. Se E é uma curva elíptica com multiplicação complexa, $j(E)$ é um inteiro algébrico.

A prova deste teorema é longa e trabalhosa, mas é construtiva: explicitamos o polinômio mônico de coeficientes inteiros que $j(E)$ satisfaz. Tal polinômio é conhecido como **polinômio modular** e possui muitos outros usos (em particular, na teoria das curvas modulares), mas que, infelizmente, fogem do nosso escopo. Direcionamos o leitor interessado na prova a [Sil94], p. 143.

Após esta longa exposição podemos, finalmente, voltar a tratar do número

[10] Você vai ter que confiar em mim desta vez, porque a demonstração deste fato exige diversos conceitos que não tratamos aqui e que não valeria a pena discutir apenas para algo tão pontual. Ao leitor incrédulo recomendamos que siga a trilha indicada no Corollary 9.4 de [Sil86]: a prova é um (belo) passeio por diversos resultados do Capítulo III deste livro.

[11] É fácil ver que Q é fixado por automorfismos de $\mathbb{C}$. Como a conjugação é um automorfismo, $j(E) \in \mathbb{R}$ mas, se $j(E)$ fosse irracional, poderíamos construir um automorfismo de $\mathbb{C}$ que não fixa $j(E)$ (à luz de [Mil18], Remark 9.18, p. 113, tome uma base de transcendência que inclua $j(E)$ e o leve em outro elemento), excluindo esta possibilidade.

4. e elevado a π raiz quadrada de... o quê, mesmo?

Lembre-se de que uma curva elíptica E é isomorfa a um toro da forma $\mathbb{C}/\Lambda_\tau$, onde $\Lambda_\tau = \mathbb{Z}\tau \oplus \mathbb{Z}$. Note que, trocando Λ_τ por $\frac{1}{\tau}\Lambda_\tau$ se necessário, podemos supor que $\tau \in \mathbb{H} = \{z \in \mathbb{C}, \mathrm{Im}(z) > 0\}$. Neste caso, o j-invariante de E coincide com o valor de uma função homônima definida em $\mathbb{H}$ calculada em τ, cuja série de Fourier é dada por[12]

$$j(z) = \frac{1}{e^{2\pi i z}} + 744 + \sum_{n=1}^{\infty} a_n e^{2\pi i n z}$$

onde os coeficientes a_n são todos inteiros! Em particular, para (de agora em diante) $\tau \doteq \frac{1+\sqrt{-163}}{2}$,

$$j\left(\frac{1+\sqrt{-163}}{2}\right) = -e^{\pi\sqrt{163}} + 744 + \sum_{n=1}^{\infty} a_n e^{2\pi i n \tau}$$

Note que $e^{2\pi i \tau}$ é um número muito pequeno, neste caso: de fato,

$$|-e^{-\pi\sqrt{163}}| \approx 3,808980937 \cdot 10^{-18}$$

Logo, a série na expressão anterior é irrelevante. Certo, mas até agora não há nada de especial com o 163, não é? Poderíamos ter escolhido um outro número e obter resultados similares. O fato importante a este respeito é que os únicos valores positivos de d para os quais $\mathcal{O}_K$, o anel de inteiros de $K = \mathbb{Q}(\sqrt{-d})$, é um Domínio de Ideais Principais são 1, 2, 3, 7, 11, 19, 43, 67 e 163, os números de Heegner-Stark[13]. Nestes casos, o número de classe de K é 1.

Considere uma curva elíptica E isomorfa ao toro $\mathbb{C}/\Lambda_\tau$. Note que E tem multiplicação complexa: τ é uma homotetia não-inteira de Λ_τ. Portanto, pelo teorema 13, $j(E)$ é um inteiro algébrico. Por outro lado, $\mathrm{End}(E)$ é um subanel de $\mathcal{O}_{\mathbb{Q}(\sqrt{-163})} = \mathbb{Z}[\tau]$. Mas τ satisfaz um polinômio quadrático *mônico* com coeficientes inteiros (qual?), de onde $\mathbb{Z}[\tau] = \mathbb{Z} \oplus \mathbb{Z}\tau$. Além disso, $\mathrm{End}(E)$ é uma ordem que contém τ e, consequentemente, $\mathrm{End}(E) = \mathbb{Z}[\tau]$. Logo, $\mathrm{End}(E) \cong \mathcal{O}_{\mathbb{Q}(\sqrt{-163})}$ e segue do teorema 12 que $j(E)$ é racional. Sendo simultaneamente racional e inteiro algébrico, isto só pode significar que $j(E)$ é um inteiro![14] Logo, como comentamos acima, $j(\tau) = j(E)$ é um inteiro, e

$$e^{\pi\sqrt{163}} \approx 744 - j\left(\frac{1+\sqrt{-163}}{2}\right) \in \mathbb{Z}$$

isto é, o celebrado número $e^{\pi\sqrt{163}}$ merece, de fato, ser chamado "quase inteiro"!

Mas por que o 163, e não outro número de Heegner-Stark? Na tabela a seguir compilamos os valores correspondentes de $e^{\pi\sqrt{d}}$ que obteríamos para os outros candidatos:

[12] Não por acaso, esta função é chamada **invariante modular** e, entre outras propriedades interessantes de que dispõe, é invariante pela ação do grupo $\mathrm{SL}_2(\mathbb{Z})$, das matrizes de entradas inteiras e determinante 1, sobre $\mathbb{H}$ por transformações de Möbius. Para mais detalhes, veja [Ser73], p. 89 e [DS05], p. 35.

[13] Sequência A003173 na *On-line Encyclopedia of Integer Sequences* (OEIS): `https://oeis.org/A003173`

[14] Seja $a/b \in \mathbb{Q}$, com $\mathrm{mdc}(a,b) = 1$ e $b > 0$, raiz de um polinômio mônico $x^n + c_1 x^{n-1} + \cdots + c_{n-1}x + c_n$. Logo, $a^n = -c_1 a^{n-1} b - \cdots - c_{n-1} a b^{n-1} - c_n b^n$ e, como b divide o lado direito, b divide a^n. Como $\mathrm{mdc}(a,b) = 1$, só resta $b = 1$.

d	$e^{-\pi\sqrt{d}} \approx$	$e^{\pi\sqrt{d}} \approx$
1	$4,321391826 \cdot 10^{-2}$	23, 140692632779269005729086367949
2	$1,176198053 \cdot 10^{-2}$	85, 019695223207217582510872858831
3	$4,333420510 \cdot 10^{-3}$	230, 764588319145879240075153931 01
7	$2,455836631 \cdot 10^{-4}$	4071, 93209522526109852456833255 76
11	$2,984527339 \cdot 10^{-5}$	33506, 14306559243876668155096281 9
19	$1,129331268 \cdot 10^{-6}$	885479, 77768015431949753789348172
43	$1,130279721 \cdot 10^{-9}$	884736743, 99977746603490666193746
67	$6,793572746 \cdot 10^{-12}$	147197952743, 99999866245422450683
163	$3,808980937 \cdot 10^{-18}$	262537412640768743, 99999999999925

Com isto, explicamos a quase integralidade de $e^{\pi\sqrt{163}}$: um curioso fato que pode ser verificado com uma simples calculadora, mas que requer ferramental um pouco mais sofisticado para ser precisamente justificado.

Referências

[DS05] F. Diamond, J. Shurman, *A First Course in Modular Forms (GTM 228)*, Springer, 2005.

[Mil18] J. Milne, *Fields and Galois Theory*, disponível em `https://www.jmilne.org/math/CourseNotes/FT.pdf`, acessado em 12 de setembro de 2018.

[Ser73] J.-P. Serre, *A Course in Arithmetic (GTM 7)*, Springer, 1973.

[Sil86] J. Silverman, *The Arithmetic of Elliptic Curves (GTM 106)*, Springer, 1986.

[Sil94] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves (GTM 151)*, Springer, 1994.

[Was08] L. Washington, *Elliptic Curves, Number Theory and Cryptography*, CRC Press, 2008.