Os Inteiros de Hurwitz e Problemas Diofantinos

António Machiavelo

Centro de Matemática da Universidade do Porto

Primeiro Encontro Português de Teoria dos Números

Universidade de Aveiro

2 de novembro de 2022

Os quaterniões racionais

$$\mathbb{H}(\mathbb{Q}) = \{a + bi + cj + dk : a, b, c, d \in \mathbb{Q}\}$$

com a adição natural e a multiplicação determinada por

$$i^2 = j^2 = k^2 = -1, \qquad ij = k = -ji$$

é uma álgebra de divisão.

Os quaterniões racionais

$$\mathbb{H}(\mathbb{Q}) = \{a + bi + cj + dk : a, b, c, d \in \mathbb{Q}\}$$

com a adição natural e a multiplicação determinada por

$$i^2 = j^2 = k^2 = -1, \qquad ij = k = -ji$$

é uma álgebra de divisão. Tem-se

$$\begin{aligned}(u_0 + u_1 i + u_2 j + u_3 k)(v_0 + v_1 i + v_2 j + v_3 k) = \\ = (u_0 v_0 - u_1 v_1 - u_2 v_2 - u_3 v_3) + (u_0 v_1 + u_1 v_0 + u_2 v_3 - u_3 v_2) i + \\ (u_0 v_2 - u_1 v_3 + u_2 v_0 + u_3 v_1) j + (u_0 v_3 + u_1 v_2 - u_2 v_1 + u_3 v_0) k.\end{aligned}$$

Os quaterniões racionais

$$\mathbb{H}(\mathbb{Q}) = \{a + bi + cj + dk : a, b, c, d \in \mathbb{Q}\}$$

com a adição natural e a multiplicação determinada por

$$i^2 = j^2 = k^2 = -1, \qquad ij = k = -ji$$

é uma álgebra de divisão. Tem-se

$$\begin{aligned}(u_0 + u_1 i + u_2 j + u_3 k)(v_0 + v_1 i + v_2 j + v_3 k) = \\ = (u_0 v_0 - u_1 v_1 - u_2 v_2 - u_3 v_3) + (u_0 v_1 + u_1 v_0 + u_2 v_3 - u_3 v_2) i + \\ (u_0 v_2 - u_1 v_3 + u_2 v_0 + u_3 v_1) j + (u_0 v_3 + u_1 v_2 - u_2 v_1 + u_3 v_0) k.\end{aligned}$$

Se $z = a + bi + cj + dk$, então:

- $\bar{z} = a - bi - cj - dk$ é o seu conjugado;

Os quaterniões racionais

$$\mathbb{H}(\mathbb{Q}) = \{a + bi + cj + dk : a, b, c, d \in \mathbb{Q}\}$$

com a adição natural e a multiplicação determinada por

$$i^2 = j^2 = k^2 = -1, \qquad ij = k = -ji$$

é uma álgebra de divisão. Tem-se

$$\begin{aligned}(u_0 + u_1 i + u_2 j + u_3 k)(v_0 + v_1 i + v_2 j + v_3 k) = \\ = (u_0 v_0 - u_1 v_1 - u_2 v_2 - u_3 v_3) + (u_0 v_1 + u_1 v_0 + u_2 v_3 - u_3 v_2) i + \\ (u_0 v_2 - u_1 v_3 + u_2 v_0 + u_3 v_1) j + (u_0 v_3 + u_1 v_2 - u_2 v_1 + u_3 v_0) k.\end{aligned}$$

Se $z = a + bi + cj + dk$, então:

- $\bar{z} = a - bi - cj - dk$ é o seu conjugado; $\quad \overline{w\,z} = \bar{z}\,\bar{w}$.

Os quaterniões racionais

$$\mathbb{H}(\mathbb{Q}) = \{a + bi + cj + dk : a, b, c, d \in \mathbb{Q}\}$$

com a adição natural e a multiplicação determinada por

$$i^2 = j^2 = k^2 = -1, \qquad ij = k = -ji$$

é uma álgebra de divisão. Tem-se

$$\begin{aligned}(u_0 + u_1 i + u_2 j + u_3 k)(v_0 + v_1 i + v_2 j + v_3 k) = \\ = (u_0 v_0 - u_1 v_1 - u_2 v_2 - u_3 v_3) + (u_0 v_1 + u_1 v_0 + u_2 v_3 - u_3 v_2) i + \\ (u_0 v_2 - u_1 v_3 + u_2 v_0 + u_3 v_1) j + (u_0 v_3 + u_1 v_2 - u_2 v_1 + u_3 v_0) k.\end{aligned}$$

Se $z = a + bi + cj + dk$, então:

- $\bar{z} = a - bi - cj - dk$ é o seu conjugado; $\quad \overline{w\,z} = \bar{z}\,\bar{w}$.
- $\mathrm{N}(z) = z\bar{z} = a^2 + b^2 + c^2 + d^2$ é a sua norma;

Os quaterniões racionais

$$\mathbb{H}(\mathbb{Q}) = \{a + bi + cj + dk : a, b, c, d \in \mathbb{Q}\}$$

com a adição natural e a multiplicação determinada por

$$i^2 = j^2 = k^2 = -1, \qquad ij = k = -ji$$

é uma álgebra de divisão. Tem-se

$$\begin{aligned}(u_0 + u_1 i + u_2 j + u_3 k)(v_0 + v_1 i + v_2 j + v_3 k) = \\ = (u_0 v_0 - u_1 v_1 - u_2 v_2 - u_3 v_3) + (u_0 v_1 + u_1 v_0 + u_2 v_3 - u_3 v_2) i + \\ (u_0 v_2 - u_1 v_3 + u_2 v_0 + u_3 v_1) j + (u_0 v_3 + u_1 v_2 - u_2 v_1 + u_3 v_0) k.\end{aligned}$$

Se $z = a + bi + cj + dk$, então:

- $\bar{z} = a - bi - cj - dk$ é o seu conjugado; $\quad \overline{w\,z} = \bar{z}\,\bar{w}$.
- $\mathrm{N}(z) = z\bar{z} = a^2 + b^2 + c^2 + d^2$ é a sua norma;

$$\mathrm{N}(w\,z) = \mathrm{N}(w)\,\mathrm{N}(z).$$

Os quaterniões racionais

$$\mathbb{H}(\mathbb{Q}) = \{a + bi + cj + dk : a, b, c, d \in \mathbb{Q}\}$$

com a adição natural e a multiplicação determinada por

$$i^2 = j^2 = k^2 = -1, \qquad ij = k = -ji$$

é uma álgebra de divisão. Tem-se

$$\begin{aligned}(u_0 + u_1 i + u_2 j + u_3 k)(v_0 + v_1 i + v_2 j + v_3 k) = \\ = (u_0 v_0 - u_1 v_1 - u_2 v_2 - u_3 v_3) + (u_0 v_1 + u_1 v_0 + u_2 v_3 - u_3 v_2) i + \\ (u_0 v_2 - u_1 v_3 + u_2 v_0 + u_3 v_1) j + (u_0 v_3 + u_1 v_2 - u_2 v_1 + u_3 v_0) k.\end{aligned}$$

Se $z = a + bi + cj + dk$, então:

- $\bar{z} = a - bi - cj - dk$ é o seu conjugado; $\quad \overline{w\,z} = \bar{z}\,\bar{w}$.
- $\mathrm{N}(z) = z\bar{z} = a^2 + b^2 + c^2 + d^2$ é a sua norma;
$$\mathrm{N}(w\,z) = \mathrm{N}(w)\,\mathrm{N}(z).$$
- $\Re(z) = a = \frac{1}{2}(z + \bar{z})$;

Os quaterniões racionais

$$\mathbb{H}(\mathbb{Q}) = \{a + bi + cj + dk : a, b, c, d \in \mathbb{Q}\}$$

com a adição natural e a multiplicação determinada por

$$i^2 = j^2 = k^2 = -1, \qquad ij = k = -ji$$

é uma álgebra de divisão. Tem-se

$$\begin{aligned}(u_0 + u_1 i + u_2 j + u_3 k)(v_0 + v_1 i + v_2 j + v_3 k) = \\ = (u_0 v_0 - u_1 v_1 - u_2 v_2 - u_3 v_3) + (u_0 v_1 + u_1 v_0 + u_2 v_3 - u_3 v_2) i + \\ (u_0 v_2 - u_1 v_3 + u_2 v_0 + u_3 v_1) j + (u_0 v_3 + u_1 v_2 - u_2 v_1 + u_3 v_0) k.\end{aligned}$$

Se $z = a + bi + cj + dk$, então:

- $\bar{z} = a - bi - cj - dk$ é o seu conjugado; $\quad \overline{w\,z} = \bar{z}\,\bar{w}$.
- $\mathrm{N}(z) = z\bar{z} = a^2 + b^2 + c^2 + d^2$ é a sua norma;
$$\mathrm{N}(w\,z) = \mathrm{N}(w)\,\mathrm{N}(z).$$
- $\Re(z) = a = \frac{1}{2}(z + \bar{z})$; $\quad \Re(u\bar{v}) = u \cdot v$.

Inteiros de Lipschitz e inteiros de Hurwitz

Inteiros de Lipschitz:

$$\mathcal{L} = \{a + bi + cj + dk \in \mathbb{H} : a, b, c, d \in \mathbb{Z}\}$$

Inteiros de Lipschitz e inteiros de Hurwitz

Inteiros de Lipschitz:

$$\mathcal{L} = \{a + bi + cj + dk \in \mathbb{H} : a, b, c, d \in \mathbb{Z}\}$$

Inteiros de Hurwitz:

$$\mathcal{H} = \mathcal{L} \cup (\omega + \mathcal{L}), \text{ where } \omega = \tfrac{1}{2}(1 + i + j + k)$$

O anel $\mathcal{H}$ é Euclidiano à esquerda e à direita e, por conseguinte é um DIP, à esquerda e à direita.

Inteiros de Lipschitz e inteiros de Hurwitz

Inteiros de Lipschitz:

$$\mathcal{L} = \{a + bi + cj + dk \in \mathbb{H} : a, b, c, d \in \mathbb{Z}\}$$

Inteiros de Hurwitz:

$$\mathcal{H} = \mathcal{L} \cup (\omega + \mathcal{L}), \text{ where } \omega = \tfrac{1}{2}(1 + i + j + k)$$

O anel $\mathcal{H}$ é Euclidiano à esquerda e à direita e, por conseguinte é um DIP, à esquerda e à direita.

Os inteiros de Hurwitz gozam de uma espécie de fatorização única em primos...

Inteiros de Lipschitz e inteiros de Hurwitz

Inteiros de Lipschitz:

$$\mathcal{L} = \{a + bi + cj + dk \in \mathbb{H} : a, b, c, d \in \mathbb{Z}\}$$

Inteiros de Hurwitz:

$$\mathcal{H} = \mathcal{L} \cup (\omega + \mathcal{L}), \text{ where } \omega = \tfrac{1}{2}(1 + i + j + k)$$

O anel $\mathcal{H}$ é Euclidiano à esquerda e à direita e, por conseguinte é um DIP, à esquerda e à direita.

Os inteiros de Hurwitz gozam de uma espécie de fatorização única em primos...

Note-se que: $\mathrm{N}(\mathcal{H}) \subseteq \mathbb{N}_0$.

Entidades aritméticas

- $\varepsilon \in \mathcal{H}^* \iff \mathrm{N}(\varepsilon) = 1$

Entidades aritméticas

- $\varepsilon \in \mathcal{H}^* \iff \mathrm{N}(\varepsilon) = 1$
- $\mathcal{L}^* = \{\pm 1, \pm i, \pm j, \pm k\}$

Entidades aritméticas

- $\varepsilon \in \mathcal{H}^* \iff \mathrm{N}(\varepsilon) = 1$
- $\mathcal{L}^* = \{\pm 1, \pm i, \pm j, \pm k\}$
- $\mathcal{H}^* = \mathcal{L}^* \cup \left\{ \frac{\pm 1 \pm i \pm j \pm k}{2} \right\}$

Entidades aritméticas

- $\varepsilon \in \mathcal{H}^* \iff \mathrm{N}(\varepsilon) = 1$
- $\mathcal{L}^* = \{\pm 1, \pm i, \pm j, \pm k\}$
- $\mathcal{H}^* = \mathcal{L}^* \cup \left\{ \frac{\pm 1 \pm i \pm j \pm k}{2} \right\}$
- Um primo de $\mathcal{L}$ ou de $\mathcal{H}$ é, por definição, um elemento irredutível. Tem-se:

$$\pi \in \mathcal{H} \text{ é primo } \iff \mathrm{N}(\pi) \text{ é um primo racional}$$

Entidades aritméticas

- $\varepsilon \in \mathcal{H}^* \iff \mathrm{N}(\varepsilon) = 1$
- $\mathcal{L}^* = \{\pm 1, \pm i, \pm j, \pm k\}$
- $\mathcal{H}^* = \mathcal{L}^* \cup \left\{ \frac{\pm 1 \pm i \pm j \pm k}{2} \right\}$
- Um primo de $\mathcal{L}$ ou de $\mathcal{H}$ é, por definição, um elemento irredutível. Tem-se:

$$\pi \in \mathcal{H} \text{ é primo } \iff \mathrm{N}(\pi) \text{ é um primo racional}$$

- $\alpha \in \mathcal{H}$ diz-se primitivo se as suas coordenadas forem coprimas, ou seja, quando não existe $m \in \mathbb{N}_{\geq 2}$ tal que $m \mid \alpha$.

Entidades aritméticas

- $\varepsilon \in \mathcal{H}^* \iff \mathrm{N}(\varepsilon) = 1$
- $\mathcal{L}^* = \{\pm 1, \pm i, \pm j, \pm k\}$
- $\mathcal{H}^* = \mathcal{L}^* \cup \left\{ \frac{\pm 1 \pm i \pm j \pm k}{2} \right\}$
- Um primo de $\mathcal{L}$ ou de $\mathcal{H}$ é, por definição, um elemento irredutível. Tem-se:

$$\pi \in \mathcal{H} \text{ é primo } \iff \mathrm{N}(\pi) \text{ é um primo racional}$$

- $\alpha \in \mathcal{H}$ diz-se primitivo se as suas coordenadas forem coprimas, ou seja, quando não existe $m \in \mathbb{N}_{\geq 2}$ tal que $m \mid \alpha$.

$$\forall_{\alpha \in \mathcal{H} \setminus \mathcal{L}} \ \exists_{\varepsilon \in \mathcal{H}^*} : \ \varepsilon\alpha, \alpha\varepsilon \in \mathcal{L}.$$

Uma espécie de fatorização única

Teorema (Lipschitz, 1886)

Seja $\alpha \in \mathcal{H}$ primitivo e $m = \mathrm{N}(\alpha)$. Para cada fatorização

$$m = p_1 p_2 \cdots p_{k-1} p_k$$

em primos racionais, existe uma fatorização

$$\alpha = \pi_1 \pi_2 \cdots \pi_{k-1} \pi_k$$

em primos de Hurwitz modelada nessa fatorização de m, o que significa que $\mathrm{N}(\pi_i) = p_i$.

$$\begin{array}{c} \pi_i \\ | \\ p_i \end{array}$$

Uma espécie de fatorização única

Teorema (Lipschitz, 1886)

Seja $\alpha \in \mathcal{H}$ primitivo e $m = \mathrm{N}(\alpha)$. Para cada fatorização

$$m = p_1 p_2 \cdots p_{k-1} p_k$$

em primos racionais, existe uma fatorização

$$\alpha = \pi_1 \pi_2 \cdots \pi_{k-1} \pi_k$$

$$\begin{array}{c} \pi_i \\ | \\ p_i \end{array}$$

em primos de Hurwitz modelada nessa fatorização de m, o que significa que $\mathrm{N}(\pi_i) = p_i$.

Mais, se $\alpha = \pi_1 \pi_2 \cdots \pi_{k-1} \pi_k$ é uma qualquer fatorização de α modelada em $p_1 p_2 \cdots p_{k-1} p_k$, então todas as outras têm a forma

$$\alpha = \pi_1 \varepsilon_1 \cdot \varepsilon_1^{-1} \pi_2 \varepsilon_2 \cdot \varepsilon_2^{-1} \pi_2 \varepsilon_3 \cdot \ \cdots \ \cdot \varepsilon_{k-2}^{-1} \pi_{k-1} \varepsilon_{k-1} \cdot \varepsilon_{k-1}^{-1} \pi_k,$$

para alguns $\varepsilon_i \in \mathcal{H}^*$, o que significa que a fatorização num dado modelo é única a menos de migração de unidades.

Metacomutação

Em particular: $p, q \in \mathbb{N}$ primos; $\pi, \rho \in \mathcal{H}$ com $\mathrm{N}(\pi) = p$, $\mathrm{N}(\rho) = q$

Metacomutação

Em particular: $p, q \in \mathbb{N}$ primos; $\pi, \rho \in \mathcal{H}$ com $\mathrm{N}(\pi) = p$, $\mathrm{N}(\rho) = q$ $\implies$ existem $\tilde{\pi}, \tilde{\rho}$, únicos, a menos de associados (esq. e dir.), tais que $\mathrm{N}(\tilde{\pi}) = p$, $\mathrm{N}(\tilde{\rho}) = q$ e

$$\pi\rho = \tilde{\rho}\,\tilde{\pi}.$$

Metacomutação

Em particular: $p, q \in \mathbb{N}$ primos; $\pi, \rho \in \mathcal{H}$ com $\mathrm{N}(\pi) = p$, $\mathrm{N}(\rho) = q$ $\implies$ existem $\tilde{\pi}, \tilde{\rho}$, únicos, a menos de associados (esq. e dir.), tais que $\mathrm{N}(\tilde{\pi}) = p$, $\mathrm{N}(\tilde{\rho}) = q$ e

$$\pi\rho = \tilde{\rho}\,\tilde{\pi}.$$

O problema da metacomutação:

Metacomutação

Em particular: $p, q \in \mathbb{N}$ primos; $\pi, \rho \in \mathcal{H}$ com $\mathrm{N}(\pi) = p$, $\mathrm{N}(\rho) = q$ $\implies$ existem $\tilde{\pi}, \tilde{\rho}$, únicos, a menos de associados (esq. e dir.), tais que $\mathrm{N}(\tilde{\pi}) = p$, $\mathrm{N}(\tilde{\rho}) = q$ e

$$\pi\rho = \tilde{\rho}\,\tilde{\pi}.$$

O problema da metacomutação: relação entre π e $\tilde{\pi}$ (ou ρ e $\tilde{\rho}$) ?

Metacomutação

Em particular: $p, q \in \mathbb{N}$ primos; $\pi, \rho \in \mathcal{H}$ com $\mathrm{N}(\pi) = p$, $\mathrm{N}(\rho) = q$ $\implies$ existem $\tilde{\pi}, \tilde{\rho}$, únicos, a menos de associados (esq. e dir.), tais que $\mathrm{N}(\tilde{\pi}) = p$, $\mathrm{N}(\tilde{\rho}) = q$ e

$$\pi\rho = \tilde{\rho}\,\tilde{\pi}.$$

O problema da metacomutação: relação entre π e $\tilde{\pi}$ (ou ρ e $\tilde{\rho}$) ?

$$\Pi_p = \{\text{classes de associados esquerdos dos primos acima de } p\}$$

Metacomutação

Em particular: $p, q \in \mathbb{N}$ primos; $\pi, \rho \in \mathcal{H}$ com $\mathrm{N}(\pi) = p$, $\mathrm{N}(\rho) = q$ $\Longrightarrow$ existem $\tilde{\pi}, \tilde{\rho}$, únicos, a menos de associados (esq. e dir.), tais que $\mathrm{N}(\tilde{\pi}) = p$, $\mathrm{N}(\tilde{\rho}) = q$ e

$$\pi\rho = \tilde{\rho}\,\tilde{\pi}.$$

O problema da metacomutação: relação entre π e $\tilde{\pi}$ (ou ρ e $\tilde{\rho}$) ?

$$\Pi_p = \{\text{classes de associados esquerdos dos primos acima de } p\}$$

$\#\Pi_p = p + 1$, se p é ímpar; $\#\Pi_2 = 1$.

Metacomutação

Em particular: $p, q \in \mathbb{N}$ primos; $\pi, \rho \in \mathcal{H}$ com $\mathrm{N}(\pi) = p$, $\mathrm{N}(\rho) = q$ $\Longrightarrow$ existem $\tilde{\pi}, \tilde{\rho}$, únicos, a menos de associados (esq. e dir.), tais que $\mathrm{N}(\tilde{\pi}) = p$, $\mathrm{N}(\tilde{\rho}) = q$ e

$$\pi\rho = \tilde{\rho}\,\tilde{\pi}.$$

O problema da metacomutação: relação entre π e $\tilde{\pi}$ (ou ρ e $\tilde{\rho}$) ?

$$\Pi_p = \{\text{classes de associados esquerdos dos primos acima de } p\}$$

$\#\Pi_p = p + 1$, se p é ímpar; $\#\Pi_2 = 1$.

$\mu_\rho : \Pi_p \to \Pi_p$, dada por $\pi \mapsto \tilde{\pi}$, é uma permutação.

Metacomutação

Em particular: $p, q \in \mathbb{N}$ primos; $\pi, \rho \in \mathcal{H}$ com $\mathrm{N}(\pi) = p$, $\mathrm{N}(\rho) = q$ $\implies$ existem $\tilde{\pi}, \tilde{\rho}$, únicos, a menos de associados (esq. e dir.), tais que $\mathrm{N}(\tilde{\pi}) = p$, $\mathrm{N}(\tilde{\rho}) = q$ e

$$\pi\rho = \tilde{\rho}\,\tilde{\pi}.$$

O problema da metacomutação: relação entre π e $\tilde{\pi}$ (ou ρ e $\tilde{\rho}$) ?

$\Pi_p = \{$classes de associados esquerdos dos primos acima de $p\}$

$\#\Pi_p = p + 1$, se p é ímpar; $\#\Pi_2 = 1$.

$\mu_\rho : \Pi_p \to \Pi_p$, dada por $\pi \mapsto \tilde{\pi}$, é uma permutação.

Teorema (H. Cohn, A. Kumar, 2015)

O sinal de μ_ρ é $\left(\frac{q}{p}\right)$

Metacomutação

Em particular: $p, q \in \mathbb{N}$ primos; $\pi, \rho \in \mathcal{H}$ com $\mathrm{N}(\pi) = p$, $\mathrm{N}(\rho) = q$ $\implies$ existem $\tilde{\pi}, \tilde{\rho}$, únicos, a menos de associados (esq. e dir.), tais que $\mathrm{N}(\tilde{\pi}) = p$, $\mathrm{N}(\tilde{\rho}) = q$ e

$$\pi\rho = \tilde{\rho}\,\tilde{\pi}.$$

O problema da metacomutação: relação entre π e $\tilde{\pi}$ (ou ρ e $\tilde{\rho}$) ?

$\Pi_p = \{$classes de associados esquerdos dos primos acima de $p\}$

$\#\Pi_p = p + 1$, se p é ímpar; $\#\Pi_2 = 1$.

$\mu_\rho : \Pi_p \to \Pi_p$, dada por $\pi \mapsto \tilde{\pi}$, é uma permutação.

Teorema (H. Cohn, A. Kumar, 2015)

O sinal de μ_ρ é $\left(\frac{q}{p}\right)$ e μ_ρ tem $1 + \left(\frac{\Re(\rho)-q}{p}\right)$ pontos fixos, exceto quando a parte imaginária de ρ é divisível por p, em cujo caso μ_ρ é a identidade.

A conjetura 1-3-5

Em 2016, Zhì-Wěi Sūn (孙智伟) conjeturou o seguinte:

A conjetura 1-3-5

Qualquer número $m \in \mathbb{N}$ pode ser escrito como uma soma de quatro quadrados, $m = x^2 + y^2 + z^2 + t^2$ com $x, y, z, t \in \mathbb{N}_0$, de tal modo que $x + 3y + 5z$ seja um quadrado perfeito.

A conjetura 1-3-5

Em 2016, Zhì-Wěi Sūn (孙智伟) conjeturou o seguinte:

A conjetura 1-3-5

Qualquer número $m \in \mathbb{N}$ pode ser escrito como uma soma de quatro quadrados, $m = x^2 + y^2 + z^2 + t^2$ com $x, y, z, t \in \mathbb{N}_0$, de tal modo que $x + 3y + 5z$ seja um quadrado perfeito.

Considere-se o problema geral:

Dados $a, b, c, d \in \mathbb{Z}$ e $m, n \in \mathbb{N}$, descrever condições que garantam a existência de uma solução para o sistema diofantino:

$$\begin{cases} x^2 + y^2 + z^2 + t^2 & = & m \\ ax + by + cz + dt & = & n^2. \end{cases}$$

Uma formulação quaterniónica

Pondo $\zeta = a + bi + cj + dk, \gamma = x + yi + zj + tk \in \mathcal{L}$, o sistema anterior pode ser rescrito como

$$\begin{cases} \mathrm{N}(\gamma) &= m \\ \gamma \cdot \zeta = \Re(\bar{\gamma}\zeta) &= n^2. \end{cases}$$

Uma formulação quaterniónica

Pondo $\zeta = a + bi + cj + dk, \gamma = x + yi + zj + tk \in \mathcal{L}$, o sistema anterior pode ser rescrito como

$$\begin{cases} \mathrm{N}(\gamma) &= m \\ \gamma \cdot \zeta = \Re(\bar{\gamma}\zeta) &= n^2. \end{cases}$$

Pondo $\delta = \bar{\gamma}\zeta$, resulta que $\delta = n^2 + Ai + Bj + Ck$, para alguns $A, B, C \in \mathbb{Z}$, e então $m\,\mathrm{N}(\zeta) - n^4 = A^2 + B^2 + C^2$.

Uma formulação quaterniónica

Pondo $\zeta = a + bi + cj + dk, \gamma = x + yi + zj + tk \in \mathcal{L}$, o sistema anterior pode ser rescrito como

$$\begin{cases} \mathrm{N}(\gamma) &= m \\ \gamma \cdot \zeta = \Re(\bar{\gamma}\zeta) &= n^2. \end{cases}$$

Pondo $\delta = \bar{\gamma}\zeta$, resulta que $\delta = n^2 + Ai + Bj + Ck$, para alguns $A, B, C \in \mathbb{Z}$, e então $m\,\mathrm{N}(\zeta) - n^4 = A^2 + B^2 + C^2$.

Assim, por um teorema de Legendre, uma condição necessária para que o sistema tenha solução é que se tenha:

$$m\ \mathrm{N}(\zeta) - n^4 \notin \{4^r(8s+7) : r, s \in \mathbb{N}_0\},$$

e que

$$n \leq \sqrt[4]{m\ \mathrm{N}(\zeta)}.$$

Reciprocamente...

Suponha-se, agora, que essas condições são satisfeitas.

Reciprocamente...

Suponha-se, agora, que essas condições são satisfeitas. Então, pelo teorema de Legendre sobre somas de três quadrados, existem $A, B, C \in \mathbb{Z}$ tais que $m\,\mathrm{N}(\zeta) - n^4 = A^2 + B^2 + C^2$.

Reciprocamente...

Suponha-se, agora, que essas condições são satisfeitas. Então, pelo teorema de Legendre sobre somas de três quadrados, existem $A, B, C \in \mathbb{Z}$ tais que $m\ \mathrm{N}(\zeta) - n^4 = A^2 + B^2 + C^2$.

Pondo $\delta = n^2 + Ai + Bj + Ck$, tem-se $\mathrm{N}(\delta) = m\ \mathrm{N}(\zeta)$. Pela existência de fatorizações modeladas em fatorizações da norma, existem $\xi, \gamma \in \mathcal{L}$ tal que $\delta = \bar{\gamma}\xi$ e $\mathrm{N}(\xi) = \mathrm{N}(\zeta)$, $\mathrm{N}(\gamma) = m$.

Reciprocamente...

Suponha-se, agora, que essas condições são satisfeitas. Então, pelo teorema de Legendre sobre somas de três quadrados, existem $A, B, C \in \mathbb{Z}$ tais que $m\ \mathrm{N}(\zeta) - n^4 = A^2 + B^2 + C^2$.

Pondo $\delta = n^2 + Ai + Bj + Ck$, tem-se $\mathrm{N}(\delta) = m\ \mathrm{N}(\zeta)$. Pela existência de fatorizações modeladas em fatorizações da norma, existem $\xi, \gamma \in \mathcal{L}$ tal que $\delta = \bar{\gamma}\xi$ e $\mathrm{N}(\xi) = \mathrm{N}(\zeta)$, $\mathrm{N}(\gamma) = m$. Resulta que γ é uma solução de

$$\begin{aligned} \mathrm{N}(\gamma) &= m \\ \gamma \cdot \xi = \Re(\bar{\gamma}\xi) &= n^2. \end{aligned}$$

Reciprocamente...

Suponha-se, agora, que essas condições são satisfeitas. Então, pelo teorema de Legendre sobre somas de três quadrados, existem $A, B, C \in \mathbb{Z}$ tais que $m\ \mathrm{N}(\zeta) - n^4 = A^2 + B^2 + C^2$.

Pondo $\delta = n^2 + Ai + Bj + Ck$, tem-se $\mathrm{N}(\delta) = m\ \mathrm{N}(\zeta)$. Pela existência de fatorizações modeladas em fatorizações da norma, existem $\xi, \gamma \in \mathcal{L}$ tal que $\delta = \bar{\gamma}\xi$ e $\mathrm{N}(\xi) = \mathrm{N}(\zeta)$, $\mathrm{N}(\gamma) = m$. Resulta que γ é uma solução de

$$\begin{aligned} \mathrm{N}(\gamma) &= m \\ \gamma \cdot \xi = \Re(\bar{\gamma}\xi) &= n^2. \end{aligned}$$

Isto mostra o seguinte:

Um resultado genérico

Proposição (A.M., N. Tsopanidis, 2019)

Sejam $m, n, \ell \in \mathbb{N}$ tais que $n \leq \sqrt[4]{m\ell}$ e assuma-se que $m\ell - n^4$ não é da forma $4^r(8s+7)$ $(r, s \in \mathbb{N}_0)$. Então, para alguns $a, b, c, d \in \mathbb{N}_0$ tais que $\mathrm{N}(a + bi + cj + dk) = \ell$, o sistema

$$\begin{cases} m &= x^2 + y^2 + z^2 + t^2 \\ n^2 &= ax + by + cz + dt \end{cases}$$

tem soluções inteiras.

Um resultado genérico

Proposição (A.M., N. Tsopanidis, 2019)

Sejam $m, n, \ell \in \mathbb{N}$ tais que $n \leq \sqrt[4]{m\ell}$ e assuma-se que $m\ell - n^4$ não é da forma $4^r(8s+7)$ $(r, s \in \mathbb{N}_0)$. Então, para alguns $a, b, c, d \in \mathbb{N}_0$ tais que $\mathrm{N}(a + bi + cj + dk) = \ell$, o sistema

$$\begin{cases} m &= x^2 + y^2 + z^2 + t^2 \\ n^2 &= ax + by + cz + dt \end{cases}$$

tem soluções inteiras.

Resulta imediatamente, por um teorema de D. H. Lehmer (1948), que há soluções inteiras para todos $a, b, c, d \in \mathbb{Z}$ tais que

$$a^2 + b^2 + c^2 + d^2 = 1, 3, 5, 7, 11, 15, 23,$$
$$2^t, 3 \cdot 2^t, 7 \cdot 2^t, \text{ onde } t \in \mathbb{N} \text{ é ímpar.}$$

O caso 1-3-5

$\mathrm{N}(1+3i+5j)=35$, e há, a menos de ordem e sinais, apenas dois quaterniões de norma 35:

$$\alpha = 1+3i+5j \quad ; \quad \beta = 1+3i+3j+4k.$$

O caso 1-3-5

$\mathrm{N}(1+3i+5j)=35$, e há, a menos de ordem e sinais, apenas dois quaterniões de norma 35:

$$\alpha = 1+3i+5j \quad ; \quad \beta = 1+3i+3j+4k.$$

Portanto, se $n \leq \sqrt[4]{m\ell}$ e $m\ell - n^4 \notin \{4^r(8s+7) : r, s \in \mathbb{N}_0\}$, então pelo menos um dos sistemas

$$\begin{cases} m &= x^2+y^2+z^2+t^2 \\ n^2 &= x+3y+5z \end{cases} \tag{1-3-5}$$

$$\begin{cases} m &= x^2+y^2+z^2+t^2 \\ n^2 &= x+3y+3z+4t \end{cases} \tag{1-3-3-4}$$

tem uma solução inteira.

Esboço

Para $\xi, \zeta \in \mathcal{L}$, escreva-se $\xi \sim \zeta$ quando ξ e ζ têm as mesmas coordenadas a menos de ordem e sinais.

Esboço

Para $\xi, \zeta \in \mathcal{L}$, escreva-se $\xi \sim \zeta$ quando ξ e ζ têm as mesmas coordenadas a menos de ordem e sinais.

Como observado atrás, se $m, n \in \mathbb{N}$ são tais que

$$0 \leq 35m - n^4 \notin \{4^r(8s+7) : r, s \in \mathbb{N}_0\},$$

então existem $A, B, C \in \mathbb{N}_0$ tais que $35m - n^4 = A^2 + B^2 + C^2$.

Esboço

Para $\xi, \zeta \in \mathcal{L}$, escreva-se $\xi \sim \zeta$ quando ξ e ζ têm as mesmas coordenadas a menos de ordem e sinais.

Como observado atrás, se $m, n \in \mathbb{N}$ são tais que

$$0 \leq 35m - n^4 \notin \{4^r(8s+7) : r, s \in \mathbb{N}_0\},$$

então existem $A, B, C \in \mathbb{N}_0$ tais que $35m - n^4 = A^2 + B^2 + C^2$.

Pondo $\delta = n^2 + Ai + Bj + Ck$, tem-se $\mathrm{N}(\delta) = 35m$, e portanto existem $\xi, \gamma \in \mathcal{L}$ com $\mathrm{N}(\xi) = 35$, $\mathrm{N}(\gamma) = m$, tais que $\delta = \bar{\gamma}\xi$.

Esboço

Para $\xi, \zeta \in \mathcal{L}$, escreva-se $\xi \sim \zeta$ quando ξ e ζ têm as mesmas coordenadas a menos de ordem e sinais.

Como observado atrás, se $m, n \in \mathbb{N}$ são tais que

$$0 \leq 35m - n^4 \notin \{4^r(8s+7) : r, s \in \mathbb{N}_0\},$$

então existem $A, B, C \in \mathbb{N}_0$ tais que $35m - n^4 = A^2 + B^2 + C^2$.

Pondo $\delta = n^2 + Ai + Bj + Ck$, tem-se $\mathrm{N}(\delta) = 35m$, e portanto existem $\xi, \gamma \in \mathcal{L}$ com $\mathrm{N}(\xi) = 35$, $\mathrm{N}(\gamma) = m$, tais que $\delta = \bar{\gamma}\xi$.

Tem-se: $\xi \sim \alpha$ ou $\xi \sim \beta$.

Esboço

Para $\xi, \zeta \in \mathcal{L}$, escreva-se $\xi \sim \zeta$ quando ξ e ζ têm as mesmas coordenadas a menos de ordem e sinais.

Como observado atrás, se $m, n \in \mathbb{N}$ são tais que

$$0 \leq 35m - n^4 \notin \{4^r(8s+7) : r, s \in \mathbb{N}_0\},$$

então existem $A, B, C \in \mathbb{N}_0$ tais que $35m - n^4 = A^2 + B^2 + C^2$.

Pondo $\delta = n^2 + Ai + Bj + Ck$, tem-se $\mathrm{N}(\delta) = 35m$, e portanto existem $\xi, \gamma \in \mathcal{L}$ com $\mathrm{N}(\xi) = 35$, $\mathrm{N}(\gamma) = m$, tais que $\delta = \bar{\gamma}\xi$.

Tem-se: $\xi \sim \alpha$ ou $\xi \sim \beta$.

Se $\xi \sim \alpha$, tem-se o que se quer. Se $\xi \sim \beta$, a ideia é usar uma solução do sistema 1-3-3-4 para obter uma solução do sistem 1-3-5, usando a observação seguinte.

Esboço

Observação: Sejam $\gamma, \delta \in \mathcal{L}$ tais que $\mathrm{N}(\gamma) = m$ e $\delta = \bar{\gamma}\beta$.
Como, para todos $\rho, \sigma \in \mathcal{L} \setminus \{0\}$, com $\mathrm{N}(\rho) = \mathrm{N}(\sigma)$, se tem:

$$\rho^{-1}\delta\rho = \rho^{-1}\bar{\gamma}\beta\rho = \left(\rho^{-1}\gamma\sigma\right)\,\left(\sigma^{-1}\beta\rho\right)$$

$$\Re(\rho^{-1}\delta\rho) = \Re(\delta) \quad , \quad \mathrm{N}(\rho^{-1}\gamma\sigma) = \mathrm{N}(\gamma).$$

vê-se que, se conseguirmos encontrar $\rho, \sigma \in \mathcal{L} \setminus \{0\}$ tais que $\sigma^{-1}\beta\rho = \alpha'$ e $\rho^{-1}\gamma\sigma \in \mathcal{L}$, com $\alpha' \sim \alpha$ e $\mathrm{N}(\rho) = \mathrm{N}(\sigma)$, então, de uma solução γ do sistema 1-3-3-4 podemos obter uma do sistema 1-3-5.

O Teorema 1-3-5

Usando os primos de norma 3, 5 e 7, e reusando adequadamente soluções do sistema 1-3-3-4, obteve-se o resultado seguinte.

O Teorema 1-3-5

Usando os primos de norma 3, 5 e 7, e reusando adequadamente soluções do sistema 1-3-3-4, obteve-se o resultado seguinte.

Teorema (A.M., N. Tsopanidis, 2019)

Sejam $m, n \in \mathbb{N}$ tais que $0 < 35m - n^4 \notin \{4^r(8s+7) : r, s \in \mathbb{N}_0\}$. Então,

- se $m \equiv 0 \pmod 3$, o sistema 1-3-5 tem soluções inteiras sempre que $(n, 15) = 1$;
- se $m \equiv 1 \pmod 3$, o sistema 1-3-5 tem soluções inteiras sempre que $n \equiv 0 \pmod 3$ e $n \not\equiv 0 \pmod 5$;
- se $m \equiv -1 \pmod 3$, o sistema 1-3-5 tem soluções inteiras sempre que $(n, 105) = 1$.

Questões

- Encontrar uma abordagem mais conceptual para a parte da demonstração da conjetura 1-3-5 que usa os primos de norma 3, 5 e 7, de modo a tentar entender porque tudo encaixa bem

Questões

- Encontrar uma abordagem mais conceptual para a parte da demonstração da conjetura 1-3-5 que usa os primos de norma 3, 5 e 7, de modo a tentar entender porque tudo encaixa bem — deve haver algo subjacente a isto! —,

Questões

- Encontrar uma abordagem mais conceptual para a parte da demonstração da conjetura 1-3-5 que usa os primos de norma 3, 5 e 7, de modo a tentar entender porque tudo encaixa bem — deve haver algo subjacente a isto! —, de modo a ser possível atacar questões semelhantes.

Questões

- Encontrar uma abordagem mais conceptual para a parte da demonstração da conjetura 1-3-5 que usa os primos de norma 3, 5 e 7, de modo a tentar entender porque tudo encaixa bem — deve haver algo subjacente a isto! —, de modo a ser possível atacar questões semelhantes.
- A "conjetura 24" de Z.-W. Sun: Todo $m \in \mathbb{N}$ pode ser escrito como soma de quatro quadrados, $m = x^2 + y^2 + z^2 + t^2$ com $x, y, z, t \in \mathbb{N}_0$, de tal modo que tanto x como $x + 24y$ são quadrados perfeitos.

Questões

- Encontrar uma abordagem mais conceptual para a parte da demonstração da conjetura 1-3-5 que usa os primos de norma 3, 5 e 7, de modo a tentar entender porque tudo encaixa bem — deve haver algo subjacente a isto! —, de modo a ser possível atacar questões semelhantes.
- A "conjetura 24" de Z.-W. Sun: Todo $m \in \mathbb{N}$ pode ser escrito como soma de quatro quadrados, $m = x^2 + y^2 + z^2 + t^2$ com $x, y, z, t \in \mathbb{N}_0$, de tal modo que tanto x como $x + 24y$ são quadrados perfeitos.
  N.B.: $\mathrm{N}(1 + 24i) = 577$, e existem, a menos de ordem e sinais, 21 quaterniões inteiros de norma 577.

A questão

Pergunta (algures em 2004...)

Há um algoritmo eficiente de decompor um número como soma de quatro quadrados?

A questão

Pergunta (algures em 2004...)

Há um algoritmo eficiente de decompor um número como soma de quatro quadrados?

Analogia... $n = a^2 + b^2 = c^2 + d^2 \quad \rightsquigarrow \quad$ fatorização de n

A questão

Pergunta (algures em 2004...)

Há um algoritmo eficiente de decompor um número como soma de quatro quadrados?

Analogia... $n = a^2 + b^2 = c^2 + d^2 \quad \rightsquigarrow \quad$ fatorização de n

Exemplo

De:

$$\begin{aligned} 221 &= 11^2 + 10^2 = (11 + 10i)(11 - 10i) \\ &= 14^2 + 5^2 = (14 + 5i)(14 - 5i), \end{aligned}$$

A questão

Pergunta (algures em 2004...)

Há um algoritmo eficiente de decompor um número como soma de quatro quadrados?

Analogia... $n = a^2 + b^2 = c^2 + d^2 \quad \rightsquigarrow \quad$ fatorização de n

Exemplo

De:
$$\begin{aligned} 221 &= 11^2 + 10^2 = (11 + 10i)(11 - 10i) \\ &= 14^2 + 5^2 = (14 + 5i)(14 - 5i), \end{aligned}$$

usando o **algoritmo de Euclides** em $\mathbb{Z}[i]$, obtém-se

$$\gcd(14 + 5i, 11 + 10i) = 1 + 4i,$$

A questão

Pergunta (algures em 2004...)

Há um algoritmo eficiente de decompor um número como soma de quatro quadrados?

Analogia... $n = a^2 + b^2 = c^2 + d^2 \quad \rightsquigarrow \quad$ fatorização de n

Exemplo

De:
$$\begin{aligned} 221 &= 11^2 + 10^2 = (11 + 10i)(11 - 10i) \\ &= 14^2 + 5^2 = (14 + 5i)(14 - 5i), \end{aligned}$$

usando o **algoritmo de Euclides** em $\mathbb{Z}[i]$, obtém-se

$$\gcd(14 + 5i, 11 + 10i) = 1 + 4i,$$

de onde resulta que $17 \mid 221$.

Algoritmos

Legendre, 1825: para todo $m \in \mathbb{N}$ e para todo $\sqrt{m} < n < 2\sqrt{m}$ podem ser encontrados $x, y, z, t \in \mathbb{Z}$ tais que

$$\begin{aligned} m &= x^2 + y^2 + z^2 + t^2 \\ n &= x + y + z + t. \end{aligned}$$

Algoritmos

Legendre, 1825: para todo $m \in \mathbb{N}$ e para todo $\sqrt{m} < n < 2\sqrt{m}$ podem ser encontrados $x, y, z, t \in \mathbb{Z}$ tais que

$$\begin{aligned} m &= x^2 + y^2 + z^2 + t^2 \\ n &= x + y + z + t. \end{aligned}$$

Reduz a decompor um número na forma $x^2 + 3y^2$.

Algoritmos

Legendre, 1825: para todo $m \in \mathbb{N}$ e para todo $\sqrt{m} < n < 2\sqrt{m}$ podem ser encontrados $x, y, z, t \in \mathbb{Z}$ tais que

$$\begin{aligned} m &= x^2 + y^2 + z^2 + t^2 \\ n &= x + y + z + t. \end{aligned}$$

Reduz a decompor um número na forma $x^2 + 3y^2$.

Rabin & Shallit, 1986: Seja $n \in \mathbb{N}$ um número ímpar.

- Encontrar $a, b < \frac{n}{2}$ tais que $a^2 + b^2 \equiv -1 \pmod{n}$

Algoritmos

Legendre, 1825: para todo $m \in \mathbb{N}$ e para todo $\sqrt{m} < n < 2\sqrt{m}$ podem ser encontrados $x, y, z, t \in \mathbb{Z}$ tais que

$$\begin{aligned} m &= x^2 + y^2 + z^2 + t^2 \\ n &= x + y + z + t. \end{aligned}$$

Reduz a decompor um número na forma $x^2 + 3y^2$.

Rabin & Shallit, 1986: Seja $n \in \mathbb{N}$ um número ímpar.

- Encontrar $a, b < \frac{n}{2}$ tais que $a^2 + b^2 \equiv -1 \pmod{n}$

  (com probabilidade de sucesso de, pelo menos, 1 em $10 \log n$);
- Calcular $\gamma = gcd_R(a + bi + j, n)$

Algoritmos

Legendre, 1825: para todo $m \in \mathbb{N}$ e para todo $\sqrt{m} < n < 2\sqrt{m}$ podem ser encontrados $x, y, z, t \in \mathbb{Z}$ tais que

$$\begin{aligned} m &= x^2 + y^2 + z^2 + t^2 \\ n &= x + y + z + t. \end{aligned}$$

Reduz a decompor um número na forma $x^2 + 3y^2$.

Rabin & Shallit, 1986: Seja $n \in \mathbb{N}$ um número ímpar.

- Encontrar $a, b < \frac{n}{2}$ tais que $a^2 + b^2 \equiv -1 \pmod{n}$

  (com probabilidade de sucesso de, pelo menos, 1 em $10 \log n$);
- Calcular $\gamma = gcd_R(a + bi + j, n) : \mathrm{N}(\gamma) = kn$, com $k < n$, $k \mid n$.

Algoritmos

Legendre, 1825: para todo $m \in \mathbb{N}$ e para todo $\sqrt{m} < n < 2\sqrt{m}$ podem ser encontrados $x, y, z, t \in \mathbb{Z}$ tais que

$$\begin{aligned} m &= x^2 + y^2 + z^2 + t^2 \\ n &= x + y + z + t. \end{aligned}$$

Reduz a decompor um número na forma $x^2 + 3y^2$.

Rabin & Shallit, 1986: Seja $n \in \mathbb{N}$ um número ímpar.

- Encontrar $a, b < \frac{n}{2}$ tais que $a^2 + b^2 \equiv -1 \pmod{n}$

  (com probabilidade de sucesso de, pelo menos, 1 em $10 \log n$);
- Calcular $\gamma = gcd_R(a + bi + j, n) : \mathrm{N}(\gamma) = kn$, com $k < n$, $k \mid n$.
- Se $k > 1$, reiniciar algoritmo com $\frac{n}{k}$.

O problema

$$n = pq \quad ; \quad n = \mathrm{N}(\alpha) = \mathrm{N}(\beta), \text{ com } \alpha, \beta \text{ não-associados}$$

O problema

$$n = pq \quad ; \quad n = \mathrm{N}(\alpha) = \mathrm{N}(\beta), \text{ com } \alpha, \beta \text{ não-associados}$$

$$\downarrow$$

$$\begin{aligned} \alpha &= \pi\rho \\ \beta &= \tilde{\pi}\tilde{\rho} \end{aligned}$$

O problema

$$
\begin{array}{rcl}
n = pq & ; & n = \mathrm{N}(\alpha) = \mathrm{N}(\beta), \text{ com } \alpha, \beta \text{ não-associados} \\
 & \downarrow & \\
\alpha & = & \pi\rho \\
\beta & = & \tilde{\pi}\tilde{\rho}
\end{array}
$$

Em $\mathbb{Z}[i]$ tem-se necessariamente $\beta = \pi\bar{\rho}$ or $\beta = \bar{\pi}\rho$.

O problema

$$n = pq \quad ; \quad n = \mathrm{N}(\alpha) = \mathrm{N}(\beta), \text{ com } \alpha, \beta \text{ não-associados}$$

$$\downarrow$$

$$\begin{aligned} \alpha &= \pi\rho \\ \beta &= \tilde{\pi}\tilde{\rho} \end{aligned}$$

Em $\mathbb{Z}[i]$ tem-se necessariamente $\beta = \pi\bar{\rho}$ or $\beta = \bar{\pi}\rho$.

Tal não acontece em $\mathcal{H}$!

Exemplo

$247 = 13 \times 19 = \mathrm{N}(-7 + 9i + 6j + 9k) = \mathrm{N}(-11 + 9i - 3j + 6k)$ *e*

$-7 + 9i + 6j + 9k = (2 + 3i)(1 + 3i + 3j)$

$-11 + 9i - 3j + 6k = (1 + 2i + 2j + 2k)(1 + i + j + 4k)$

Unicidade de factores

Teorema (M. Lipschitz, 1886 + G. Pall, 1940)

Dado $\alpha \in \mathcal{L}$, primitivo, e $m \in \mathbb{Z}$ ímpar tal que

$$m \mid \mathrm{N}(\alpha),$$

existe um único divisor esquerdo (resp. direito) de α com norma m, a menos de associados direitos (resp. esquerdos).

Unicidade de factores

Teorema (M. Lipschitz, 1886 + G. Pall, 1940)

Dado $\alpha \in \mathcal{L}$, primitivo, e $m \in \mathbb{Z}$ ímpar tal que

$$m \mid \mathrm{N}(\alpha),$$

existe um único divisor esquerdo (resp. direito) de α com norma m, a menos de associados direitos (resp. esquerdos).

$$\alpha = \mu\beta = (\mu u)(u^{-1}\beta), \quad \mathrm{N}(\mu) = m$$

Unicidade de factores

Teorema (M. Lipschitz, 1886 + G. Pall, 1940)

Dado $\alpha \in \mathcal{L}$, primitivo, e $m \in \mathbb{Z}$ ímpar tal que

$$m \mid \mathrm{N}(\alpha),$$

existe um único divisor esquerdo (resp. direito) de α com norma m, a menos de associados direitos (resp. esquerdos).

$$\alpha = \mu\beta = (\mu u)(u^{-1}\beta), \quad \mathrm{N}(\mu) = m$$
$$\alpha = \gamma\nu = (\gamma u^{-1})(u\nu), \quad \mathrm{N}(\nu) = m$$

Unicidade de factores

Teorema (M. Lipschitz, 1886 + G. Pall, 1940)

Dado $\alpha \in \mathcal{L}$, primitivo, e $m \in \mathbb{Z}$ ímpar tal que

$$m \mid \mathrm{N}(\alpha),$$

existe um único divisor esquerdo (resp. direito) de α com norma m, a menos de associados direitos (resp. esquerdos).

$$\alpha = \mu\beta = (\mu u)(u^{-1}\beta), \quad \mathrm{N}(\mu) = m$$
$$\alpha = \gamma\nu = (\gamma u^{-1})(u\nu), \quad \mathrm{N}(\nu) = m$$

Exemplo

Se $\alpha = \pi_1\pi_2\pi_3 \hookleftarrow \mathrm{N}(\alpha) = p_1p_2p_3$; $\alpha = \tilde{\pi}_2\tilde{\pi}_1\tilde{\pi}_3 \hookleftarrow \mathrm{N}(\alpha) = p_2p_1p_3$, então $\pi_1\pi_2$, $\tilde{\pi}_2\tilde{\pi}_1$ são associados direitos e π_3, $\tilde{\pi}_3$ são associados esquerdos.

Um resultado de Gordon Pall

Teorema (G. Pall, 1940)

Seja $m \in \mathbb{N}$, $m > 1$ e ímpar, e sejam $\alpha, \beta \in \mathcal{L}$ primitivos módulo m, com $m \mid \mathrm{N}(\alpha) \ \wedge \ m \mid \mathrm{N}(\beta)$. Então existe uma fatorização $m = m_1 m_2$ tal que α e β têm os mesmos divisores esquerdos de norma m_1 e os mesmos divisores direitos de norma m_2 se e só se $m \mid \alpha \cdot \beta$.

Um resultado de Gordon Pall

Teorema (G. Pall, 1940)

Seja $m \in \mathbb{N}$, $m > 1$ e ímpar, e sejam $\alpha, \beta \in \mathcal{L}$ primitivos módulo m, com $m \mid \mathrm{N}(\alpha) \ \wedge \ m \mid \mathrm{N}(\beta)$. Então existe uma fatorização $m = m_1 m_2$ tal que α e β têm os mesmos divisores esquerdos de norma m_1 e os mesmos divisores direitos de norma m_2 se e só se $m \mid \alpha \cdot \beta$.

Em particular, se $m = \mathrm{N}(\alpha) = \mathrm{N}(\beta)$ e $\alpha \perp \beta$, então existe tal fatorização.

Uma observação simples

Sejam $p, q \in \mathbb{N}$ dois números primos ímpares, distintos e sejam $\pi, \rho \in \mathcal{L}$ tais que $\mathrm{N}(\pi) = p$ e $\mathrm{N}(\rho) = q$. Tem-se:

$$\pi i \rho \perp \pi \rho$$

(resulta de $2\,\alpha \cdot \beta = \Re(\alpha\bar{\beta}) = \alpha\bar{\beta} + \beta\bar{\alpha}$)

Uma observação simples

Sejam $p, q \in \mathbb{N}$ dois números primos ímpares, distintos e sejam $\pi, \rho \in \mathcal{L}$ tais que $\mathrm{N}(\pi) = p$ e $\mathrm{N}(\rho) = q$. Tem-se:

$$\pi i \rho \perp \pi \rho$$

(resulta de $2\,\alpha \cdot \beta = \Re(\alpha\bar{\beta}) = \alpha\bar{\beta} + \beta\bar{\alpha}$)

Proposição (A.M., L. Roçadas, 2012)

Seja $\gamma = \alpha + \beta j \in \mathcal{L}$, onde $\alpha, \beta \in \mathbb{Z}[i]$ e $\mathrm{N}(\gamma)$ é ímpar.

Tem-se: $(i\gamma, \gamma)_R = 1 \iff (\alpha, \beta) = 1 \quad (\text{in } \mathbb{Z}[i])$.

Uma observação simples

Sejam $p, q \in \mathbb{N}$ dois números primos ímpares, distintos e sejam $\pi, \rho \in \mathcal{L}$ tais que $\mathrm{N}(\pi) = p$ e $\mathrm{N}(\rho) = q$. Tem-se:

$$\pi i \rho \perp \pi \rho$$

(resulta de $2\,\alpha \cdot \beta = \Re(\alpha\bar{\beta}) = \alpha\bar{\beta} + \beta\bar{\alpha}$)

Proposição (A.M., L. Roçadas, 2012)

Seja $\gamma = \alpha + \beta j \in \mathcal{L}$, onde $\alpha, \beta \in \mathbb{Z}[i]$ e $\mathrm{N}(\gamma)$ é ímpar.

Tem-se: $(i\gamma, \gamma)_R = 1 \iff (\alpha, \beta) = 1 \quad (\text{in } \mathbb{Z}[i])$.

Em particular: $\gcd_L(\pi i \rho, \pi \rho) = \pi$, $\gcd_R(\pi i \rho, \pi \rho) = \rho$.

Uma observação simples

Reciprocamente:

$$\alpha = \pi\rho \quad \wedge \quad \beta \perp \alpha \quad \wedge \quad \mathrm{N}(\beta) = \mathrm{N}(\alpha) = pq$$

Uma observação simples

Reciprocamente:

$$\alpha = \pi\rho \quad \wedge \quad \beta \perp \alpha \quad \wedge \quad \mathrm{N}(\beta) = \mathrm{N}(\alpha) = pq$$

$$\Downarrow$$

$$\exists_{u \in \mathcal{L}^* \setminus \{\pm 1\}} : \quad \beta = \pi u \rho \quad \vee \quad \beta = u \pi \rho \quad \vee \quad \beta = \pi \rho u$$

Uma observação simples

Reciprocamente:

$$\alpha = \pi\rho \quad \wedge \quad \beta \perp \alpha \quad \wedge \quad \mathrm{N}(\beta) = \mathrm{N}(\alpha) = pq$$

$$\Downarrow$$

$$\exists_{u \in \mathcal{L}^* \setminus \{\pm 1\}} : \quad \beta = \pi u \rho \quad \vee \quad \beta = u \pi \rho \quad \vee \quad \beta = \pi \rho u$$

Como encontrar $\pi i \rho$ conhecendo $\pi\rho$?

O produto vetorial ternário em $\mathbb{H}$

Definição

Para $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{H}$, define-se

$$\alpha_1 \times \alpha_2 \times \alpha_3 = \begin{vmatrix} a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \\ a_3 & b_3 & c_3 & d_3 \\ 1 & i & j & k \end{vmatrix}$$

(com o significado óbvio), onde $\alpha_* = a_* + b_* i + c_* j + d_* k$.

O produto vetorial ternário em $\mathbb{H}$

Definição

Para $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{H}$, define-se

$$\alpha_1 \times \alpha_2 \times \alpha_3 = \begin{vmatrix} a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \\ a_3 & b_3 & c_3 & d_3 \\ 1 & i & j & k \end{vmatrix}$$

(com o significado óbvio), onde $\alpha_* = a_* + b_* i + c_* j + d_* k$.

Tem-se:

$$\beta \perp \alpha \ \wedge \ \gamma \perp \alpha \implies \mathrm{N}(\alpha) \mid \mathrm{N}(\alpha \times \beta \times \gamma)$$

Não é por aqui...

Teorema (A.M., L. Roçadas, 2012)

Dado $\alpha \in \mathcal{L}$, e $\beta, \gamma \in \mathcal{L}$ tais que $\beta \perp \alpha$ e $\gamma \perp \alpha$, tem-se:

$$\alpha \times \beta \times \gamma \in \alpha\mathcal{L} \cap \mathcal{L}\alpha.$$

Não é por aqui...

Teorema (A.M., L. Roçadas, 2012)

Dado $\alpha \in \mathcal{L}$, e $\beta, \gamma \in \mathcal{L}$ tais que $\beta \perp \alpha$ e $\gamma \perp \alpha$, tem-se:

$$\alpha \times \beta \times \gamma \in \alpha\mathcal{L} \cap \mathcal{L}\alpha.$$

Teorema (A.M., L. Roçadas, 2012)

Dados $\alpha, \beta, \gamma, \delta \in \mathcal{L}$, tem-se

$$\alpha\beta \times \alpha\gamma \times \delta \in \alpha\mathcal{L}.$$

Questões

- Como obter $\pi i \rho$ de $\pi \rho$?

Questões

- Como obter $\pi i \rho$ de $\pi \rho$?

  Ou, como limitar a região onde possa estar?

Questões

- Como obter $\pi i \rho$ de $\pi\rho$?

  Ou, como limitar a região onde possa estar?

- Para todos $\alpha, \beta, \gamma, \delta \in \mathcal{L}$, o quaternião $\alpha\beta \times \alpha\gamma \times \delta$ tem um divisor direito de norma $\mathrm{N}(\alpha)$. Que relação tem este divisor com α?

Questões

- Como obter $\pi i \rho$ de $\pi \rho$?

  Ou, como limitar a região onde possa estar?
- Para todos $\alpha, \beta, \gamma, \delta \in \mathcal{L}$, o quaternião $\alpha\beta \times \alpha\gamma \times \delta$ tem um divisor direito de norma $\mathrm{N}(\alpha)$. Que relação tem este divisor com α?
- Será possível usar a aritmética de quaterniões para construir um algoritmo de fatorização de inteiros?

Para saber mais...

- Rudolf Lipschitz, *Recherches sur la transformation, par des substitutions réelles, d'une somme de deux ou de trois carrés en elle-même*, Journal de Mathématiques Pures et Appliquées 4e série, **2** (1886), pp. 373–440.
- Adolf Hurwitz, *Vorlesungen Über Die Zahlentheorie der Quaternionen*, Julius Springer, 1919.
- Gordon Pall, *On the Arithmetic of Quaternions*, Trans. Am. Math. Soc. **47** (1940) pp. 487–500.
- A. Machiavelo and L. Roçadas, *Connections Between the Arithmetic and the Geometry of Lipschitz Integers*, preprint CMUP 2011-18, available at arXiv:1201.5817 (January 2012).
- Zhi-Wei Sun, *Refining Lagrange's Four-Square Theorem*, Journal of Number Theory **175** (2017) 167–190.
- A. Machiavelo, Nikolaos Tsopanidis, *Zhi-Wei Sun's 1-3-5 Conjecture and Variations*, Journal of Number Theory **222** (2021) 1–20.
- A. Machiavelo, Rogério Reis, Nikolaos Tsopanidis, *Report on Zhi-Wei Sun's "1-3-5 Conjecture" and Some of Its Refinements*, Journal of Number Theory **222** (2021) 21–29.