Passeios com primos de Euclides,
conexões de Galois e primos de Gauss

Jorge Picado

Departamento de Matemática

Universidade de Coimbra

Centre for Mathematics
University of Coimbra

J. Lambek e L. Moser (1954)

$f(n) = n$-ésimo primo

J. Lambek e L. Moser (1954)

$f(n) = n$-ésimo primo

n	$f(n)$
0	0
1	2
2	3
3	5
4	7
5	11
6	13
7	17
$\vdots$	$\vdots$

J. Lambek e L. Moser (1954)

$f(n) = n$-ésimo primo

$g(n) = \#\{\text{primos } \leq n\}$

n	$f(n)$	$g(n)$
0	0	0
1	2	0
2	3	1
3	5	2
4	7	2
5	11	3
6	13	3
7	17	4
$\vdots$	$\vdots$	$\vdots$

UMA OBSERVAÇÃO SOBRE PRIMOS

J. Lambek e L. Moser (1954)

$f(n) = n$-ésimo primo

$g(n) = \#\{\text{primos } \leq n\}$

n	$f(n)$	$f(n)+n$	$g(n)$
0	0	0	0
1	2	3	0
2	3	5	1
3	5	8	2
4	7	11	2
5	11	16	3
6	13	19	3
7	17	24	4
$\vdots$	$\vdots$	$\vdots$	$\vdots$

J. Lambek e L. Moser (1954)

$f(n) = n$-ésimo primo

$g(n) = \#\{\text{primos } \leq n\}$

n	$f(n)$	$f(n)+n$	$g(n)$	$g(n)+n+1$
0	0	0	0	1
1	2	3	0	2
2	3	5	1	4
3	5	8	2	6
4	7	11	2	7
5	11	16	3	9
6	13	19	3	10
7	17	24	4	12
⋮	⋮	⋮	⋮	⋮

J. Lambek e L. Moser (1954)

$f(n) = n$-ésimo quadrado perfeito

n	$f(n)$
0	0
1	0
2	1
3	4
4	9
5	16
6	25
$\vdots$	$\vdots$

MAIS EXEMPLOS

J. Lambek e L. Moser (1954)

$f(n) = n$-ésimo quadrado perfeito

$g(n) = \#\{\text{quad. perf.} \leq n\}$

n	$f(n)$	$g(n)$
0	0	1
1	0	2
2	1	2
3	4	2
4	9	3
5	16	3
6	25	3
$\vdots$	$\vdots$	$\vdots$

J. Lambek e L. Moser (1954)

$f(n) = n$-ésimo quadrado perfeito

$g(n) = \#\{\text{quad. perf. } \leq n\}$

n	$f(n)$	$f(n)+n$	$g(n)$
0	0	0	1
1	0	1	2
2	1	3	2
3	4	7	2
4	9	13	3
5	16	21	3
6	25	31	3
$\vdots$	$\vdots$	$\vdots$	$\vdots$

MAIS EXEMPLOS

J. Lambek e L. Moser (1954)

$f(n) = n$-ésimo quadrado perfeito

$g(n) = \#\{\text{quad. perf.} \leq n\}$

n	$f(n)$	$f(n)+n$	$g(n)$	$g(n)+n+1$
0	0	0	1	2
1	0	1	2	4
2	1	3	2	5
3	4	7	2	6
4	9	13	3	8
5	16	21	3	9
6	25	31	3	10
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

partição complementar de $\mathbb{N}$

MAIS EXEMPLOS

J. Lambek e L. Moser (1954)

$f(n) = n$-ésimo número par

$g(n) = \#\{\text{pares } \leq n\}$

MAIS EXEMPLOS

J. Lambek e L. Moser (1954)

$f(n) = n$-ésimo número par $\qquad g(n) = \#\{\text{pares } \leq n\}$

$f(n) = n$-ésimo número triangular $\qquad g(n) = \#\{\text{triangulares } \leq n\}$

MAIS EXEMPLOS

J. Lambek e L. Moser (1954)

$f(n) = n$-ésimo número par $\qquad g(n) = \#\{\text{pares } \leq n\}$

$f(n) = n$-ésimo número triangular $\qquad g(n) = \#\{\text{triangulares } \leq n\}$

$f(n) = n$-ésimo número P $\qquad g(n) = \#\{\text{núm. P } \leq n\}$

MAIS EXEMPLOS

J. Lambek e L. Moser (1954)

$f(n) = n$-ésimo número par $\qquad g(n) = \#\{\text{pares } \leq n\}$

$f(n) = n$-ésimo número triangular $\qquad g(n) = \#\{\text{triangulares } \leq n\}$

$f(n) = n$-ésimo número P $\qquad g(n) = \#\{\text{núm. P } \leq n\}$

$$\boxed{f(n) \leq m \iff n \leq g(m)}$$

MAIS EXEMPLOS

J. Lambek e L. Moser (1954)

$f(n) = n$-ésimo número par $\qquad g(n) = \#\{\text{pares } \leq n\}$

$f(n) = n$-ésimo número triangular $\qquad g(n) = \#\{\text{triangulares } \leq n\}$

$f(n) = n$-ésimo número P $\qquad g(n) = \#\{\text{núm. P } \leq n\}$

$$\boxed{f(n) \leq m \iff n \leq g(m)}$$

$$(\mathbb{N}, \leq) \underset{g}{\overset{f}{\rightleftarrows}} (\mathbb{N}, \leq)$$

CONEXÃO DE GALOIS

CONEXÕES DE GALOIS

$$(\mathbb{N}, \leq) \underset{g}{\overset{f}{\rightleftarrows}} (\mathbb{N}, \leq)$$

$$\boxed{f(n) \leq m \iff n \leq g(m)}$$

CONEXÕES DE GALOIS

$$\begin{tikzcd}(\mathbb{N}, \leq) \arrow[r, shift left, "f"] & (\mathbb{N}, \leq) \arrow[l, shift left, "g"]\end{tikzcd}$$

$$\boxed{f(n) \leq m \iff n \leq g(m)}$$

$$f \dashv g$$

CONEXÕES DE GALOIS

$$(\mathbb{N}, \leq) \underset{g}{\overset{f}{\rightleftarrows}} (\mathbb{N}, \leq) \qquad \boxed{f(n) \leq m \iff n \leq g(m)}$$

$$f \dashv g$$

PROPRIEDADES:

(1) $fg \leq \mathrm{id}$ e $\mathrm{id} \leq gf$. (“quase-inversas”)

CONEXÕES DE GALOIS

$$(\mathbb{N}, \leq) \underset{g}{\overset{f}{\rightleftarrows}} (\mathbb{N}, \leq)$$

$$\boxed{f(n) \leq m \iff n \leq g(m)}$$

$$f \dashv g$$

PROPRIEDADES:

(1) $fg \leq \mathrm{id}$ e $\mathrm{id} \leq gf$. ("quase-inversas")

(2) f e g são monótonas. ($f \dashv g \iff (1) + (2)$)

CONEXÕES DE GALOIS

$$(\mathbb{N}, \leq) \underset{g}{\overset{f}{\rightleftarrows}} (\mathbb{N}, \leq) \qquad \boxed{f(n) \leq m \iff n \leq g(m)}$$

$$f \dashv g$$

PROPRIEDADES:

(1) $fg \leq \mathrm{id}$ e $\mathrm{id} \leq gf$. (“quase-inversas”)

(2) f e g são monótonas. ($f \dashv g \iff (1) + (2)$)

(3) $fgf = f$ e $gfg = g$.

CONEXÕES DE GALOIS

$$(\mathbb{N}, \leq) \underset{g}{\overset{f}{\rightleftarrows}} (\mathbb{N}, \leq) \qquad \boxed{f(n) \leq m \iff n \leq g(m)}$$

$$f \dashv g$$

PROPRIEDADES:

(1) $fg \leq \mathrm{id}$ e $\mathrm{id} \leq gf$. ("quase-inversas")

(2) f e g são monótonas. ($f \dashv g \iff (1) + (2)$)

(3) $fgf = f$ e $gfg = g$.

(4) $g(m) = \max\{n \in \mathbb{N} \mid f(n) \leq m\}$ (g é determinado por f)

$f(n) = \min\{m \in \mathbb{N} \mid n \leq g(m)\}$ (f é determinado por g)

PROPOSIÇÃO RECÍPROCA

Sejam

$$F = \{F(n) \mid n \in \mathbb{N}\} \quad \text{e} \quad G = \{G(n) \mid n \in \mathbb{N}\}$$

sucessões complementares (estrit. crescentes) de $\mathbb{N}$ com $0 \in F$.

PROPOSIÇÃO RECÍPROCA

Sejam

$$F = \{F(n) \mid n \in \mathbb{N}\} \quad \text{e} \quad G = \{G(n) \mid n \in \mathbb{N}\}$$

sucessões complementares (estrit. crescentes) de $\mathbb{N}$ com $0 \in F$.

As funções

$$(\mathbb{N}, \leq) \underset{g}{\overset{f}{\rightleftarrows}} (\mathbb{N}, \leq)$$

PROPOSIÇÃO RECÍPROCA

Sejam

$$F = \{F(n) \mid n \in \mathbb{N}\} \quad \text{e} \quad G = \{G(n) \mid n \in \mathbb{N}\}$$

sucessões complementares (estrit. crescentes) de $\mathbb{N}$ com $0 \in F$.

As funções

$$\begin{tikzcd} (\mathbb{N}, \leq) \arrow[r, shift left, "f"] & (\mathbb{N}, \leq) \arrow[l, shift left, "g"] \end{tikzcd}$$

definidas por

$$f(n) = F(n) - n \quad \text{e} \quad g(n) = G(n) - n - 1$$

PROPOSIÇÃO RECÍPROCA

Sejam

$$F = \{F(n) \mid n \in \mathbb{N}\} \quad \text{e} \quad G = \{G(n) \mid n \in \mathbb{N}\}$$

sucessões complementares (estrit. crescentes) de $\mathbb{N}$ com $0 \in F$.

As funções

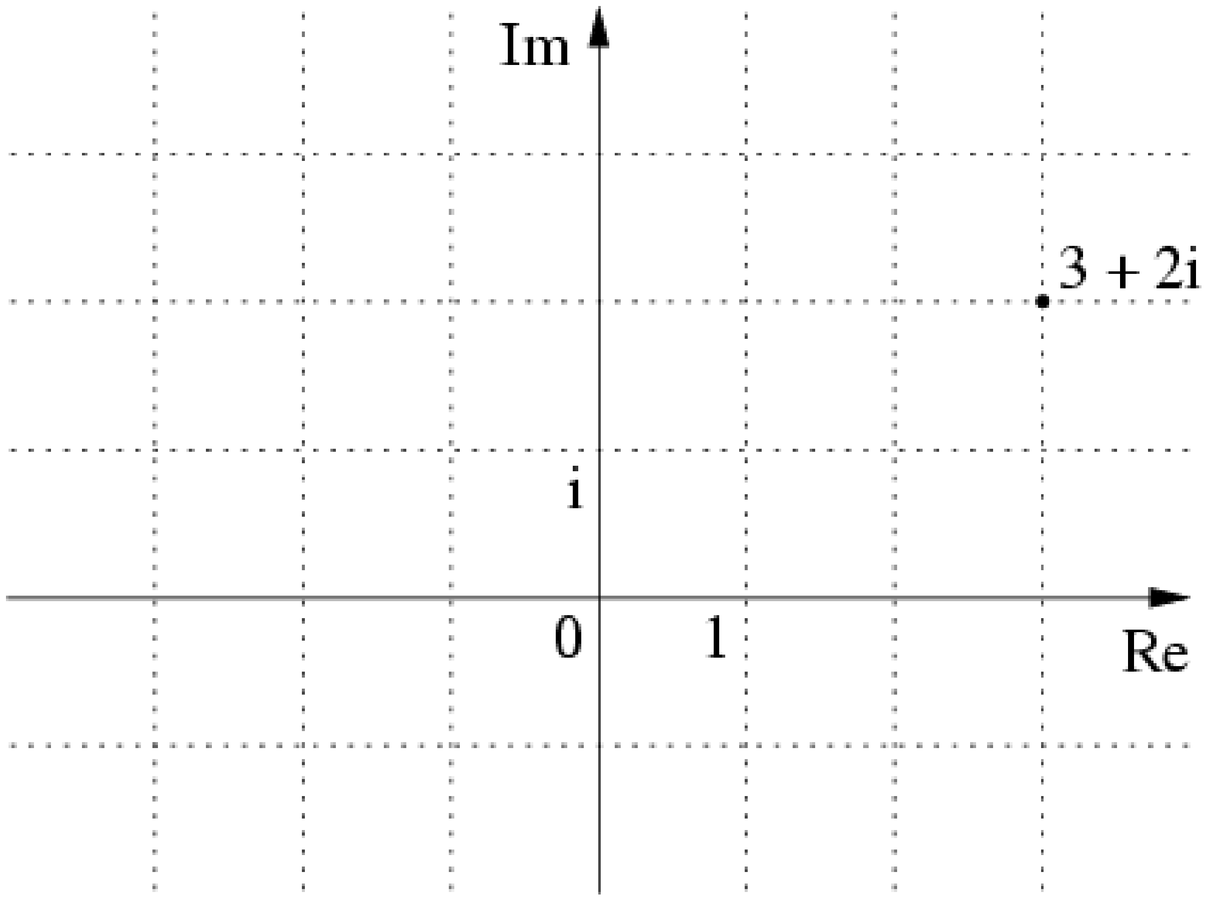
$$(\mathbb{N}, \leq) \underset{g}{\overset{f}{\rightleftarrows}} (\mathbb{N}, \leq)$$

definidas por

$$f(n) = F(n) - n \quad \text{e} \quad g(n) = G(n) - n - 1$$

formam uma conexão de Galois $f \dashv g$.

INTEIROS DE GAUSS



PRIMOS DE GAUSS

Inteiros < 100, primos de Euclides, que também são primos de Gauss:

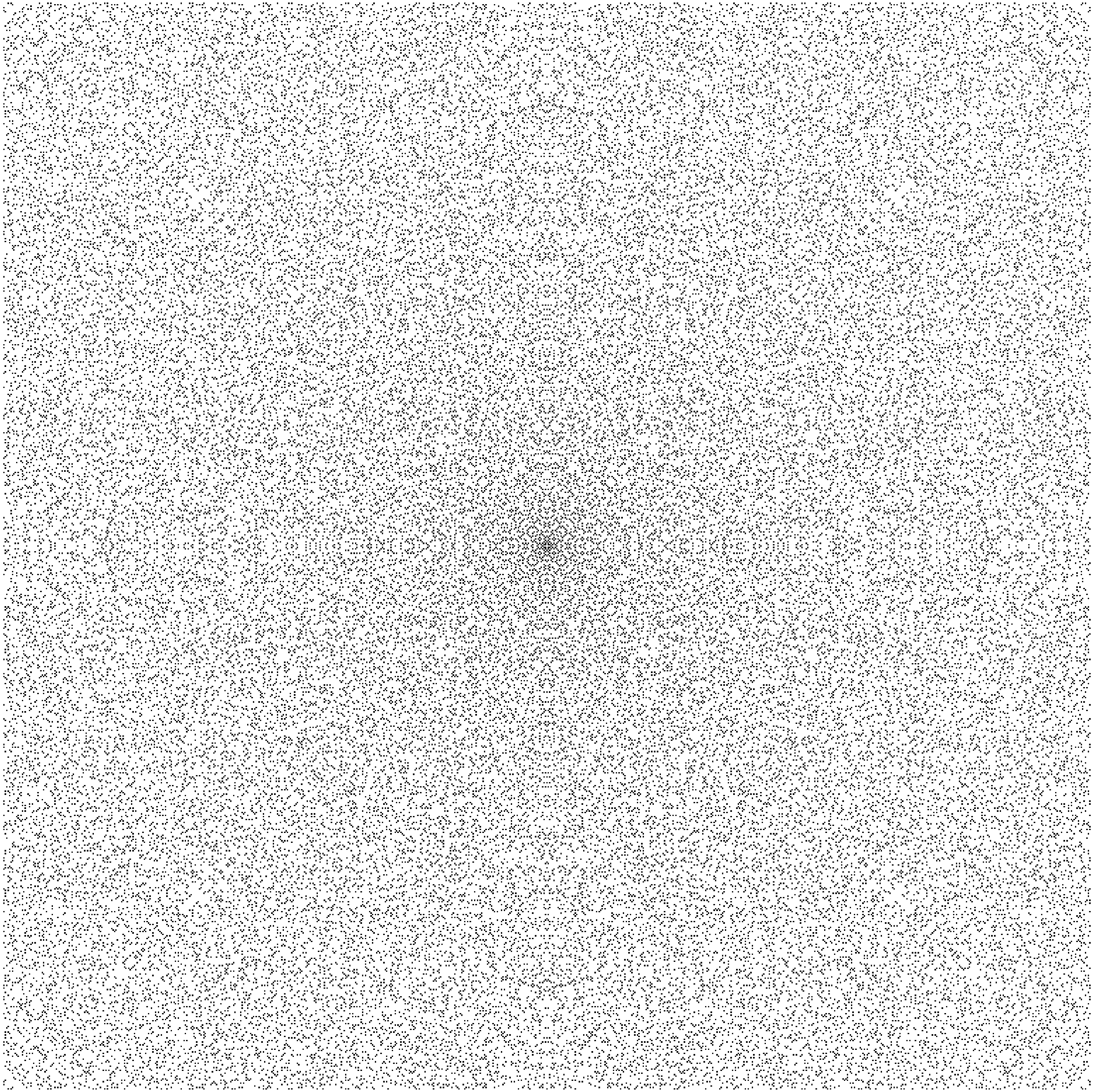
3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 83

Inteiros < 100, primos de Euclides, que também são primos de Gauss:

3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 83

$\boxed{\text{Um primo } p \text{ de Euclides é primo de Gauss se e só se } p \equiv 3 \pmod 4}$

PRIMOS DE GAUSS



PROBLEMA DO FOSSO

Será possível caminhar para o infinito,
saltando de primo em primo,
com passos de comprimento c limitado?

PROBLEMA DO FOSSO

Será possível caminhar para o infinito,
saltando de primo em primo,
com passos de comprimento c limitado?

Em $\mathbb{Z}$: NÃO!

PROBLEMA DO FOSSO

Será possível caminhar para o infinito,
saltando de primo em primo,
com passos de comprimento **c** limitado?

Em $\mathbb{Z}$: NÃO!

$$n!+2 \quad n!+3 \quad n!+4 \quad \ldots \quad n!+(n-1) \quad n!+n$$

PROBLEMA DO FOSSO

Será possível caminhar para o infinito,
saltando de primo em primo,
com passos de comprimento **c** limitado?

Em $\mathbb{Z}$: NÃO!

$$\underbrace{n!+2 \qquad n!+3 \qquad n!+4 \qquad \ldots \qquad n!+(n-1) \qquad n!+n}$$

fosso de comprimento $n-1$

PROBLEMA DO FOSSO GAUSSIANO

Basil Gordon (1962)

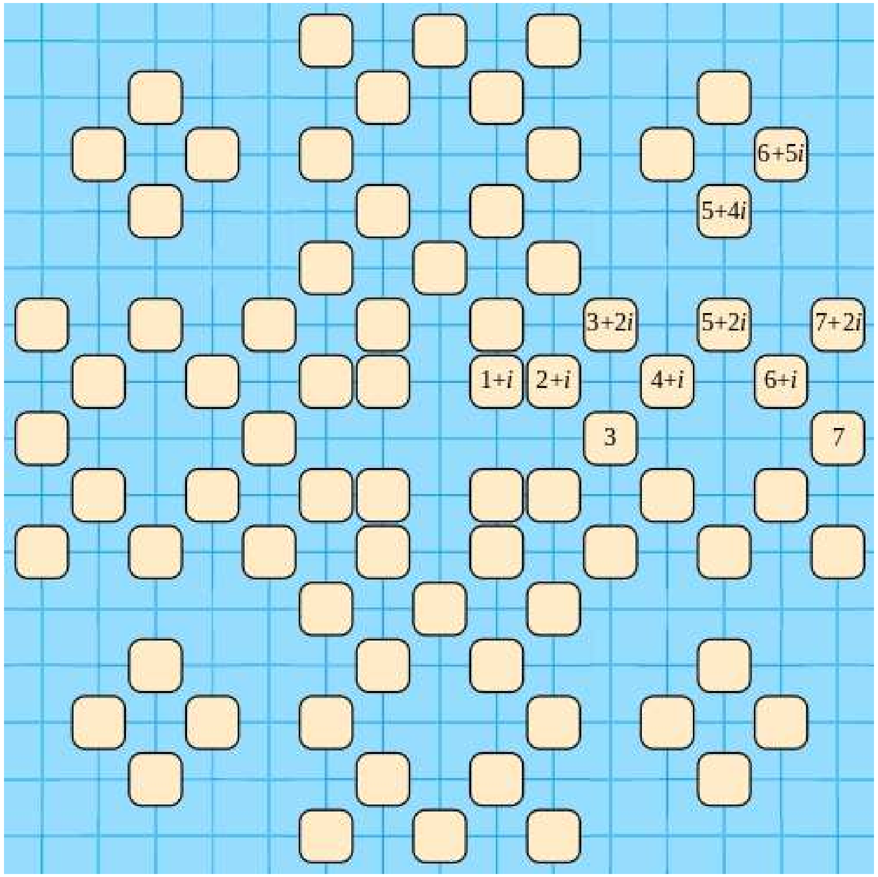
Será possível encontrar uma sequência infinita de primos de Gauss distintos tal que a diferença entre números consecutivos na sequência seja limitado?

PROBLEMA DO FOSSO GAUSSIANO

Basil Gordon (1962)

Será possível encontrar uma sequência infinita de primos de Gauss distintos tal que a diferença entre números consecutivos na sequência seja limitado?

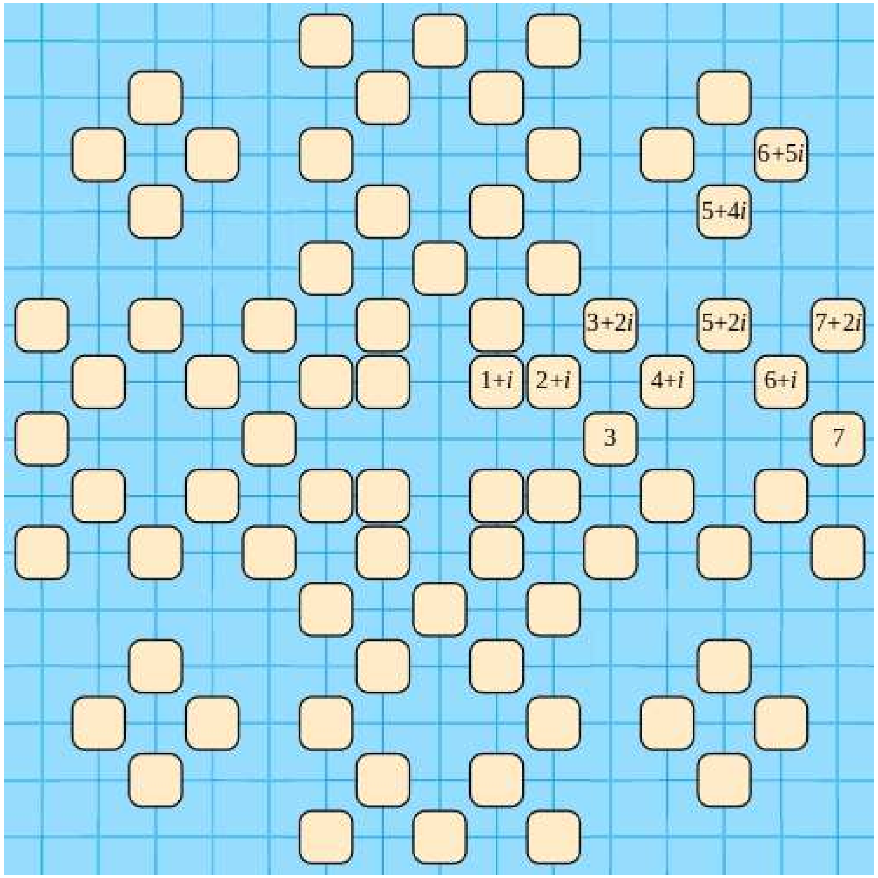
Imaginando os primos de Gauss pedras num lago de complexos:



PROBLEMA DO FOSSO GAUSSIANO

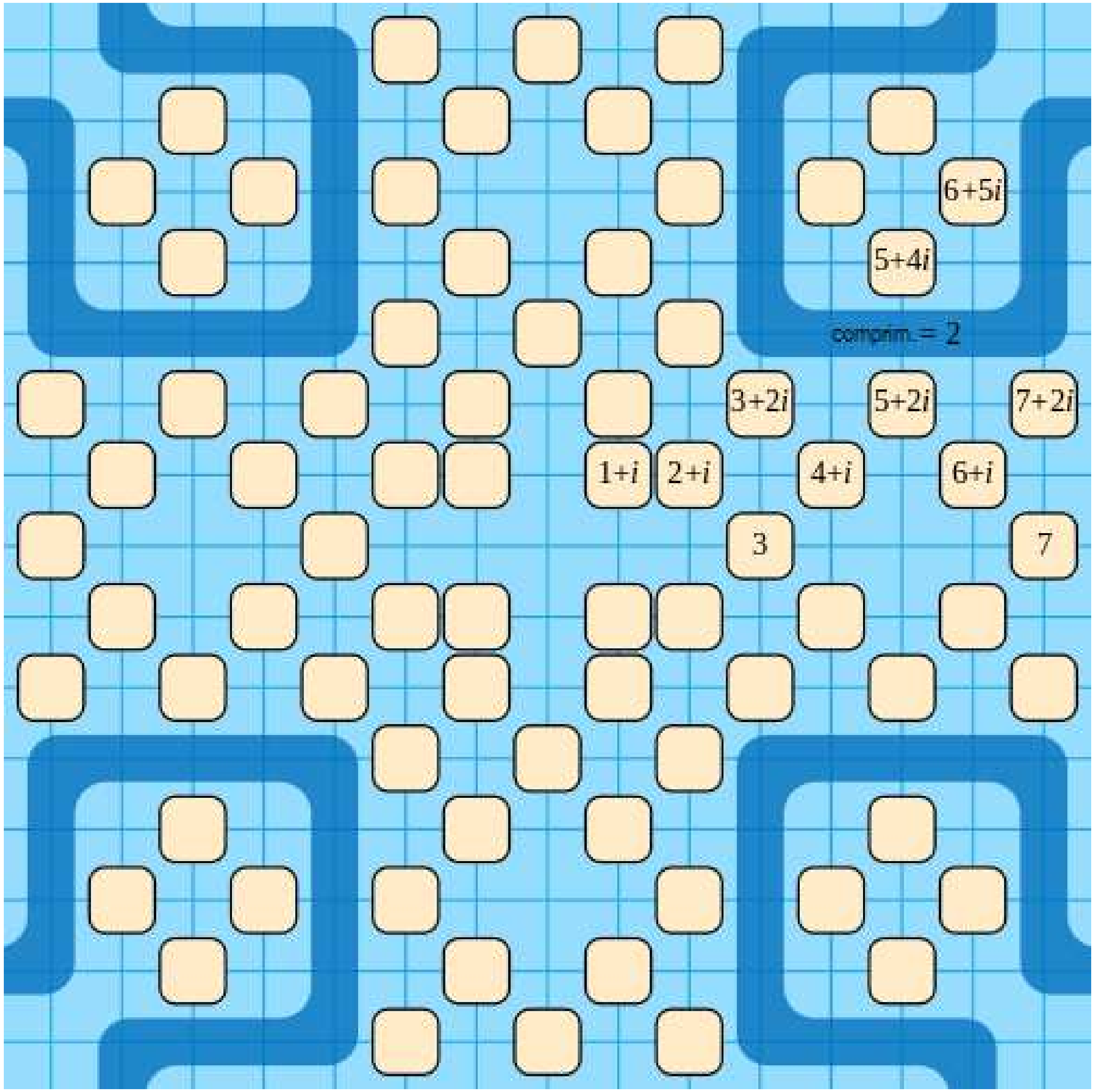
Basil Gordon (1962)

Será possível caminharmos (saltando de pedra em pedra) desde a origem até ao infinito com passos de comprimento limitado, sem nos molharmos?



PROBLEMA DO FOSSO GAUSSIANO

Basil Gordon (1962)



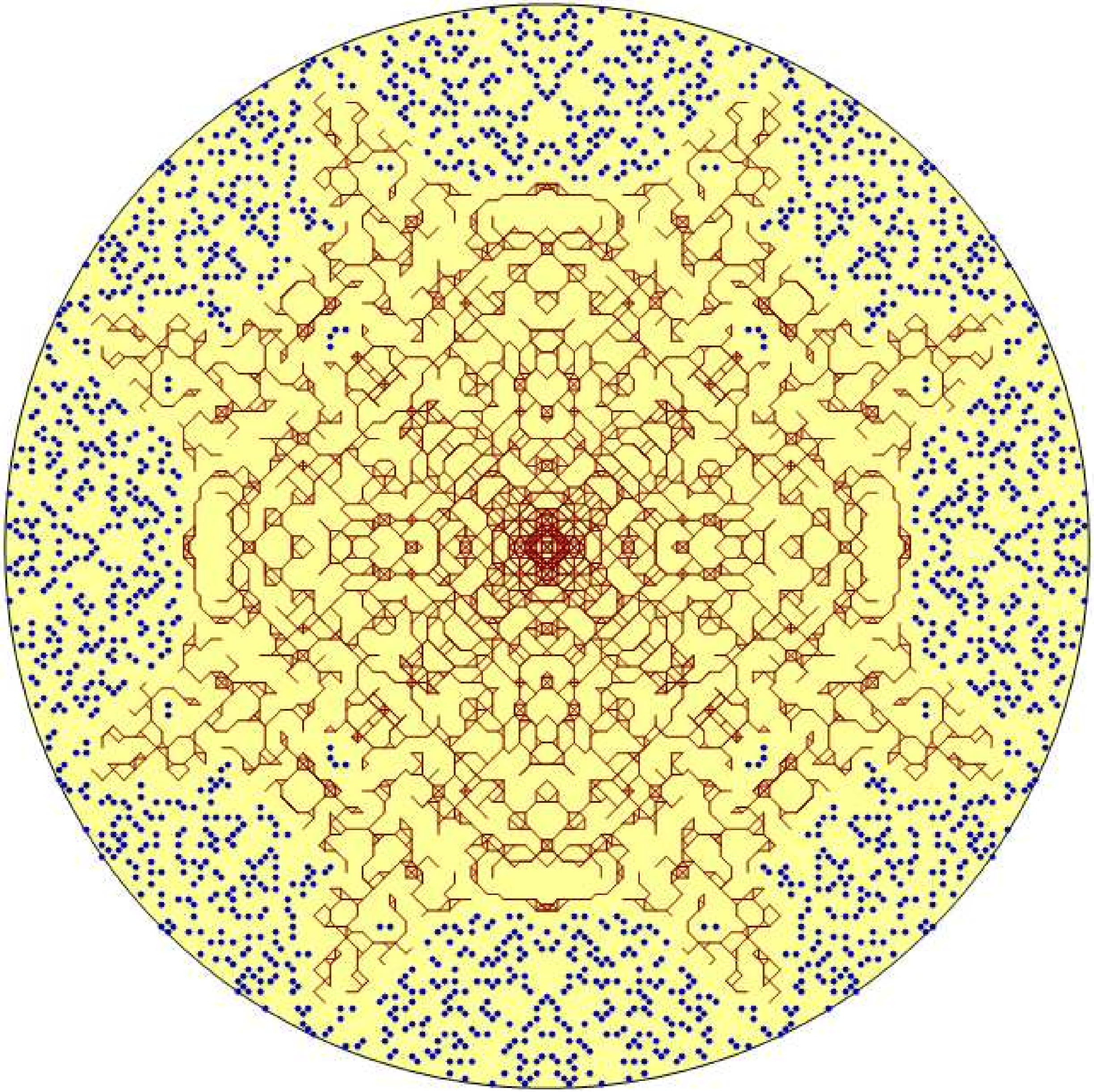
$$a \leq 7, b \leq 7$$

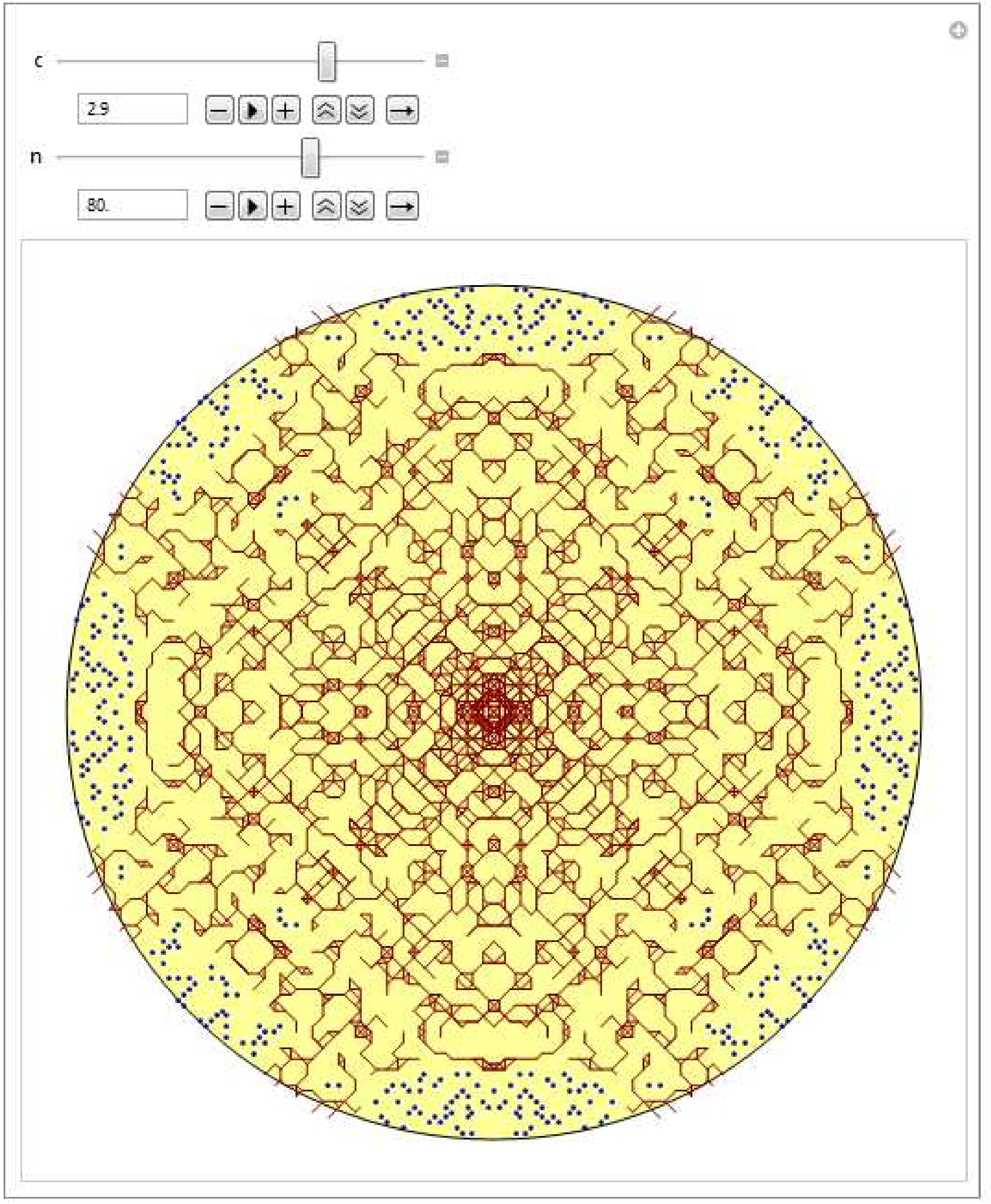
PROBLEMA DO FOSSO GAUSSIANO

primos alcançáveis

com $\mathrm{passo} = \sqrt{8}$

até $n = 100$





$$\text{passo} = 2.9$$

$$\text{distância} \leq 80$$

PROBLEMA DO FOSSO GAUSSIANO

O QUE SE SABE:

c	Distância máx.	Ponto mais longe
1	2.23	$2+i$

PROBLEMA DO FOSSO GAUSSIANO

O QUE SE SABE:

c	Distância máx.	Ponto mais longe
1	2.23	$2+i$
$\sqrt{2}$	11.70	$11+4i$

PROBLEMA DO FOSSO GAUSSIANO

O QUE SE SABE:

c	Distância máx.	Ponto mais longe
1	2.23	$2+i$
$\sqrt{2}$	11.70	$11+4i$
2	45.31	$42+17i$

PROBLEMA DO FOSSO GAUSSIANO

O QUE SE SABE:

c	Distância máx.	Ponto mais longe
1	2.23	$2+i$
$\sqrt{2}$	11.70	$11+4i$
2	45.31	$42+17i$
$\sqrt{8}$	93.47	$84+41i$

PROBLEMA DO FOSSO GAUSSIANO

O QUE SE SABE:

c	Distância máx.	Ponto mais longe
1	2.23	$2+i$
$\sqrt{2}$	11.70	$11+4i$
2	45.31	$42+17i$
$\sqrt{8}$	93.47	$84+41i$
$\sqrt{10}$	1024.35	$976+311i$

PROBLEMA DO FOSSO GAUSSIANO

O QUE SE SABE:

c	Distância máx.	Ponto mais longe
1	2.23	$2+i$
$\sqrt{2}$	11.70	$11+4i$
2	45.31	$42+17i$
$\sqrt{8}$	93.47	$84+41i$
$\sqrt{10}$	1024.35	$976+311i$
$\vdots$	$\vdots$	$\vdots$
$\sqrt{26}$	1015638.765	$943460+376039i$

PROBLEMA DO FOSSO GAUSSIANO

O QUE SE SABE:

c	Distância máx.	Ponto mais longe
1	2.23	$2+i$
$\sqrt{2}$	11.70	$11+4i$
2	45.31	$42+17i$
$\sqrt{8}$	93.47	$84+41i$
$\sqrt{10}$	1024.35	$976+311i$
$\vdots$	$\vdots$	$\vdots$
$\sqrt{26}$	1015638.765	$943460+376039i$
6	$\leq$ 80015782	??

[Tsuchimura, 2005]

PROBLEMA DO FOSSO GAUSSIANO

Quem? O infinito?
Diz-lhe que entre.
Faz bem ao infinito
estar entre gente.

— Alexandre O'Neill,
De Porta em Porta (1960)