Los secretos de los números primos

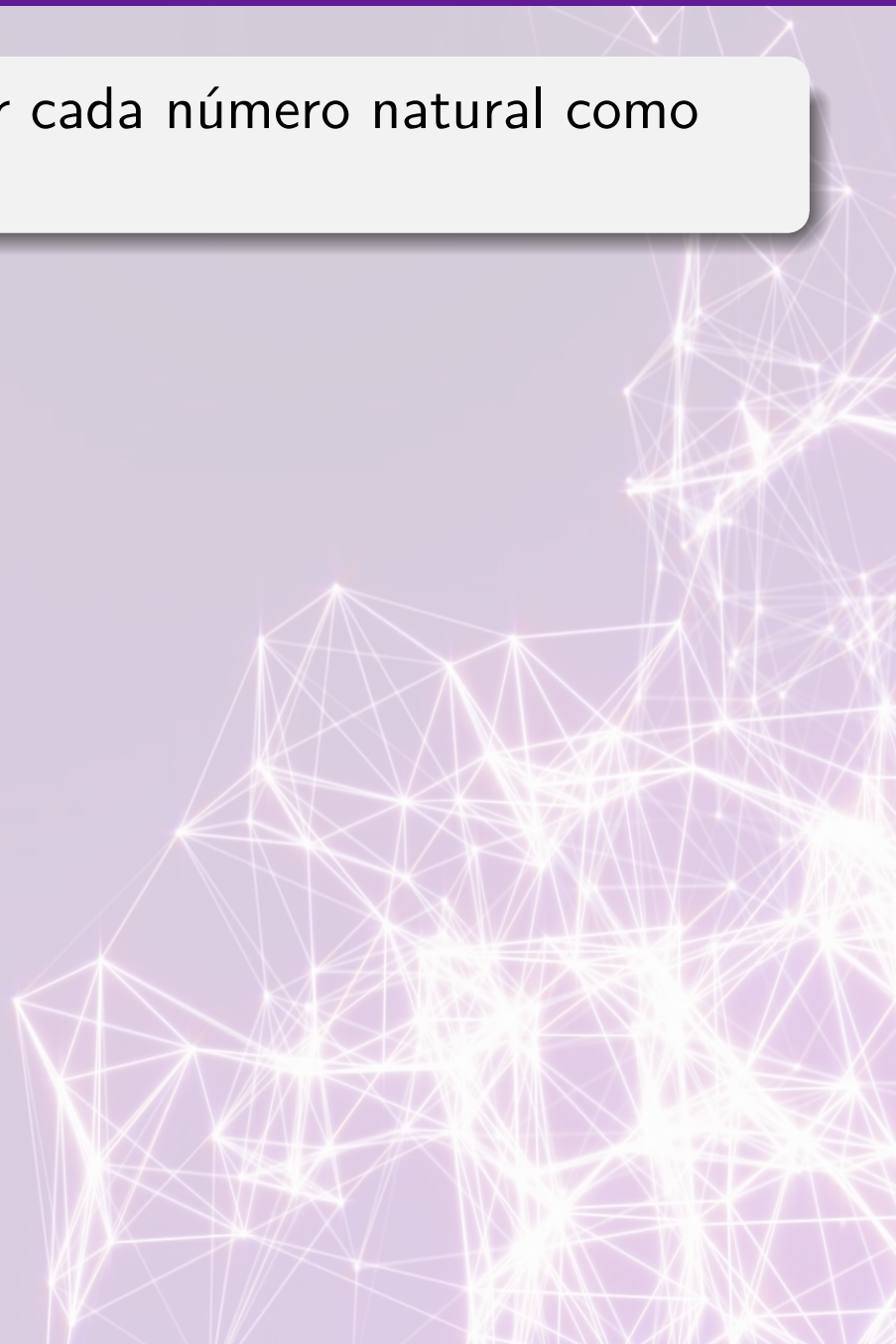
Marta Sánchez Pavón

STEM Talent Girl

21 de abril de 2023

Números primos

¿De cuántas maneras podemos expresar cada número natural como producto de otros números naturales?



Números primos

¿De cuántas maneras podemos expresar cada número natural como producto de otros números naturales?

- $2 = 1 \times 2$

Números primos

¿De cuántas maneras podemos expresar cada número natural como producto de otros números naturales?

- $2 = 1 \times 2$
- $3 = 1 \times 3$

Números primos

¿De cuántas maneras podemos expresar cada número natural como producto de otros números naturales?

- $2 = 1 \times 2$
- $3 = 1 \times 3$
- $4 = 1 \times 2 \times 2 = 1 \times 4$

Números primos

¿De cuántas maneras podemos expresar cada número natural como producto de otros números naturales?

- $2 = 1 \times 2$
- $3 = 1 \times 3$
- $4 = 1 \times 2 \times 2 = 1 \times 4$
- $5 = 1 \times 5$

Números primos

¿De cuántas maneras podemos expresar cada número natural como producto de otros números naturales?

- $2 = 1 \times 2$
- $3 = 1 \times 3$
- $4 = 1 \times 2 \times 2 = 1 \times 4$
- $5 = 1 \times 5$
- $6 = 1 \times 2 \times 3 = 1 \times 6$

Números primos

¿De cuántas maneras podemos expresar cada número natural como producto de otros números naturales?

- $2 = 1 \times 2$
- $3 = 1 \times 3$
- $4 = 1 \times 2 \times 2 = 1 \times 4$
- $5 = 1 \times 5$
- $6 = 1 \times 2 \times 3 = 1 \times 6$
- $7 = 1 \times 7$

Números primos

¿De cuántas maneras podemos expresar cada número natural como producto de otros números naturales?

- $2 = 1 \times 2$
- $3 = 1 \times 3$
- $4 = 1 \times 2 \times 2 = 1 \times 4$
- $5 = 1 \times 5$
- $6 = 1 \times 2 \times 3 = 1 \times 6$
- $7 = 1 \times 7$
- $8 = 1 \times 2 \times 4 = 1 \times 2 \times 2 \times 2 = 1 \times 8$

$\vdots$

Números primos

¿De cuántas maneras podemos expresar cada número natural como producto de otros números naturales?

- $2 = 1 \times 2$
- $3 = 1 \times 3$
- $4 = 1 \times 2 \times 2 = 1 \times 4$
- $5 = 1 \times 5$
- $6 = 1 \times 2 \times 3 = 1 \times 6$
- $7 = 1 \times 7$
- $8 = 1 \times 2 \times 4 = 1 \times 2 \times 2 \times 2 = 1 \times 8$

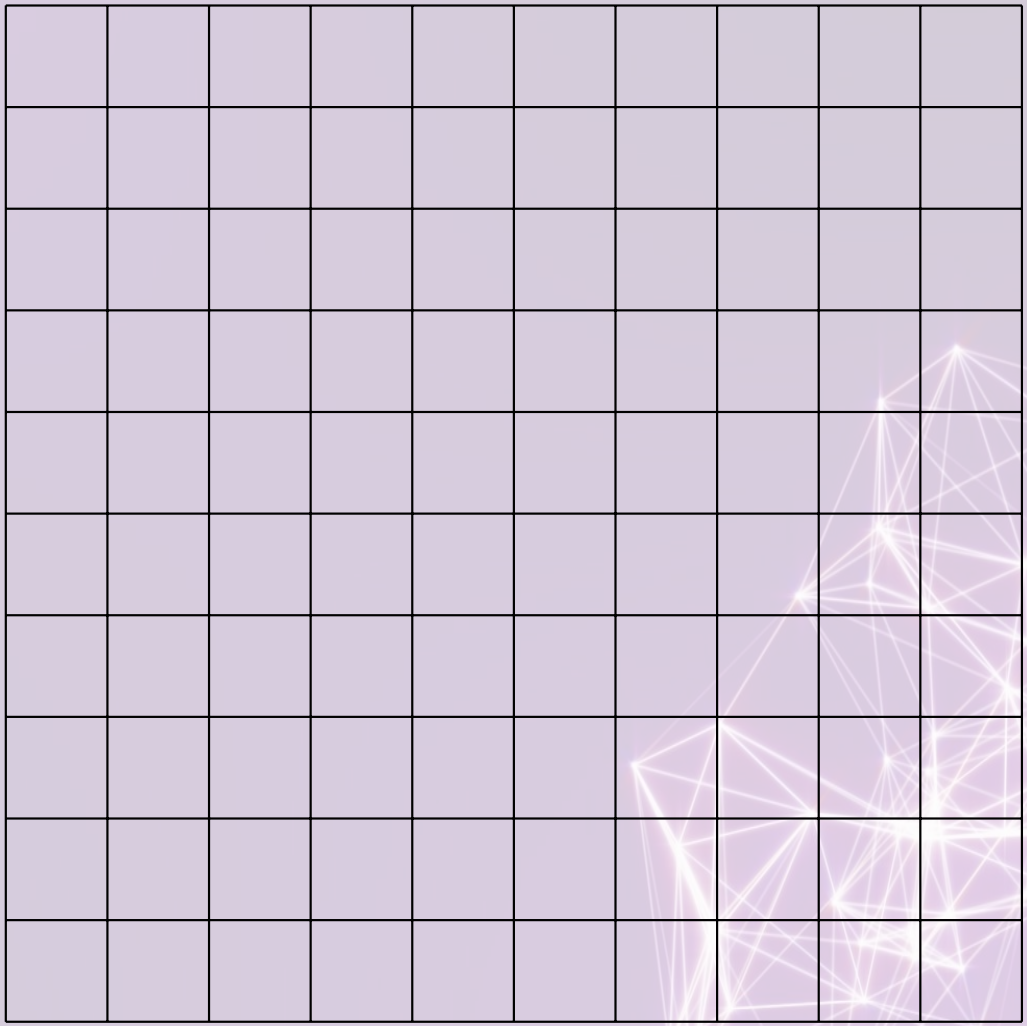
$\vdots$

Definición

Un **número primo** es un número natural mayor que 1 que sólo es divisible por sí mismo y por 1.

Criba de Eratóstenes

Eratóstenes, en el siglo III a.C. desarrolló un algoritmo para calcular números primos en un conjunto finito de naturales dados.



Criba de Eratóstenes

Eratóstenes, en el siglo III a.C. desarrolló un algoritmo para calcular números primos en un conjunto finito de naturales dados.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	60
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Criba de Eratóstenes

Eratóstenes, en el siglo III a.C. desarrolló un algoritmo para calcular números primos en un conjunto finito de naturales dados.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	60
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Criba de Eratóstenes

Eratóstenes, en el siglo III a.C. desarrolló un algoritmo para calcular números primos en un conjunto finito de naturales dados.

	2	3		5		7		9
11		13		15		17		19
21		23		25		27		29
31		33		35		37		39
41		43		45		47		49
51		53		55		57		59
61		63		65		67		69
71		73		75		77		79
81		83		85		87		89
91		93		95		97		99

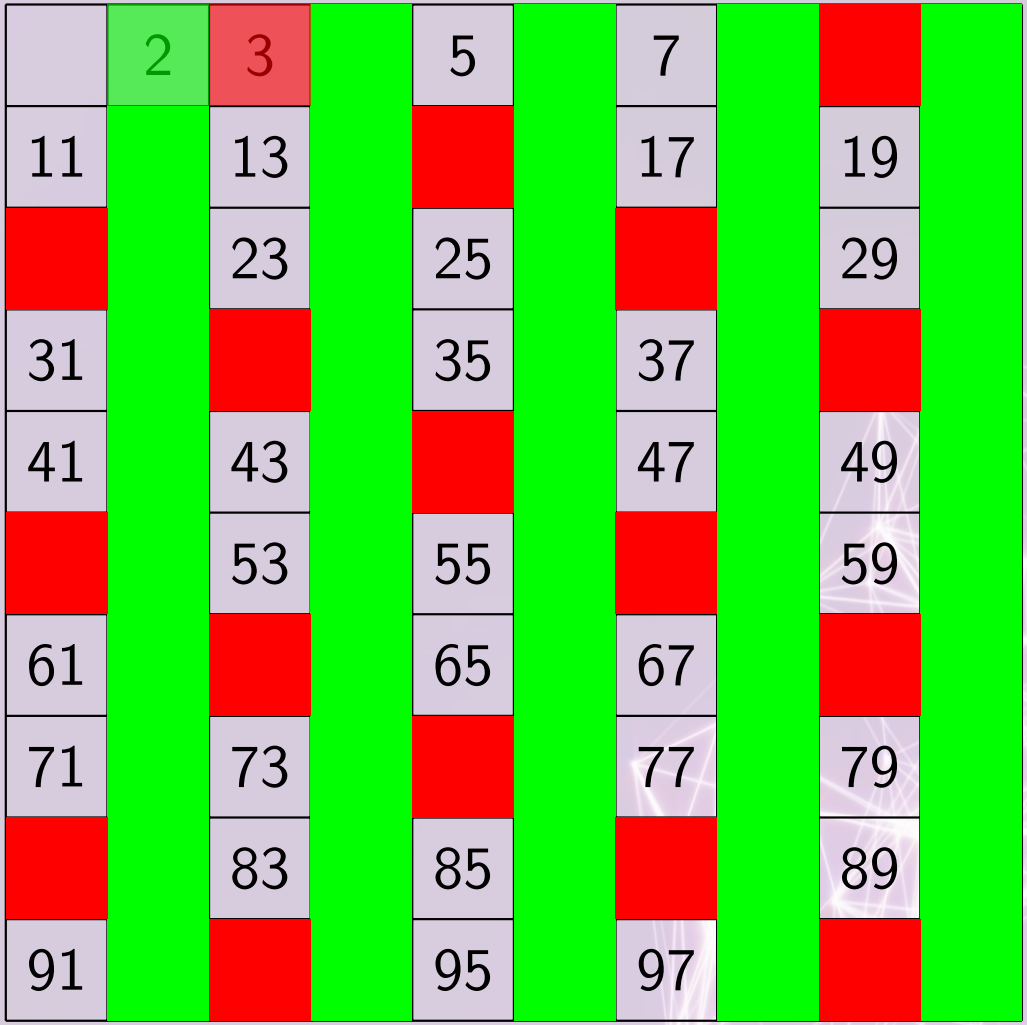
Criba de Eratóstenes

Eratóstenes, en el siglo III a.C. desarrolló un algoritmo para calcular números primos en un conjunto finito de naturales dados.

	2	3		5		7		9
11		13		15		17		19
21		23		25		27		29
31		33		35		37		39
41		43		45		47		49
51		53		55		57		59
61		63		65		67		69
71		73		75		77		79
81		83		85		87		89
91		93		95		97		99

Criba de Eratóstenes

Eratóstenes, en el siglo III a.C. desarrolló un algoritmo para calcular números primos en un conjunto finito de naturales dados.



Criba de Eratóstenes

Eratóstenes, en el siglo III a.C. desarrolló un algoritmo para calcular números primos en un conjunto finito de naturales dados.

Criba de Eratóstenes

Eratóstenes, en el siglo III a.C. desarrolló un algoritmo para calcular números primos en un conjunto finito de naturales dados.

Criba de Eratóstenes

Eratóstenes, en el siglo III a.C. desarrolló un algoritmo para calcular números primos en un conjunto finito de naturales dados.

Criba de Eratóstenes

Eratóstenes, en el siglo III a.C. desarrolló un algoritmo para calcular números primos en un conjunto finito de naturales dados.

Primeros 200 números primos

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71,
73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149,
151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227,
229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307,
311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389,
397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467,
479, 487, 491, 499, 503, 509, 521, 523, 541, 547, 557, 563, 569, 571,
577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653,
659, 661, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751,
757, 761, 769, 773, 787, 797, 809, 811, 821, 823, 827, 829, 839, 853,
857, 859, 863, 877, 881, 883, 887, 907, 911, 919, 929, 937, 941, 947,
953, 967, 971, 977, 983, 991, 997, 1009, 1013, 1019, 1021, 1031,
1033, 1039, 1049, 1051, 1061, 1063, 1069, 1087, 1091, 1093, 1097,
1103, 1109, 1117, 1123, 1129, 1151, 1153, 1163, 1171, 1181, 1187,
1193, 1201, 1213, 1217, ...

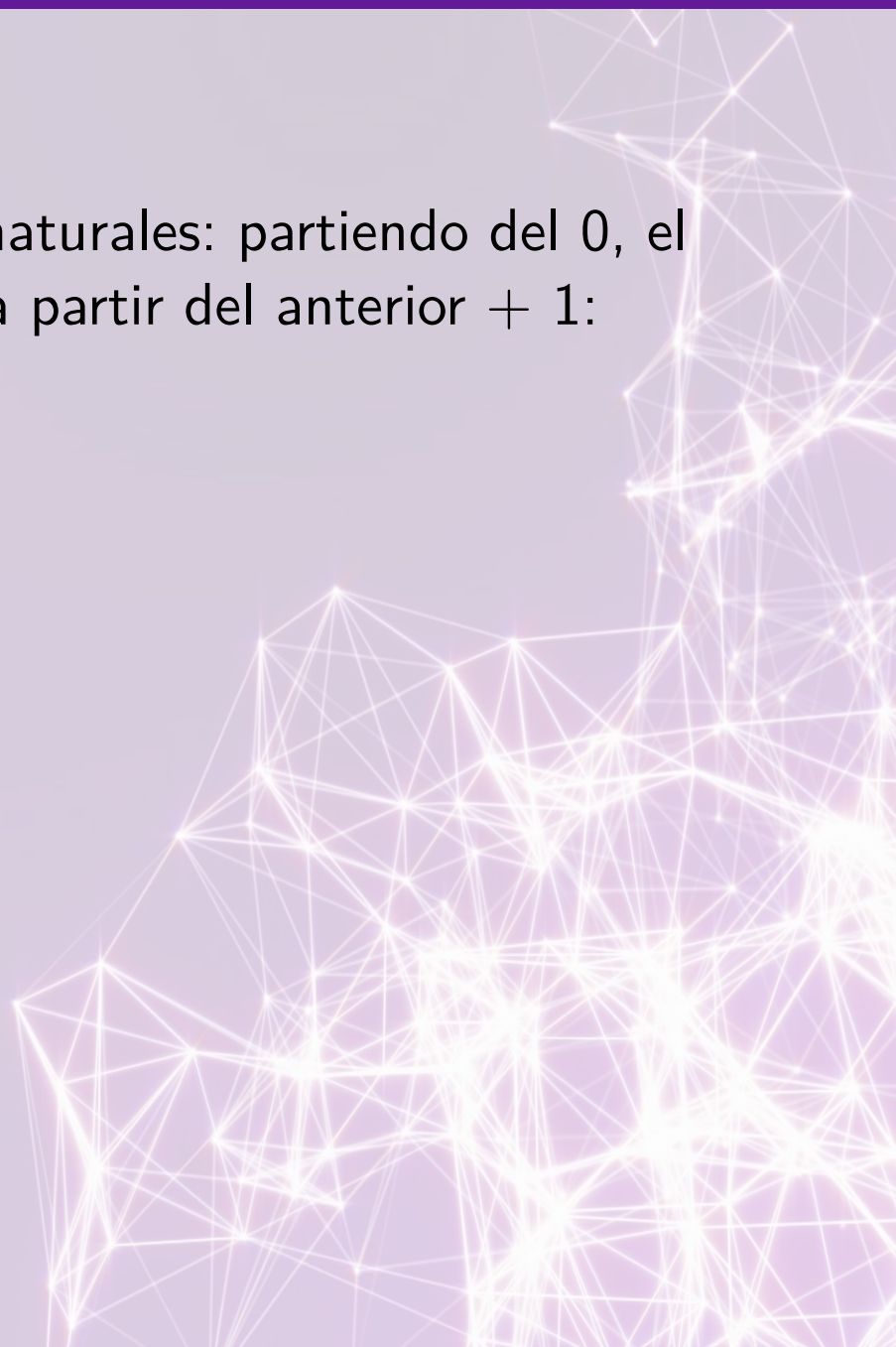
Primeros 200 números primos

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71,
73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149,
151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227,
229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307,
311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389,
397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467,
479, 487, 491, 499, 503, 509, 521, 523, 541, 547, 557, 563, 569, 571,
577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653,
659, 661, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751,
757, 761, 769, 773, 787, 797, 809, 811, 821, 823, 827, 829, 839, 853,
857, 859, 863, 877, 881, 883, 887, 907, 911, 919, 929, 937, 941, 947,
953, 967, 971, 977, 983, 991, 997, 1009, 1013, 1019, 1021, 1031,
1033, 1039, 1049, 1051, 1061, 1063, 1069, 1087, 1091, 1093, 1097,
1103, 1109, 1117, 1123, 1129, 1151, 1153, 1163, 1171, 1181, 1187,
1193, 1201, 1213, 1217, ...

¿Se acaba en algún momento?

Números naturales

Hay una cantidad *infinita* de números naturales: partiendo del 0, el siguiente número natural se construye a partir del anterior + 1:



Números naturales

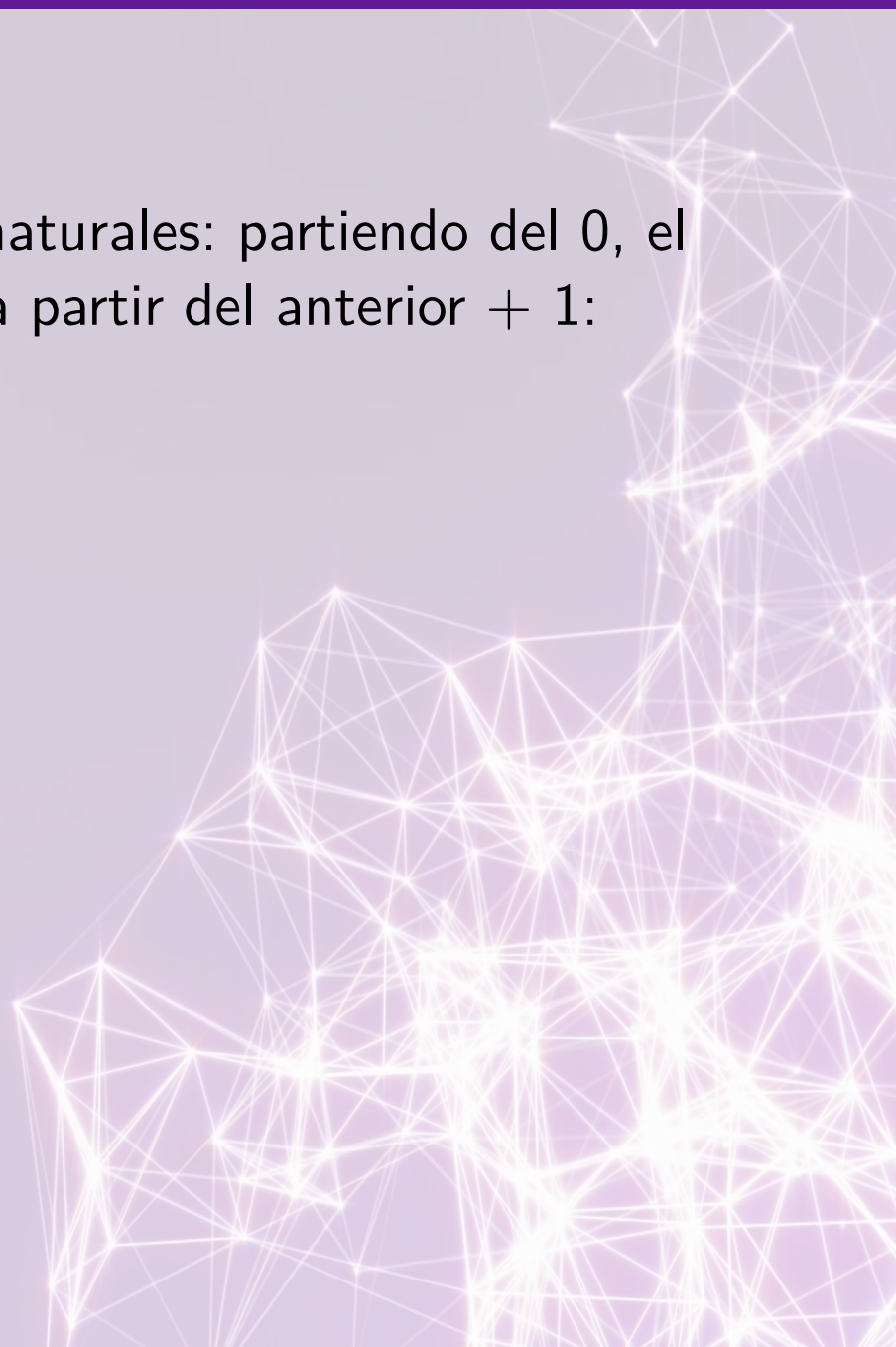
Hay una cantidad *infinita* de números naturales: partiendo del 0, el siguiente número natural se construye a partir del anterior + 1:

- 0

Números naturales

Hay una cantidad *infinita* de números naturales: partiendo del 0, el siguiente número natural se construye a partir del anterior + 1:

- 0
- $0 + 1 = 1$



Números naturales

Hay una cantidad *infinita* de números naturales: partiendo del 0, el siguiente número natural se construye a partir del anterior + 1:

- 0
- $0 + 1 = 1$
- $1 + 1 = 2$

Números naturales

Hay una cantidad *infinita* de números naturales: partiendo del 0, el siguiente número natural se construye a partir del anterior + 1:

- 0
- $0 + 1 = 1$
- $1 + 1 = 2$
- $2 + 1 = 3$

$\vdots$

Números naturales

Hay una cantidad *infinita* de números naturales: partiendo del 0, el siguiente número natural se construye a partir del anterior + 1:

- 0
- $0 + 1 = 1$
- $1 + 1 = 2$
- $2 + 1 = 3$
- $\vdots$

Por esta propia construcción, sabemos que hay infinitos números naturales.

Números naturales

Hay una cantidad *infinita* de números naturales: partiendo del 0, el siguiente número natural se construye a partir del anterior + 1:

- 0
- $0 + 1 = 1$
- $1 + 1 = 2$
- $2 + 1 = 3$

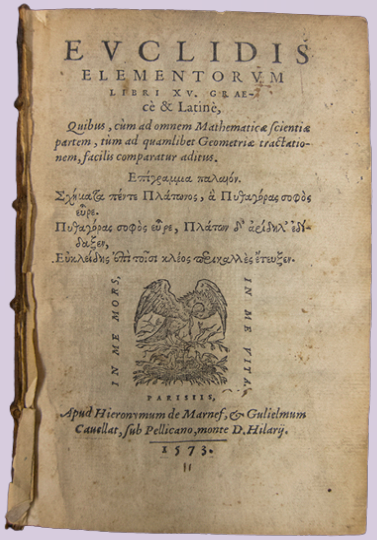
$\vdots$

Por esta propia construcción, sabemos que hay infinitos números naturales.

Spoiler: hay infinitos números primos.

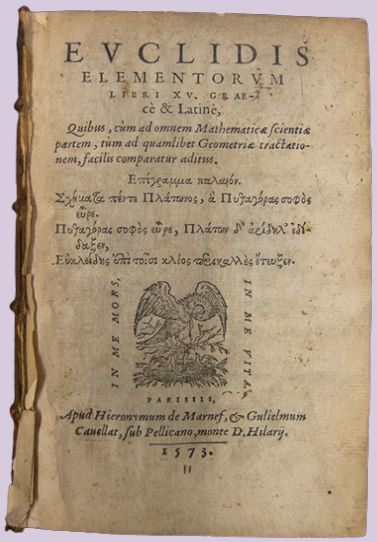
Euclides

- En el siglo III a.C., Euclides escribió un tratado matemático, compuesto de 13 libros, llamado *Elementos*.


EVCLIDIS
ELEMENTORVM
LIBRI XV. GRAE-
cè & Latinè,
Quibus, cùm ad omnem Mathematicæ scientiæ partem, tùm ad quamlibet Geometriæ tractationem, facilis comparatur aditus.
Επίγραμμα παλαιόν.
Σχήματα πέντε Πλάτωνος, ἃ Πυθαγόρας σοφὸς εὗρε.
Πυθαγόρας σοφὸς ὦρε, Πλάτων δ' ἀσίδυκ' ἰδέδα-ξεν,
Εὐκλείδης ὅτι τοῖσι κλέος ἄφθιτον ἔτευξεν.
IN ME MORS.
IN ME VITA.
PARISIIS,
Apud Hieronymum de Marnef, & Gulielmum Cauellat, sub Pellicano, monte D. Hilarij.
1573.

Euclides

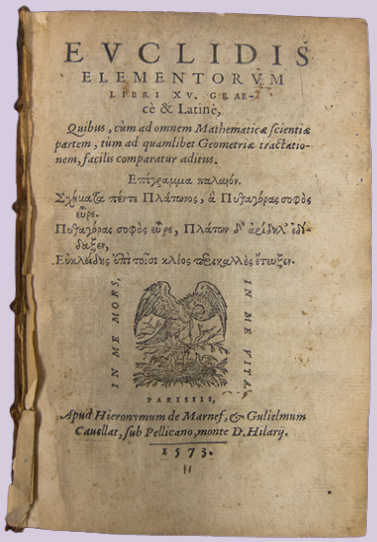
- En el siglo III a.C., Euclides escribió un tratado matemático, compuesto de 13 libros, llamado *Elementos*.


EVCLIDIS
ELEMENTORVM
LIBRI XV. GRAE-
cè & Latinè,
Quibus, cùm ad omnem Mathematicæ scientiæ partem, tùm ad quamlibet Geometriæ tractationem, facilis comparatur aditus.
Επίγραμμα παλαιόν.
Σχήματα πέντε Πλάτωνος, ἃ Πυθαγόρας σοφὸς εὗρε.
Πυθαγόρας σοφὸς ὤφρε, Πλάτων δ' ἀείδελ' ἰδέ-
δαξεν,
Εὐκλείδης ὅτι τοῖσι κλέος ἀθανάτοις ἔπυζεν.
IN ME MORS,
IN ME VITA.
PARISIIS,
Apud Hieronymum de Marnef, & Guilielmum Cauellat, sub Pellicano, monte D. Hilarij.
1573.
11

- *Elementos* es uno de los libros más divulgado de la historia, siendo el segundo en número de ediciones publicadas después de la Biblia (más de 1000).

Euclides

- En el siglo III a.C., Euclides escribió un tratado matemático, compuesto de 13 libros, llamado *Elementos*.


EVCLIDIS
ELEMENTORVM
LIBRI XV. GRAE-
cè & Latinè,
Quibus, cùm ad omnem Mathematicæ scientiæ partem, tùm ad quamlibet Geometriæ tractationem, facilis comparatur aditus.
Επίγραμμα παλαιόν.
Σχήματα πέντε Πλάτωνος, ἃ Πυθαγόρας σοφὸς εὗρε.
Πυθαγόρας σοφὸς ὤφρε, Πλάτων δ' ἐδίδαξ' ἰδίοις,
Εὐκλείδης δ' ἔτι τοῖσι κλέος ἀθάνατον ἔτευξεν.
IN ME MORS, IN ME VITA.
PARISIIS,
Apud Hieronymum de Marnef, & Guilielmum Cauellat, sub Pellicano, monte D. Hilarij.
1573.

- *Elementos* es uno de los libros más divulgado de la historia, siendo el segundo en número de ediciones publicadas después de la Biblia (más de 1000).
- En este tratado, Euclides *demostró matemáticamente* que hay **infinitos números primos**, y que **todo número natural se descompone de manera única en producto de primos**; entre otros resultados importantes.

Distribución de los números primos

¿Existe algún patrón que nos permita describir a los números primos?
¿Cómo están distribuidos?

Distribución de los números primos

¿Existe algún patrón que nos permita describir a los números primos?
¿Cómo están distribuidos?

- A día de hoy, casi 2500 años más tarde, estas cuestiones *no se han resuelto* de manera precisa.

Distribución de los números primos

¿Existe algún patrón que nos permita describir a los números primos?
¿Cómo están distribuidos?

- A día de hoy, casi 2500 años más tarde, estas cuestiones *no se han resuelto* de manera precisa.
- Después de los descubrimientos de Euclides, no hubo muchos avances en teoría de números durante varios siglos.

Distribución de los números primos

¿Existe algún patrón que nos permita describir a los números primos?
¿Cómo están distribuidos?

- A día de hoy, casi 2500 años más tarde, estas cuestiones *no se han resuelto* de manera precisa.
- Después de los descubrimientos de Euclides, no hubo muchos avances en teoría de números durante varios siglos.
- Sin embargo, a partir del siglo XVII, muchos matemáticos importantes trataron de descubrir cuál es el patrón que siguen los números primos, y hubo grandes avances rápidamente.

Marin Mersenne
1588 - 1648

Pierre de Fermat
1601 - 1665

Leonhard Euler
1707 - 1783

Adrien-Marie Legendre
1752 - 1833

Sophie Germain
1776 - 1831

Carl Friedrich Gauss
1777 - 1855

Peter Gustav Lejeune Dirichlet
1805 - 1859

Bernhard Riemann
1826 - 1866

Función contadora de primos

Dado un número positivo x, vamos a representar por $\pi(x)$ a la cantidad de números primos que hay por debajo de x. Por ejemplo,

Función contadora de primos

Dado un número positivo x, vamos a representar por $\pi(x)$ a la cantidad de números primos que hay por debajo de x. Por ejemplo,

- Los primos por debajo de 4 son: 2 y 3. Luego $\pi(4) = 2$.

Función contadora de primos

Dado un número positivo x, vamos a representar por $\pi(x)$ a la cantidad de números primos que hay por debajo de x. Por ejemplo,

- Los primos por debajo de 4 son: 2 y 3. Luego $\pi(4) = 2$.
- Los primos por debajo de 7 son: 2, 3, 5 y 7. Luego $\pi(7) = 4$.

Función contadora de primos

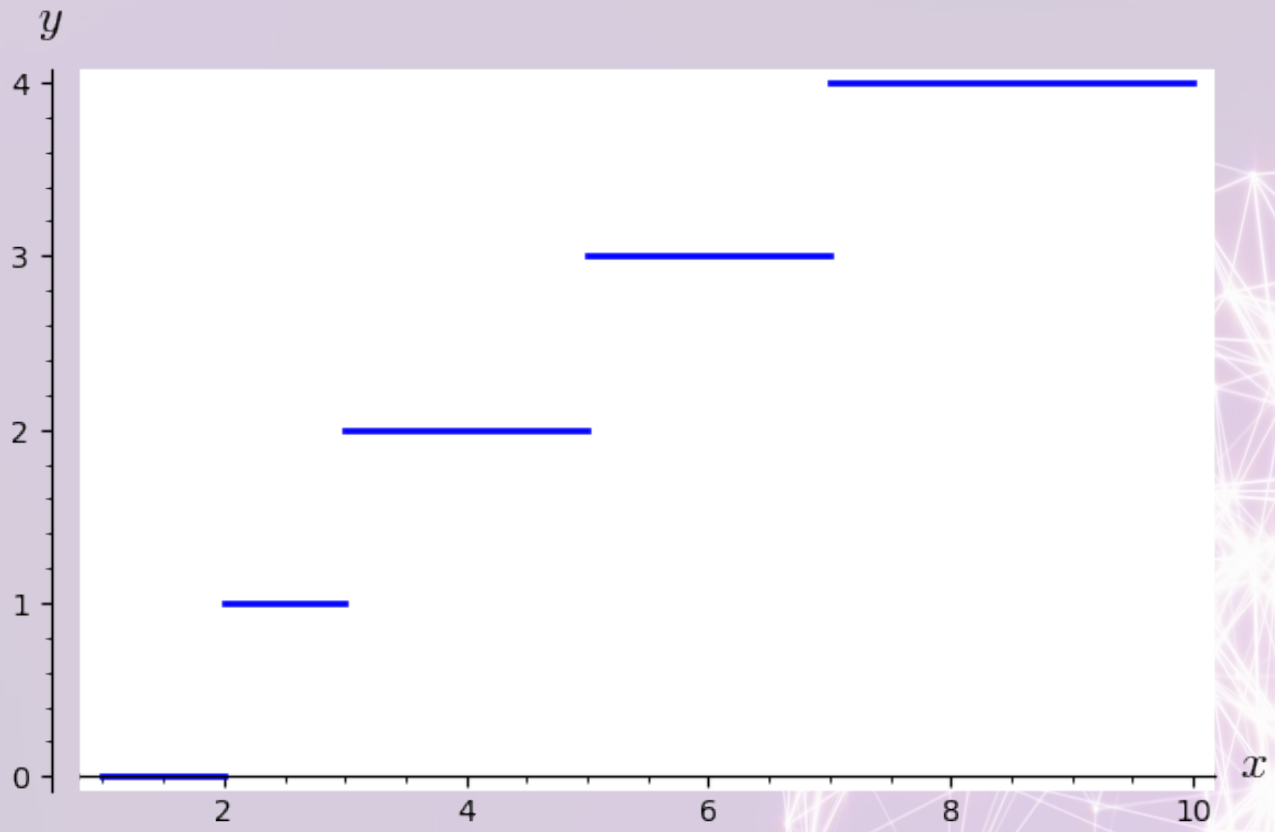
Dado un número positivo x, vamos a representar por $\pi(x)$ a la cantidad de números primos que hay por debajo de x. Por ejemplo,

- Los primos por debajo de 4 son: 2 y 3. Luego $\pi(4) = 2$.
- Los primos por debajo de 7 son: 2, 3, 5 y 7. Luego $\pi(7) = 4$.
- Los primos por debajo de 10 son: 2, 3, 5 y 7. Luego $\pi(10) = 4$.

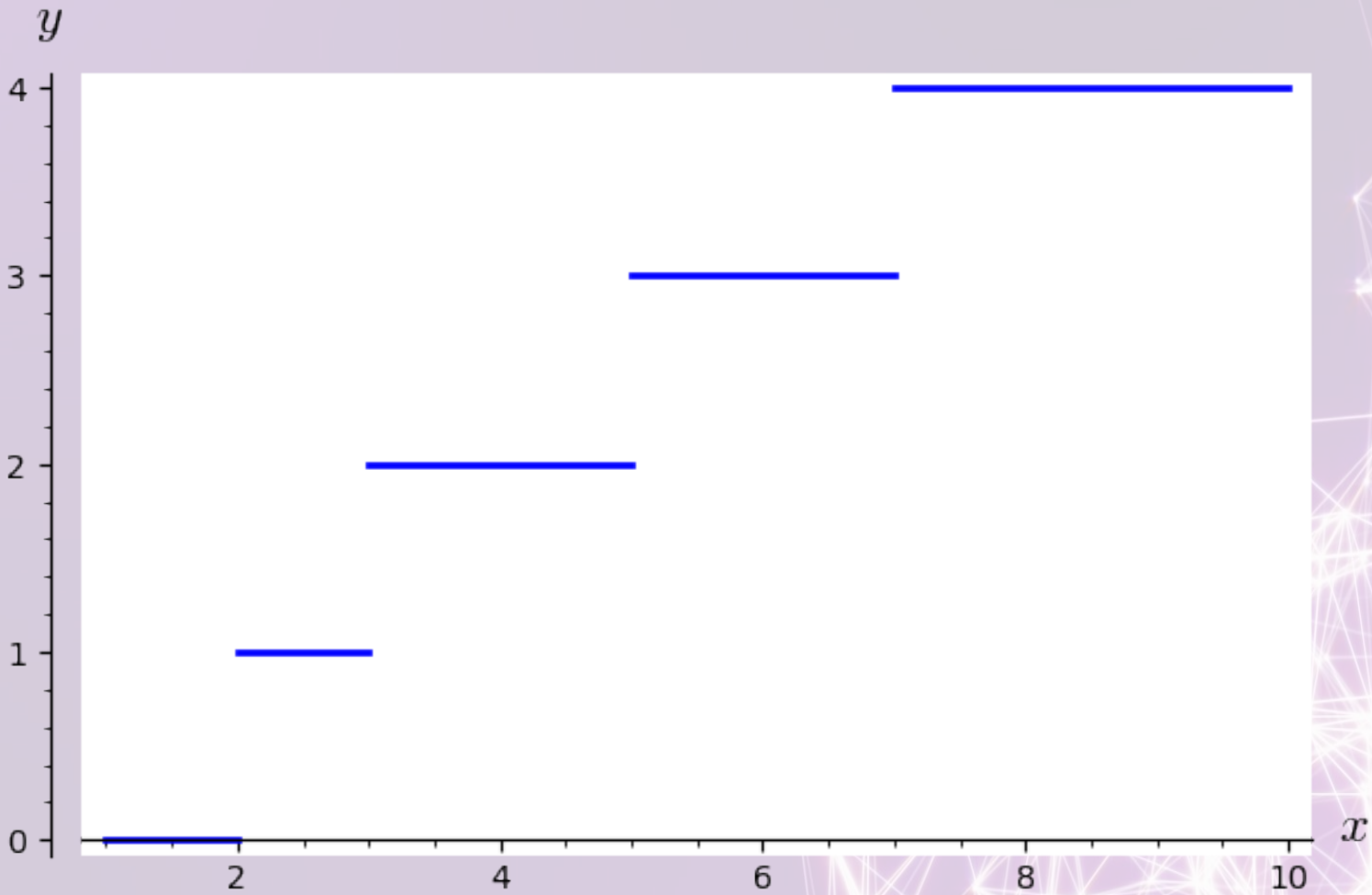
Función contadora de primos

Dado un número positivo x, vamos a representar por $\pi(x)$ a la cantidad de números primos que hay por debajo de x. Por ejemplo,

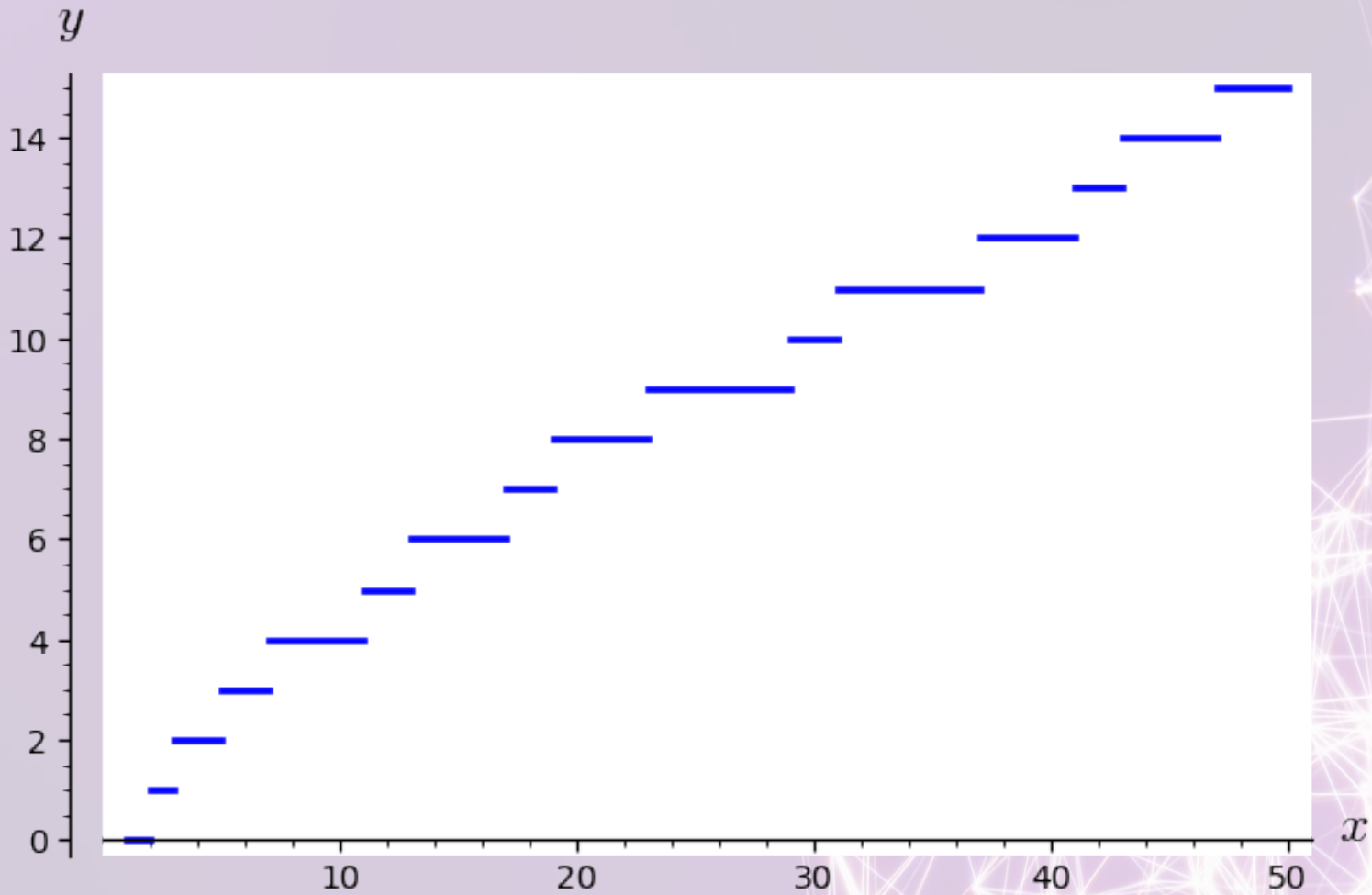
- Los primos por debajo de 4 son: 2 y 3. Luego $\pi(4) = 2$.
- Los primos por debajo de 7 son: 2, 3, 5 y 7. Luego $\pi(7) = 4$.
- Los primos por debajo de 10 son: 2, 3, 5 y 7. Luego $\pi(10) = 4$.



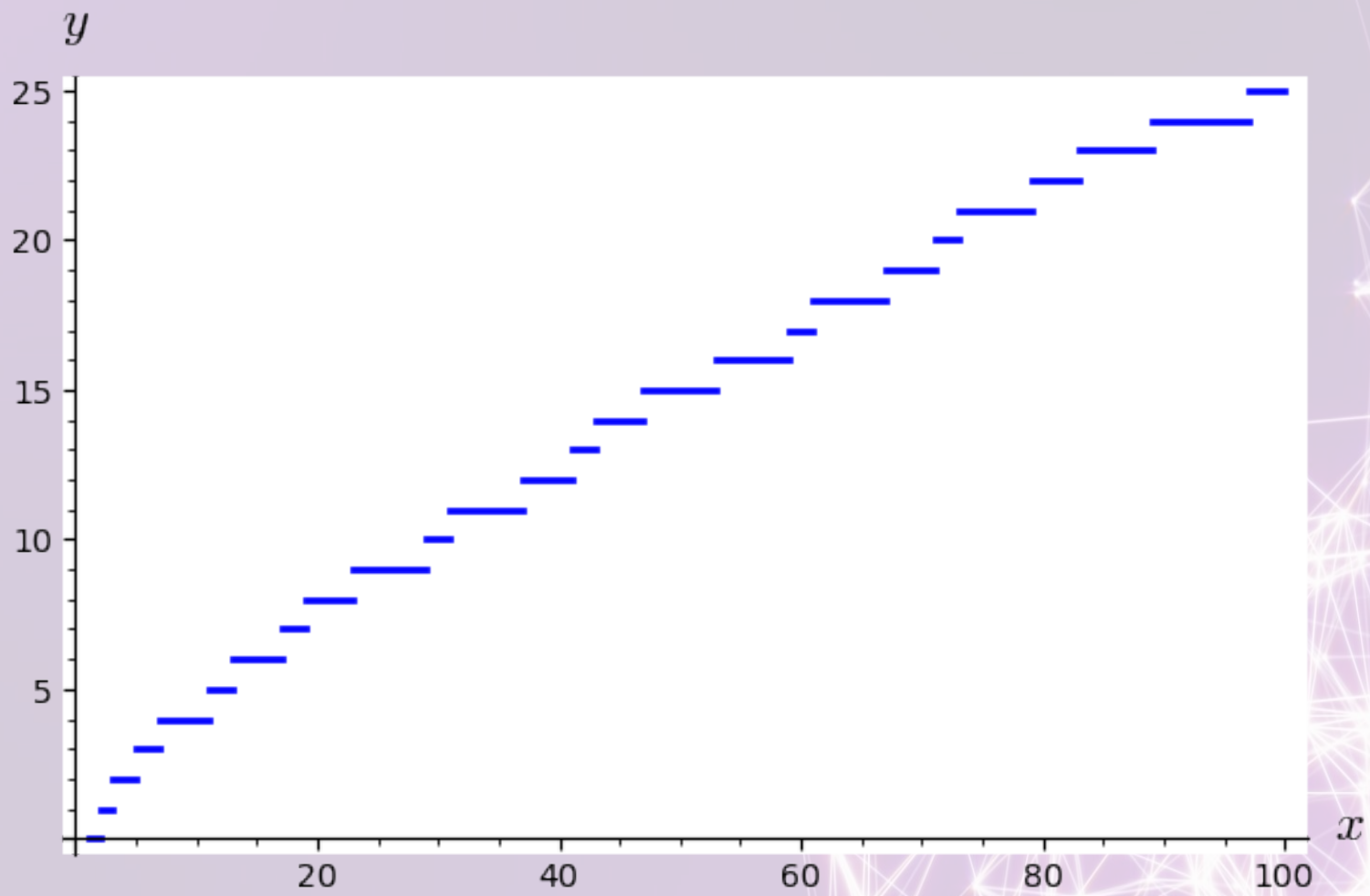
Distribución gráfica de los números primos



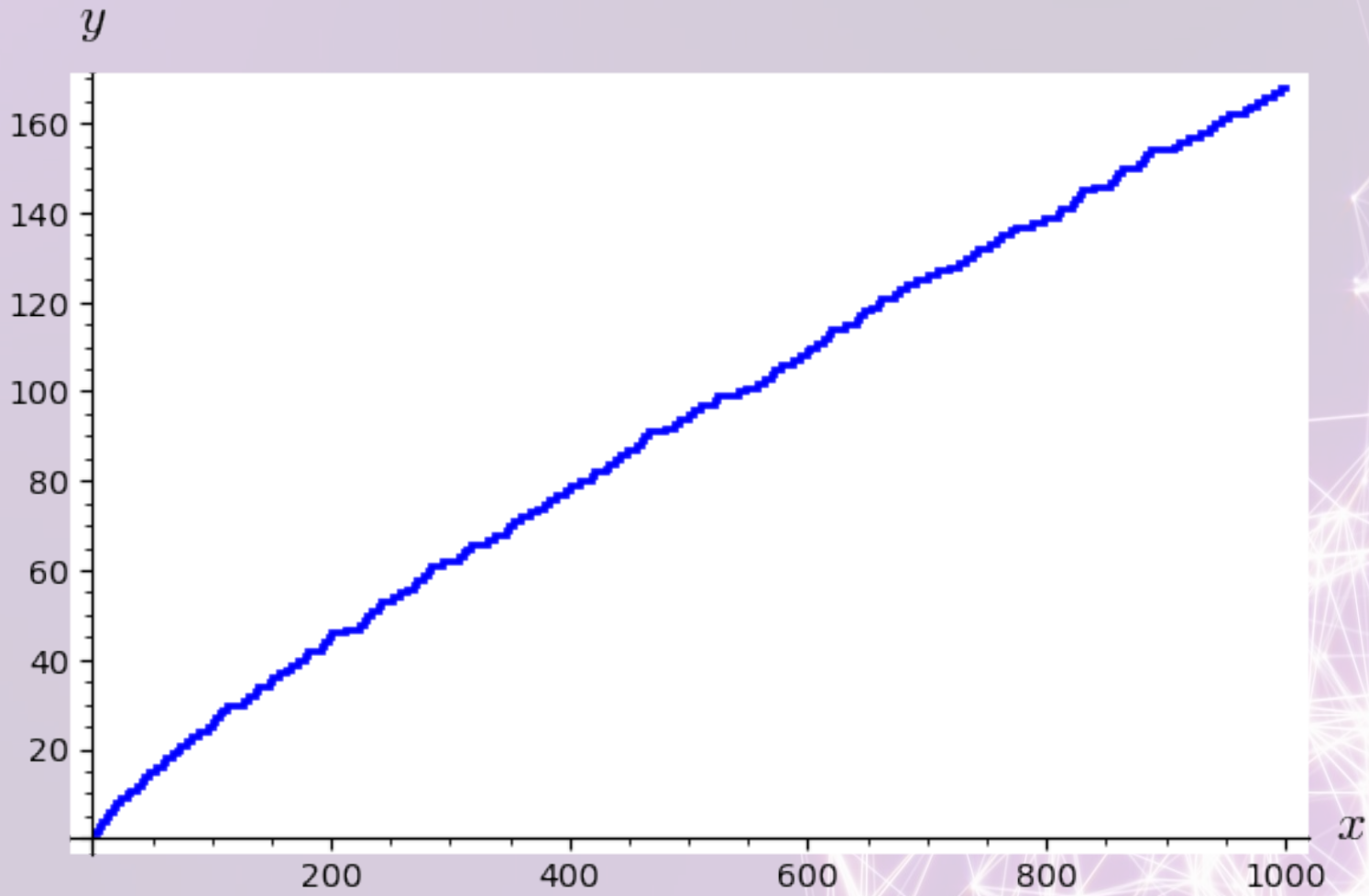
Distribución gráfica de los números primos



Distribución gráfica de los números primos



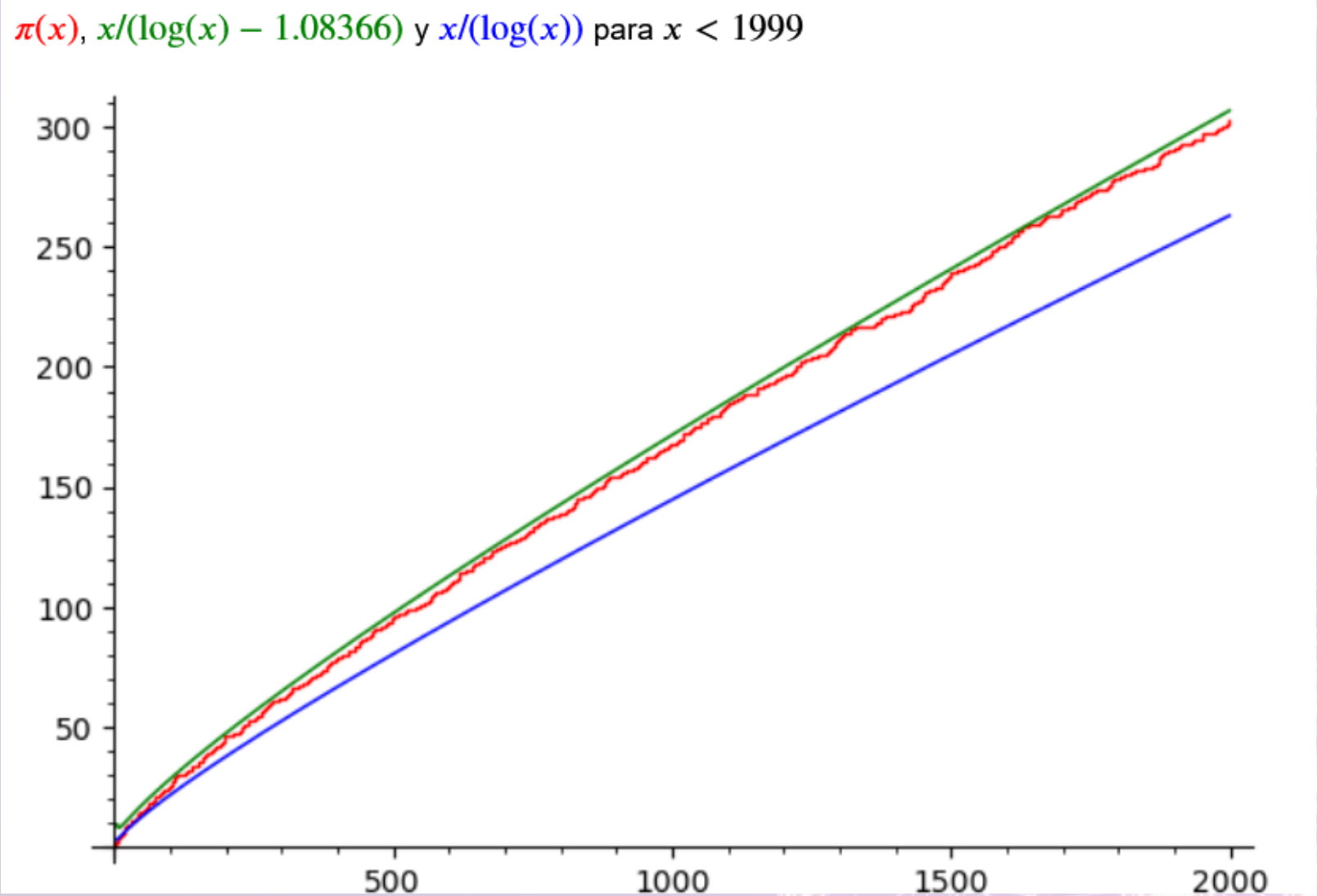
Distribución gráfica de los números primos



Gauss

Con tan sólo 14 años Gauss escribió una nota indicando el patrón una aproximación de los números primos. Para ello, comparó tablas de números primos (que llegaban hasta el número 400.00) con las de los logaritmos. Concluyó que, $\pi(x)$ se aproxima mucho a $\frac{x}{\ln(x)}$ cuando x es lo suficientemente grande.

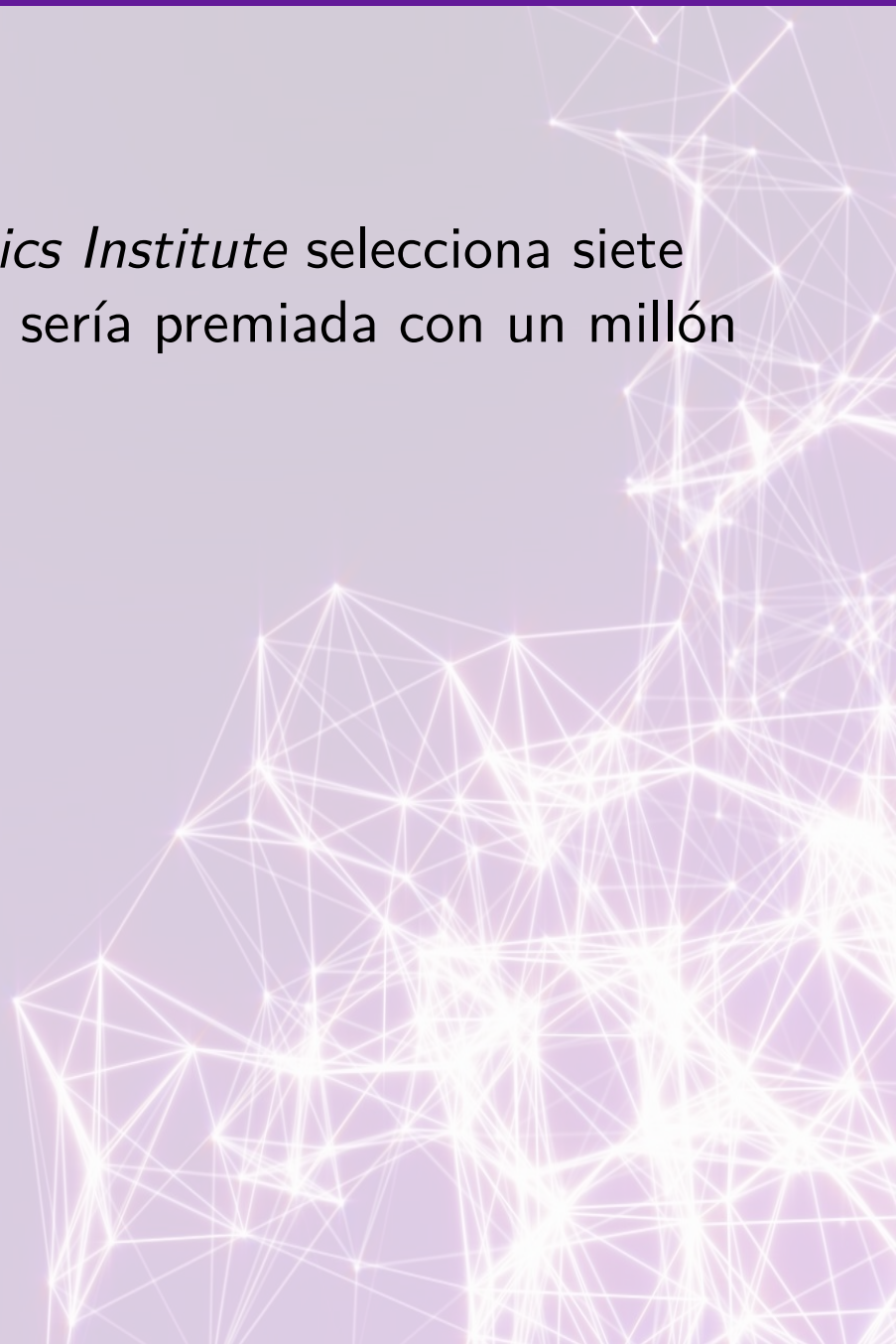
Gracias a las correspondencias entre Gauss y Legendre, y a la contribución de otros matemáticos como Dirichlet o Riemann, lograron dar una aproximación mejor: $\pi(x) \sim \frac{x}{\ln(x)-1{,}08366}$



Conexión con la hipótesis de Riemann

Conexión con la hipótesis de Riemann

- En el año 2000, el *Clay Mathematics Institute* selecciona siete problemas abiertos cuya resolución sería premiada con un millón de dólares cada uno.



Conexión con la hipótesis de Riemann

- En el año 2000, el *Clay Mathematics Institute* selecciona siete problemas abiertos cuya resolución sería premiada con un millón de dólares cada uno.
- Uno de ellos es la *hipótesis de Riemann* y está profundamente conectada con la distribución de los números primos.

Conexión con la hipótesis de Riemann

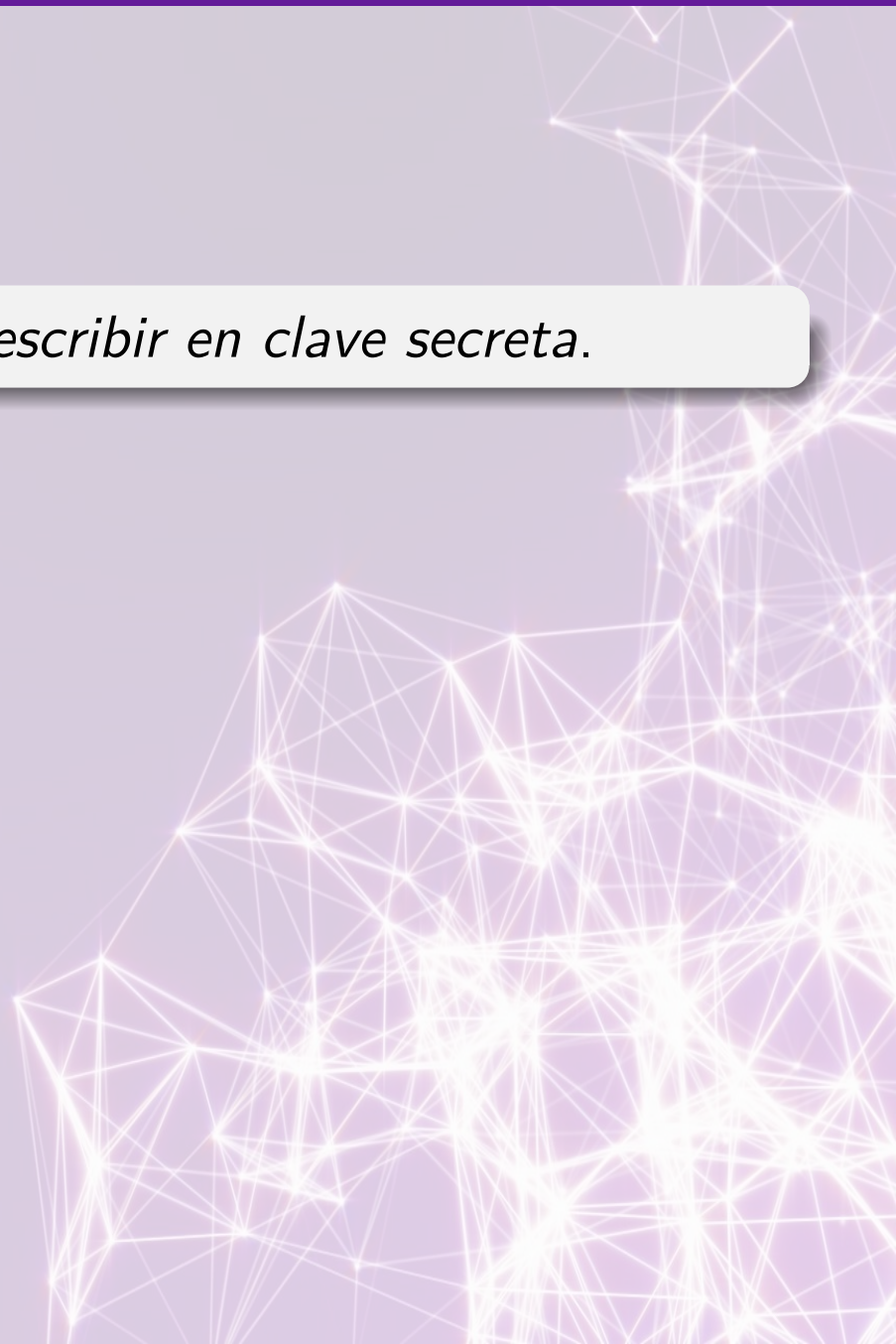
- En el año 2000, el *Clay Mathematics Institute* selecciona siete problemas abiertos cuya resolución sería premiada con un millón de dólares cada uno.
- Uno de ellos es la *hipótesis de Riemann* y está profundamente conectada con la distribución de los números primos.
- "*Si me despertara después de haber dormido durante mil años, mi primera pregunta sería: ¿ha sido demostrada la hipótesis de Riemann?*" - David Hilbert, 1900.

Conexión con la hipótesis de Riemann

- En el año 2000, el *Clay Mathematics Institute* selecciona siete problemas abiertos cuya resolución sería premiada con un millón de dólares cada uno.
- Uno de ellos es la *hipótesis de Riemann* y está profundamente conectada con la distribución de los números primos.
- "*Si me despertara después de haber dormido durante mil años, mi primera pregunta sería: ¿ha sido demostrada la hipótesis de Riemann?*" - David Hilbert, 1900.
- Si fuera cierta, implicaría que los números primos están distribuidos de la forma más regular posible, y que las irregularidades en su distribución sólo procede de "ruido aleatorio".

Qué es la criptografía

La **criptografía** es el arte y ciencia de *escribir en clave secreta*.



Qué es la criptografía

La **criptografía** es el arte y ciencia de *escribir en clave secreta*.

Hay dos grandes épocas que se distinguen en criptografía:

Qué es la criptografía

La **criptografía** es el arte y ciencia de *escribir en clave secreta*.

Hay dos grandes épocas que se distinguen en criptografía:

- Clásica: abarca hasta mediados del siglo XX.

Qué es la criptografía

La **criptografía** es el arte y ciencia de *escribir en clave secreta*.

Hay dos grandes épocas que se distinguen en criptografía:

- Clásica: abarca hasta mediados del siglo XX.
- Moderna: surge con el desarrollo de los ordenadores y la informática.

Qué es la criptografía

La **criptografía** es el arte y ciencia de *escribir en clave secreta*.

Hay dos grandes épocas que se distinguen en criptografía:

- Clásica: abarca hasta mediados del siglo XX.
- Moderna: surge con el desarrollo de los ordenadores y la informática.

Aunque no nos demos cuenta la *criptografía está presente en nuestro día a día*: al enviar un e-mail, al hacer una búsqueda en internet, al enviar un mensaje por chat, para proteger las cuentas bancarias...

Cifrado César

- El *cifrado César* es uno de los primeros cifrados más de la historia: tuvo su origen en el siglo I a.C.

Cifrado César

- El *cifrado César* es uno de los primeros cifrados más de la historia: tuvo su origen en el siglo I a.C.
- Su nombre se debe al militar romano Julio César, quien utilizaba este cifrado en sus correspondencias privadas, e incluso durante la guerra de las Galias.

Cifrado César

- El *cifrado César* es uno de los primeros cifrados más de la historia: tuvo su origen en el siglo I a.C.
- Su nombre se debe al militar romano Julio César, quien utilizaba este cifrado en sus correspondencias privadas, e incluso durante la guerra de las Galias.

Cifrado César

- El *cifrado César* es uno de los primeros cifrados más de la historia: tuvo su origen en el siglo I a.C.
- Su nombre se debe al militar romano Julio César, quien utilizaba este cifrado en sus correspondencias privadas, e incluso durante la guerra de las Galias.

E	U	C	L	I	D	E	S

Cifrado César

- El *cifrado César* es uno de los primeros cifrados más de la historia: tuvo su origen en el siglo I a.C.
- Su nombre se debe al militar romano Julio César, quien utilizaba este cifrado en sus correspondencias privadas, e incluso durante la guerra de las Galias.

E	U	C	L	I	D	E	S

$\downarrow +3$

H	X	F	O	L	G	H	V

Cifrado César

- El *cifrado César* es uno de los primeros cifrados más de la historia: tuvo su origen en el siglo I a.C.
- Su nombre se debe al militar romano Julio César, quien utilizaba este cifrado en sus correspondencias privadas, e incluso durante la guerra de las Galias.

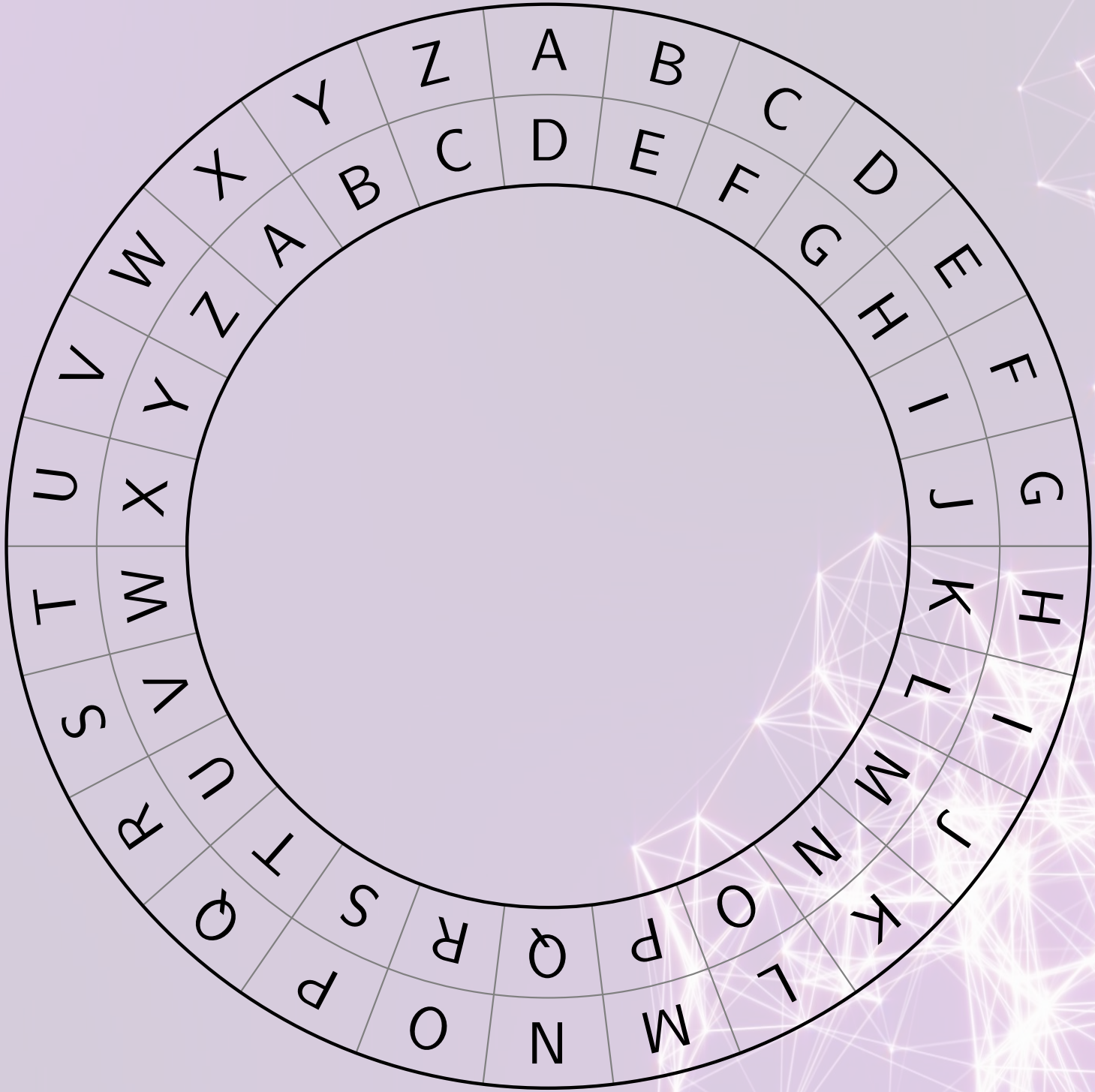
E	U	C	L	I	D	E	S

$\downarrow +3$

H	X	F	O	L	G	H	V

$\downarrow$ -3

E	U	C	L	I	D	E	S


A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
B C D E F G H I J K L M N O P Q R S T U V W X Y Z A
C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
F G H I J K L M N O P Q R S T U V W X Y Z A B C D E
G H I J K L M N O P Q R S T U V W X Y Z A B C D E F
H I J K L M N O P Q R S T U V W X Y Z A B C D E F G
I J K L M N O P Q R S T U V W X Y Z A B C D E F G H
J K L M N O P Q R S T U V W X Y Z A B C D E F G H I
K L M N O P Q R S T U V W X Y Z A B C D E F G H I J
L M N O P Q R S T U V W X Y Z A B C D E F G H I J K
M N O P Q R S T U V W X Y Z A B C D E F G H I J K L
N O P Q R S T U V W X Y Z A B C D E F G H I J K L M
O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
P Q R S T U V W X Y Z A B C D E F G H I J K L M N O
Q R S T U V W X Y Z A B C D E F G H I J K L M N O P
R S T U V W X Y Z A B C D E F G H I J K L M N O P Q
S T U V W X Y Z A B C D E F G H I J K L M N O P Q R
T U V W X Y Z A B C D E F G H I J K L M N O P Q R S
U V W X Y Z A B C D E F G H I J K L M N O P Q R S T
V W X Y Z A B C D E F G H I J K L M N O P Q R S T U
W X Y Z A B C D E F G H I J K L M N O P Q R S T U V
X Y Z A B C D E F G H I J K L M N O P Q R S T U V W
Y Z A B C D E F G H I J K L M N O P Q R S T U V W X
Z A B C D E F G H I J K L M N O P Q R S T U V W X Y

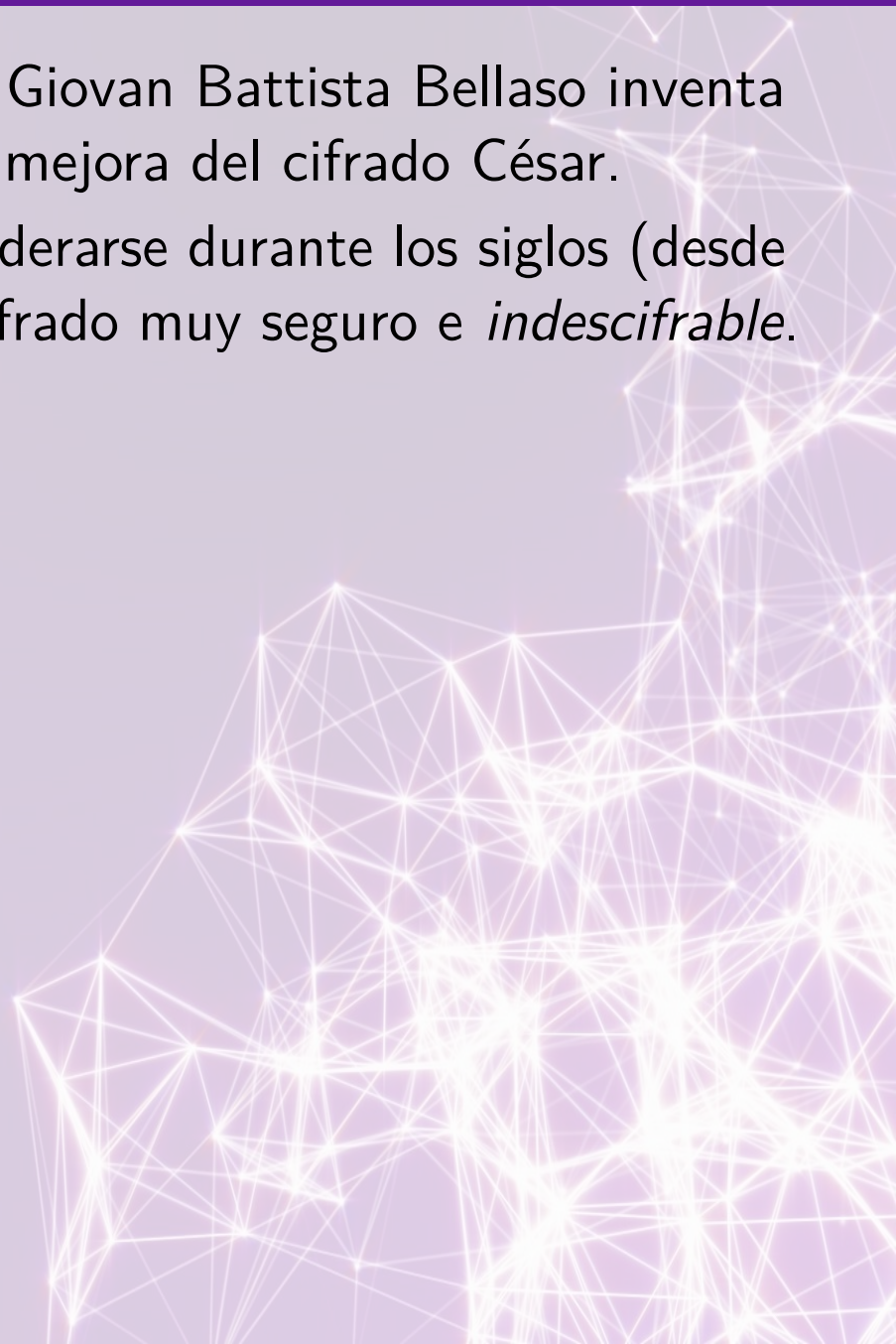

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
G H I J K L M N O P Q R S T U V W X Y Z A B C D E F
I J K L M N O P Q R S T U V W X Y Z A B C D E F G H
K L M N O P Q R S T U V W X Y Z A B C D E F G H I J
M N O P Q R S T U V W X Y Z A B C D E F G H I J K L
O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
Q R S T U V W X Y Z A B C D E F G H I J K L M N O P
S T U V W X Y Z A B C D E F G H I J K L M N O P Q R
U V W X Y Z A B C D E F G H I J K L M N O P Q R S T
W X Y Z A B C D E F G H I J K L M N O P Q R S T U V
Y Z A B C D E F G H I J K L M N O P Q R S T U V W X
Z A B C D E F G H I J K L M N O P Q R S T U V W X Y

Cifrado de Vigenère

- Durante el siglo XVI, el criptólogo Giovan Battista Bellaso inventa el *cifrado de Vigenère*, que es una mejora del cifrado César.

Cifrado de Vigenère

- Durante el siglo XVI, el criptólogo Giovan Battista Bellaso inventa el *cifrado de Vigenère*, que es una mejora del cifrado César.
- El cifrado de Vigenère llegó a considerarse durante los siglos (desde el XVII hasta finales del XIX) un cifrado muy seguro e *indescifrable*.



Cifrado de Vigenère

- Durante el siglo XVI, el criptólogo Giovan Battista Bellaso inventa el *cifrado de Vigenère*, que es una mejora del cifrado César.
- El cifrado de Vigenère llegó a considerarse durante los siglos (desde el XVII hasta finales del XIX) un cifrado muy seguro e *indescifrable*.

Blaise de Vigenère

Ejemplo de cifrado de Vigènere

Elegimos la clave: `L E O N (11, 4, 14, 13)`

E	U	C	L	I	D	E	S
L	E	O	N	L	E	O	N

Ejemplo de cifrado de Vigènere

Elegimos la clave: `L E O N (11, 4, 14, 13)`

E	U	C	L	I	D	E	S
L	E	O	N	L	E	O	N

↓

P	

Ejemplo de cifrado de Vigènere

Elegimos la clave: `L E O N (11, 4, 14, 13)`

E	U	C	L	I	D	E	S
L	E	O	N	L	E	O	N

↓

P	Y	

Ejemplo de cifrado de Vigènere

Elegimos la clave: `L E O N (11, 4, 14, 13)`

E	U	C	L	I	D	E	S
L	E	O	N	L	E	O	N

↓

P	Y	Q	

Ejemplo de cifrado de Vigènere

Elegimos la clave: `L E O N (11, 4, 14, 13)`

E	U	C	L	I	D	E	S
L	E	O	N	L	E	O	N

↓

P	Y	Q	Y	

Ejemplo de cifrado de Vigènere

Elegimos la clave: `L E O N (11, 4, 14, 13)`

E	U	C	L	I	D	E	S
L	E	O	N	L	E	O	N

↓

P	Y	Q	Y	T	

Ejemplo de cifrado de Vigènere

Elegimos la clave: `L E O N (11, 4, 14, 13)`

E	U	C	L	I	D	E	S
L	E	O	N	L	E	O	N

↓

P	Y	Q	Y	T	H		

Ejemplo de cifrado de Vigènere

Elegimos la clave: `L E O N (11, 4, 14, 13)`

E	U	C	L	I	D	E	S
L	E	O	N	L	E	O	N

↓

P	Y	Q	Y	T	H	S	

Ejemplo de cifrado de Vigènere

Elegimos la clave: `L E O N (11, 4, 14, 13)`

E	U	C	L	I	D	E	S
L	E	O	N	L	E	O	N

↓

P	Y	Q	Y	T	H	S	F

Ejemplo del cifrado de Vigenère

P	Y	Q	Y	T	H	S	F
L	E	O	N	L	E	O	N

Ejemplo del cifrado de Vigenère

P	Y	Q	Y	T	H	S	F
L	E	O	N	L	E	O	N

↓

E	

Ejemplo del cifrado de Vigenère

P	Y	Q	Y	T	H	S	F
L	E	O	N	L	E	O	N

E	U	

Ejemplo del cifrado de Vigenère

P	Y	Q	Y	T	H	S	F
L	E	O	N	L	E	O	N

E	U	C	

Ejemplo del cifrado de Vigenère

P	Y	Q	Y	T	H	S	F
L	E	O	N	L	E	O	N

↓

E	U	C	L	

Ejemplo del cifrado de Vigenère

P	Y	Q	Y	T	H	S	F
L	E	O	N	L	E	O	N

E	U	C	L	I	

Ejemplo del cifrado de Vigenère

P	Y	Q	Y	T	H	S	F
L	E	O	N	L	E	O	N

E	U	C	L	I	D	

Ejemplo del cifrado de Vigenère

P	Y	Q	Y	T	H	S	F
L	E	O	N	L	E	O	N

E	U	C	L	I	D	E	

Ejemplo del cifrado de Vigenère

P	Y	Q	Y	T	H	S	F
L	E	O	N	L	E	O	N

↓

E	U	C	L	I	D	E	S

Enigma

- En 1918, el ingeniero eléctrico Arthur Scherbius inventa la *máquina Enigma*.

Enigma

- En 1918, el ingeniero eléctrico Arthur Scherbius inventa la *máquina Enigma*.
- Se trata de un mecanismo de cifrado cuyo diseño hace posible que tuviera más de 150 billones de configuraciones distintas.

Enigma

- En 1918, el ingeniero eléctrico Arthur Scherbius inventa la *máquina Enigma*.
- Se trata de un mecanismo de cifrado cuyo diseño hace posible que tuviera más de 150 billones de configuraciones distintas.

Enigma

- En 1918, el ingeniero eléctrico Arthur Scherbius inventa la *máquina Enigma*.
- Se trata de un mecanismo de cifrado cuyo diseño hace posible que tuviera más de 150 billones de configuraciones distintas.

Posibles configuraciones:

- César: 26
- Vigenère (clave de 4 letras): 456976
- Enigma: 158,962,555,217,826,360,000

Alan Turing

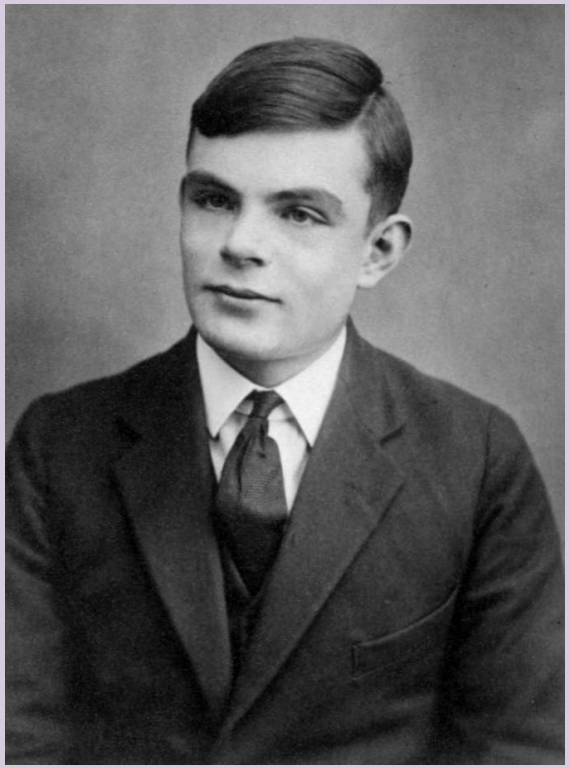
- Durante la Segunda Guerra Mundial, las fuerzas alemanas cifraban mensajes usando la máquina Enigma.

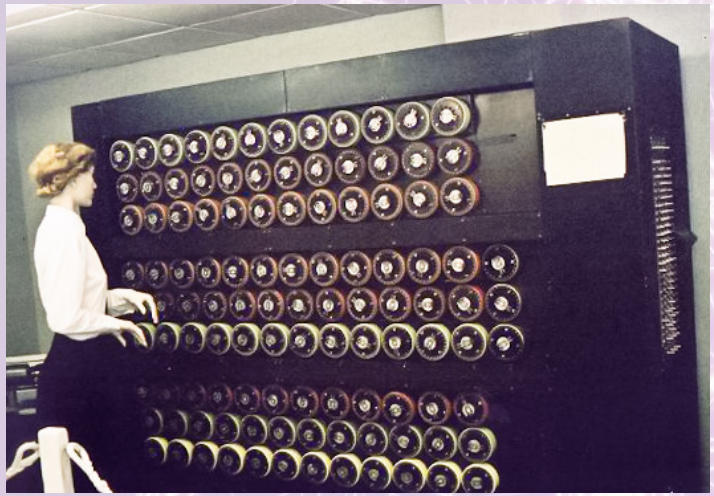
Alan Turing

- Durante la Segunda Guerra Mundial, las fuerzas alemanas cifraban mensajes usando la máquina Enigma.
- El matemático y criptógrafo Alan Turing jugó un rol crucial en la creación de la máquina Bombe, que ayudaba a descifrar los mensajes encriptados con Enigma.

Alan Turing

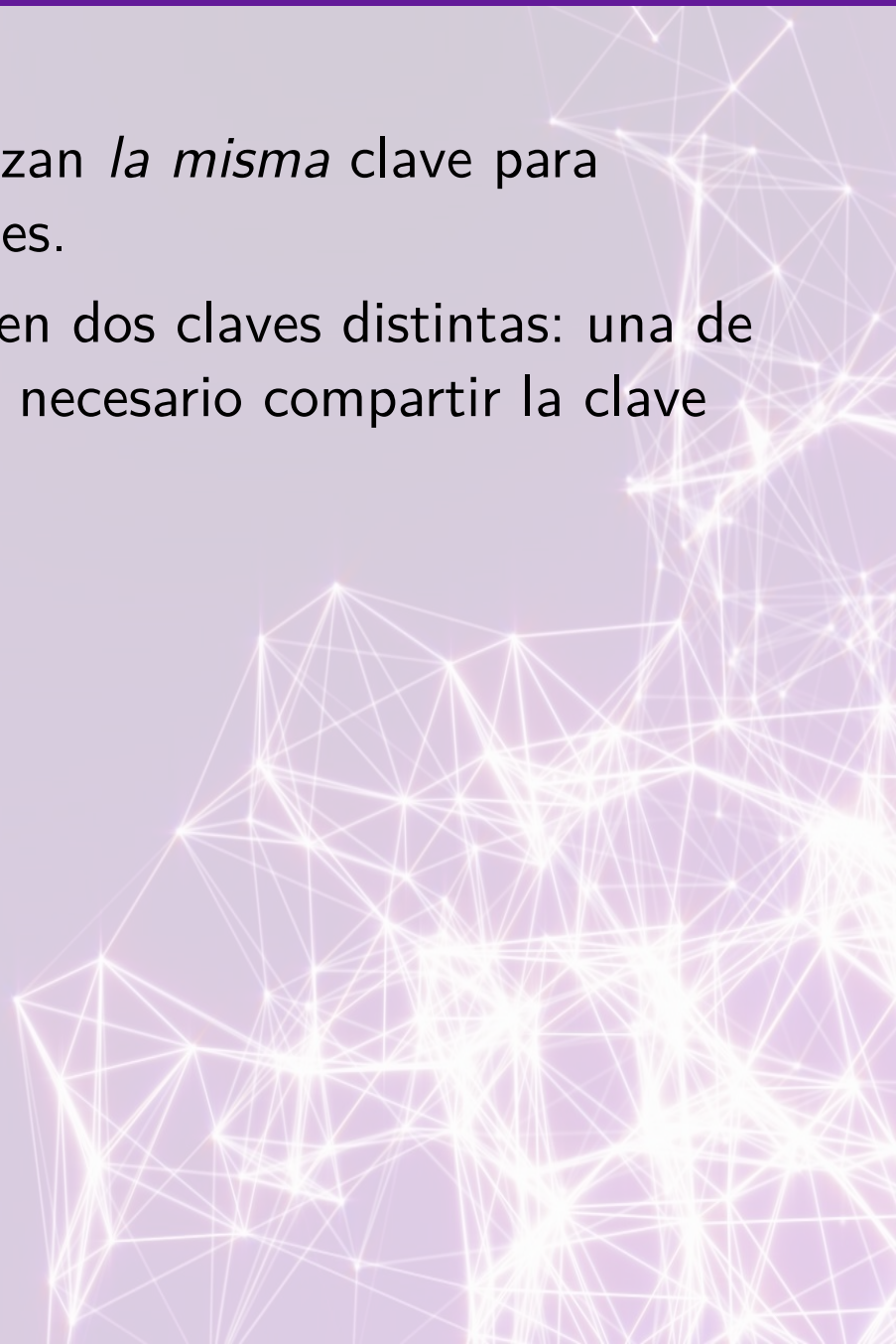
- Durante la Segunda Guerra Mundial, las fuerzas alemanas cifraban mensajes usando la máquina Enigma.
- El matemático y criptógrafo Alan Turing jugó un rol crucial en la creación de la máquina Bombe, que ayudaba a descifrar los mensajes encriptados con Enigma.





Clave pública

- Los cifrados de **clave privada** utilizan *la misma* clave para encriptar y desencriptar los mensajes.
- Los cifrados de **clave pública** tienen dos claves distintas: una de cifrado y otra de descifrado. No es necesario compartir la clave privada con el destinatario.



Clave pública

- Los cifrados de **clave privada** utilizan *la misma* clave para encriptar y desencriptar los mensajes.
- Los cifrados de **clave pública** tienen dos claves distintas: una de cifrado y otra de descifrado. No es necesario compartir la clave privada con el destinatario.

Clave pública

- Los cifrados de **clave privada** utilizan *la misma* clave para encriptar y desencriptar los mensajes.
- Los cifrados de **clave pública** tienen dos claves distintas: una de cifrado y otra de descifrado. No es necesario compartir la clave privada con el destinatario.

Clave pública

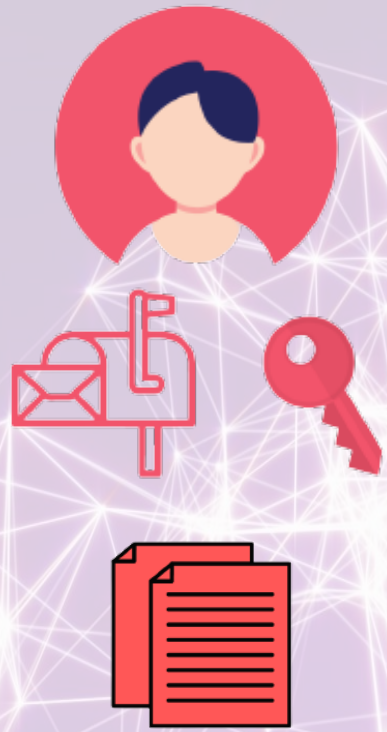
- Los cifrados de **clave privada** utilizan *la misma* clave para encriptar y desencriptar los mensajes.
- Los cifrados de **clave pública** tienen dos claves distintas: una de cifrado y otra de descifrado. No es necesario compartir la clave privada con el destinatario.

Clave pública

- Los cifrados de **clave privada** utilizan *la misma* clave para encriptar y desencriptar los mensajes.
- Los cifrados de **clave pública** tienen dos claves distintas: una de cifrado y otra de descifrado. No es necesario compartir la clave privada con el destinatario.

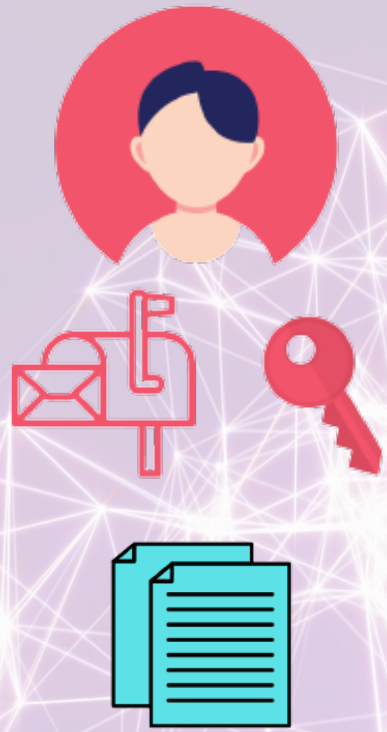
Clave pública

- Los cifrados de **clave privada** utilizan *la misma* clave para encriptar y desencriptar los mensajes.
- Los cifrados de **clave pública** tienen dos claves distintas: una de cifrado y otra de descifrado. No es necesario compartir la clave privada con el destinatario.



Clave pública

- Los cifrados de **clave privada** utilizan *la misma* clave para encriptar y desencriptar los mensajes.
- Los cifrados de **clave pública** tienen dos claves distintas: una de cifrado y otra de descifrado. No es necesario compartir la clave privada con el destinatario.



Funciones trampilla

La generación de las claves de cifrado y descifrado se basa en el uso de las **funciones trampilla**, funciones que son fáciles de calcular pero "*deshacerlas*" es prácticamente imposible.

Funciones trampilla

La generación de las claves de cifrado y descifrado se basa en el uso de las **funciones trampilla**, funciones que son fáciles de calcular pero "*deshacerlas*" es prácticamente imposible.

Idea fundamental

Si conocemos la clave de cifrado debe ser fácil hallar la de descifrado, pero el camino inverso no es computacionalmente factible.

Funciones trampilla

La generación de las claves de cifrado y descifrado se basa en el uso de las **funciones trampilla**, funciones que son fáciles de calcular pero "*deshacerlas*" es prácticamente imposible.

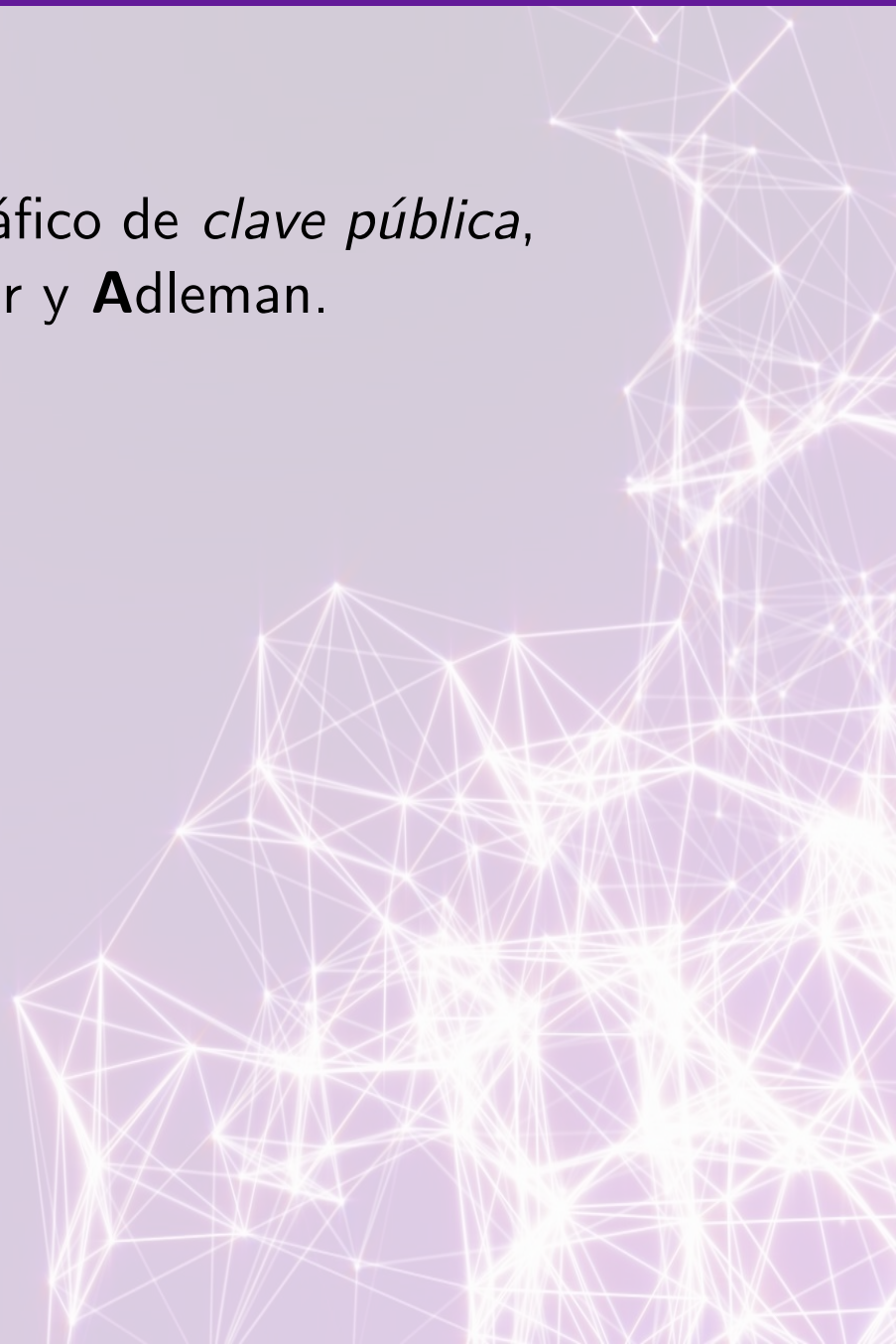
Idea fundamental

Si conocemos la clave de cifrado debe ser fácil hallar la de descifrado, pero el camino inverso no es computacionalmente factible.

Toda la seguridad del cifrado recae en la función trampilla elegida.

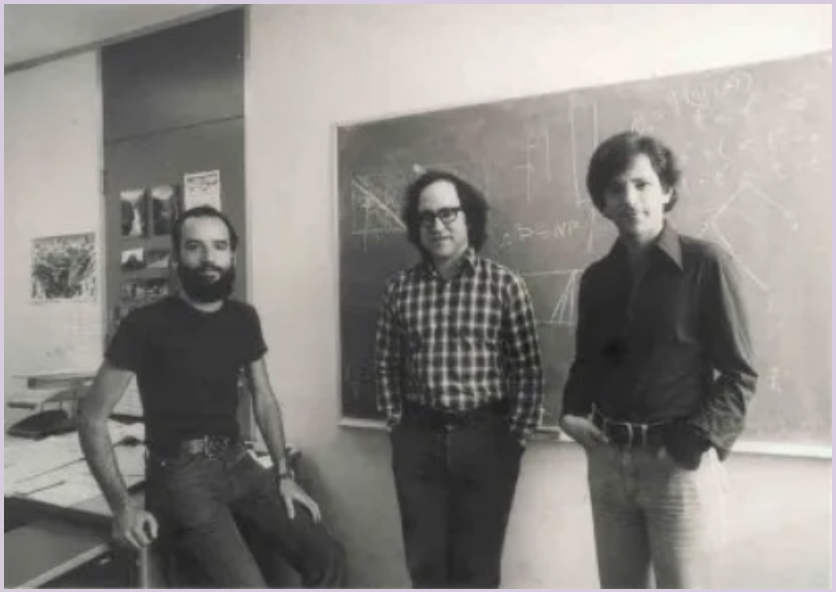
RSA

El **RSA** es el primer protocolo criptográfico de *clave pública*, desarrollado en 1979 por **R**ivest, **S**hamir y **A**dleman.



RSA

El **RSA** es el primer protocolo criptográfico de *clave pública*, desarrollado en 1979 por **R**ivest, **S**hamir y **A**dleman.



En RSA, la función trampilla utilizada para generar las claves es la **factorización**.
La seguridad del RSA reside en que multiplicar dos números primos muy grandes es sencillo, pero factorizar un número (muy grande) en primos sin conocer ningun de sus factores es computacionalmente infactible.

Conclusiones

Conclusiones

- La teoría de números y la criptografía son campos fascinantes en constante evolución. Ningún descubrimiento es en vano.

Conclusiones

- La teoría de números y la criptografía son campos fascinantes en constante evolución. Ningún descubrimiento es en vano.
- En general, las matemáticas no son sobre memorizar fórmulas o ecuaciones. Ser creativo y curioso es mucho más importante: hacerse preguntas y plantear problemas es lo que permite que la ciencia avance.

Conclusiones

- La teoría de números y la criptografía son campos fascinantes en constante evolución. Ningún descubrimiento es en vano.
- En general, las matemáticas no son sobre memorizar fórmulas o ecuaciones. Ser creativo y curioso es mucho más importante: hacerse preguntas y plantear problemas es lo que permite que la ciencia avance.
- Todo el mundo puede hacer matemáticas, y debemos luchar para crear y mantener un ambiente inclusivo sin discriminaciones.

Conclusiones

- La teoría de números y la criptografía son campos fascinantes en constante evolución. Ningún descubrimiento es en vano.
- En general, las matemáticas no son sobre memorizar fórmulas o ecuaciones. Ser creativo y curioso es mucho más importante: hacerse preguntas y plantear problemas es lo que permite que la ciencia avance.
- Todo el mundo puede hacer matemáticas, y debemos luchar para crear y mantener un ambiente inclusivo sin discriminaciones.

"A veces la persona que nadie imagina capaz de nada es la que hace cosas que nadie imagina." - Alan Turing

Conclusiones

- La teoría de números y la criptografía son campos fascinantes en constante evolución. Ningún descubrimiento es en vano.
- En general, las matemáticas no son sobre memorizar fórmulas o ecuaciones. Ser creativo y curioso es mucho más importante: hacerse preguntas y plantear problemas es lo que permite que la ciencia avance.
- Todo el mundo puede hacer matemáticas, y debemos luchar para crear y mantener un ambiente inclusivo sin discriminaciones.

"A veces la persona que nadie imagina capaz de nada es la que hace cosas que nadie imagina." - Alan Turing

Muchas gracias!!!