Qui vol guanyar 1 000 000 $?

Berenguer Sabadell i Noguera
Institut Santa Eugènia, Girona
Escola Politècnica Superior-UdG
berenguer.sabadell@udg.edu

$2^2 \cdot 5$ / $2 \cdot 5$ / $2 \cdot 3 \cdot 337$
(293è dia de l'any)

Universitat de Girona
Càtedra Lluís A. Santaló d'Aplicacions de la Matemàtica

Els set problemes del mil·lenni

Maig 2000, College de France, Paris
The Clay Mathematics Institute, Cambridge (Massachusetts)

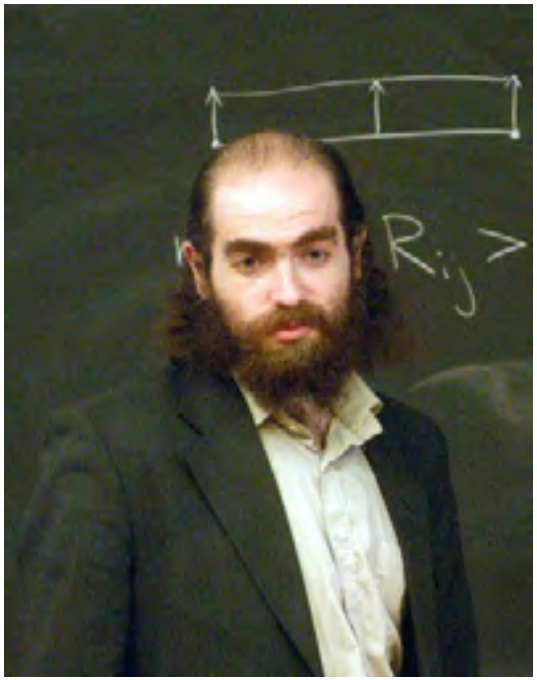
- ***Teoria quàntica de Yang i Mills.***
- ***La hipòtesi de Riemann.***
- ***P versus NP.***
- ***Equacions de Navier-Stokes.***
- ***La conjectura de Hodge.***
- ***La conjectura de Poincaré.***
- ***La conjectura de Birch i Swinnerton-Dyer.***

Universitat de Girona
Càtedra Lluís A. Santaló d'Aplicacions de la Matemàtica

Els set problemes del mil·lenni

Maig 2000, College de France, Paris
The Clay Mathematics Institute, Cambridge (Massachusetts)

- *Teoria quàntica de Yang i Mills.*
- *La hipòtesi de Riemann.*
- *P versus NP.*
- *Equacions de Navier-Stokes.*
- *La conjectura de Hodge.*
- ***La conjectura de Poincaré.***
- *La conjectura de Birch i Swinnerton-Dyer.*



Grigoriu Perelman
(1966-)

Universitat de Girona
Càtedra Lluís A. Santaló d'Aplicacions de la Matemàtica

Els set problemes del mil·lenni

Maig 2000, College de France, Paris
The Clay Mathematics Institute, Cambridge (Massachusetts)

- *Teoria quàntica de Yang i Mills.*
- ***La hipòtesi de Riemann.***
- *P versus NP.*
- *Equacions de Navier-Stokes.*
- *La conjectura de Hodge.*
- *La conjectura de Poincaré.*
- *La conjectura de Birch i Swinnerton-Dyer.*

Bernhard Riemann
(1826-1866)

Universitat de Girona
Càtedra Lluís A. Santaló d'Aplicacions de la Matemàtica

La hipòtesi de Riemann (RH)

Donada la funció

$$\zeta(s) = \sum_{n=1}^{+\infty} n^{-s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots \ , \quad \text{amb } s \in \mathbb{C} \setminus \{1\} \ .$$

Exemple: $\zeta(2) = 1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \cdots = \frac{\pi^2}{6}$

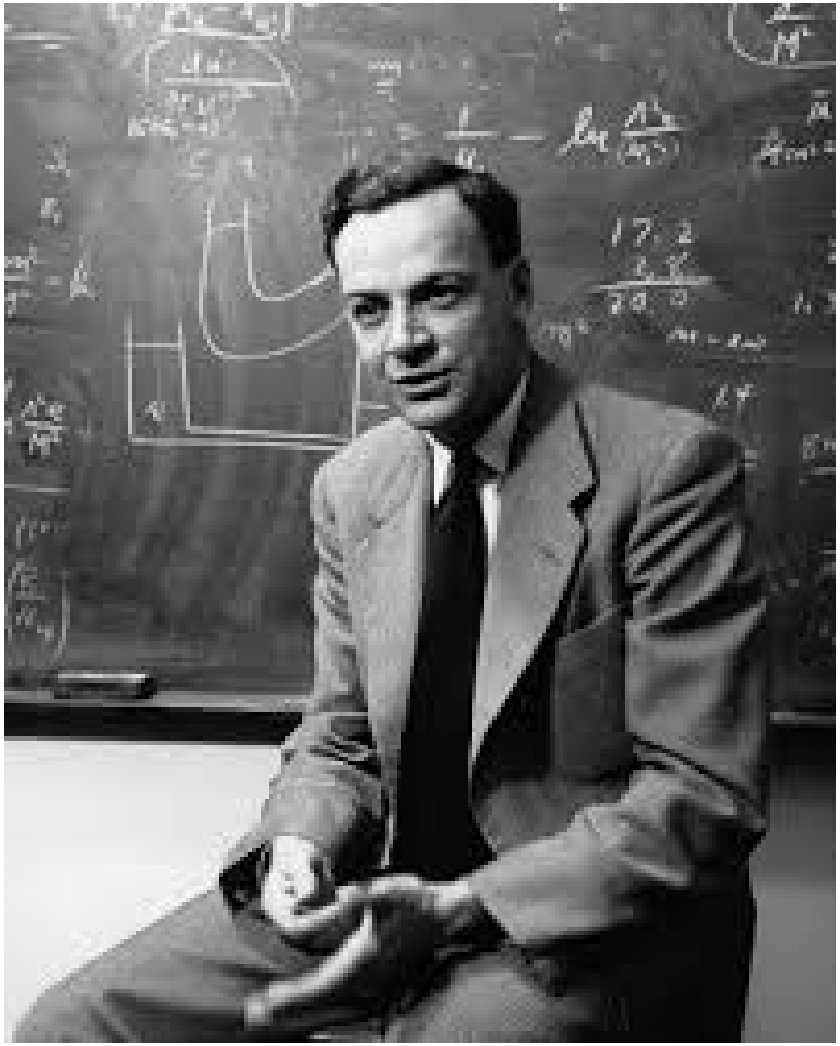
Demostreu que tots els zeros no trivials de $\zeta(s)$ compleixen:

$$\mathrm{Re}(s) = \frac{1}{2} \ .$$

És a dir,

$$\text{si} \quad \zeta(s) = 0 \ \Rightarrow \ \begin{cases} s = -2n \ , \ n \in \mathbb{N} \\ \mathrm{Re}(s) = 1/2 \end{cases}$$

Principi de Richard Feynmann



Premi Nobel de Física (1965)

"pel seu treball fonamental en electrodinàmica quàntica, amb profundes conseqüències per a la física de les partícules elementals"

P: *"Ens pot explicar en cinc minuts perquè li han donat el premi Nobel de Física?"*

R: *"Si ho pogués explicar en cinc minuts, no hauria valgut el premi Nobel."*

Universitat de Girona
Càtedra Lluís A. Santaló d'Aplicacions de la Matemàtica

Nombres primers i nombres compostos

Nombres naturals: $\mathbb{N} = \{1, 2, 3, 4, 5, ...\}$

$$24 = 1 \cdot 24 = 2 \cdot 12 = 3 \cdot 8 = 4 \cdot 6 \;\Rightarrow\; \boxed{24 \textbf{ és compost}}$$

$$17 = 1 \cdot 17 \;\Rightarrow\; \boxed{17 \textbf{ és primer}}$$

$$\mathbb{N} = 1 \cup \{\textsc{Primers}\} \cup \{\textsc{Compostos}\}$$

$$\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, 19, ...\}$$

Primera pregunta ⚠ : **Per què són tan importants?**

Girona
Càtedra Lluís A. Santaló
d'Aplicacions
de la Matemàtica

Teorema Fonamental de l'Aritmètica

Euclides. *"Elements"*, llibre VII, proposició 30

Qualsevol nombre natural $n > 1$ es pot representar com a **producte de factors primers de manera única** (llevat de l'ordre dels factors).

Exemple

$$24 = 2 \cdot 12 = 2 \cdot 2 \cdot 6 = 2 \cdot 2 \cdot 2 \cdot 3$$

$$24 = 3 \cdot 8 = 3 \cdot 2 \cdot 4 = 3 \cdot 2 \cdot 2 \cdot 2$$

$$24 = 4 \cdot 6 = 2 \cdot 2 \cdot 2 \cdot 3$$

$$\longrightarrow \boxed{24 = 2^3 \cdot 3}$$

Els nombres primers són els àtoms de l'Aritmètica!

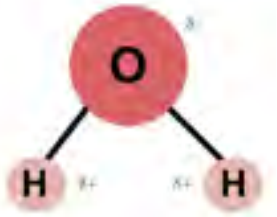
Girona
Càtedra Lluís A. Santaló d'Aplicacions de la Matemàtica

Els àtoms de l'Aritmètica

Taula periòdica dels elements químics

H																	He
Li	Be											B	C	N	O	F	Ne
Na	Mg											Al	Si	P	S	Cl	Ar
K	Ca	Sc	Ti	V	Cr	Mn	Fe	Co	Ni	Cu	Zn	Ga	Ge	As	Se	Br	Kr
Rb	Sr	Y	Zr	Nb	Mo	Tc	Ru	Rh	Pd	Ag	Cd	In	Sn	Sb	Te	I	Xe
Cs	Ba	La-Lu	Hf	Ta	W	Re	Os	Ir	Pt	Au	Hg	Tl	Pb	Bi	Po	At	Rn
Fr	Ra	Ac-Lr	Rf	Db	Sg	Bh	Hs	Mt	Ds	Rg	Cn	Nh	Fl	Mc	Lv	Ts	Og
		La	Ce	Pr	Nd	Pm	Sm	Eu	Gd	Tb	Dy	La	Ho	Er	Yb	Lu	
		Ac	Th	Pa	U	Np	Pu	Am	Cm	Bk	Cf	Es	Fm	Md	No	Lr	

Molècula d'aigua: H_2O



Universitat de Girona
Càtedra Lluís A. Santaló d'Aplicacions de la Matemàtica

Taula ~~periòdica~~ dels nombres primers

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 ↓ 353	359	367	373	379	383	389	397	401	409	419	421	431	433	439	443
449	457	461 ↓ 563	569	571	577	587	593	599	601	607	613	617	619	631	641	643	$\cdots$
		269	271	277	281	283	293	307	311	313	317	331	337	347	349	353	
		461	463	467	479	487	491	499	503	509	521	523	541	547	557	563	

"molècula d'aigua matemàtica": $2^2 \cdot 19 = 76$

$$420 = 2^2 \cdot 3 \cdot 5 \cdot 7$$

~~HHe~~ : $2 \cdot 3 = 6$

Universitat de Girona
Càtedra Lluís A. Santaló d'Aplicacions de la Matemàtica

Quants nombres primers hi ha?

Euclides. *"Elements"*, llibre IX, proposició 20

El conjunt $\mathbb{P}$ dels nombres primers és infinit.

Demostració *(reducció a l'absurd)*

Suposem que el conjunt $\mathbb{P}$ és finit: $\mathbb{P} = \{2, 3, 5, ..., p_N\}$

Construïm el següent nombre natural: $A = 2 \cdot 3 \cdot 5 \cdots p_N + 1$

Si A és primer, ja tenim la contradicció!

Si A és compost, factoritza com a producte de primers.
Però **cap** dels elements de $\mathbb{P}$ divideix A
(El residu de la divisió entera de A per cada element de $\mathbb{P}$ és 1).
Per tant, els factors primers de A **no són** de $\mathbb{P}$. $\square$

Exemple

Si $\mathbb{P} = \{2, 3, 5, 7, 11, 13\}$, aleshores:

$$A = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30\,031 = 59 \cdot 509$$

Nombres primerials (apunt tècnic)

$$\#p_n = 2 \cdot 3 \cdot 5 \cdot 7 \cdots p_n \;\rightarrow\; \text{nombre } \textit{primerial}$$

n	$\mathbb{P}$	$\#p_n + 1$	Factorització
1	$\{2\}$	3	3 (primer)
2	$\{2,3\}$	7	7 (primer)
3	$\{2,3,5\}$	31	31 (primer)
4	$\{2,3,5,7\}$	211	211 (primer)
5	$\{2,3,5,7,11\}$	2311	2311 (primer)
6	$\{2,3,5,7,11,13\}$	30 031	$59 \cdot 509$
7	$\{2,3,5,7,11,13,17\}$	510 511	$19 \cdot 97 \cdot 277$

Si $p < 100\,000$, $\#p + 1$ és primer quan:

$p \in \{2, 3, 5, 7, 11, 31, 379, 1019, 11021, 2657, 3229, 4547, 4787, 11\,549,$
$13\,649, 18\,523, 23\,801, 24\,029, 42\,209\}$ (19 primers de 9592!)

Universitat de Girona
Càtedra Lluís A. Santaló d'Aplicacions de la Matemàtica

Magicicada septendecim i *Magicicada tredecim*

Magicicada septendecim (17)

Magicicada tredecim (13)

Dues teories:

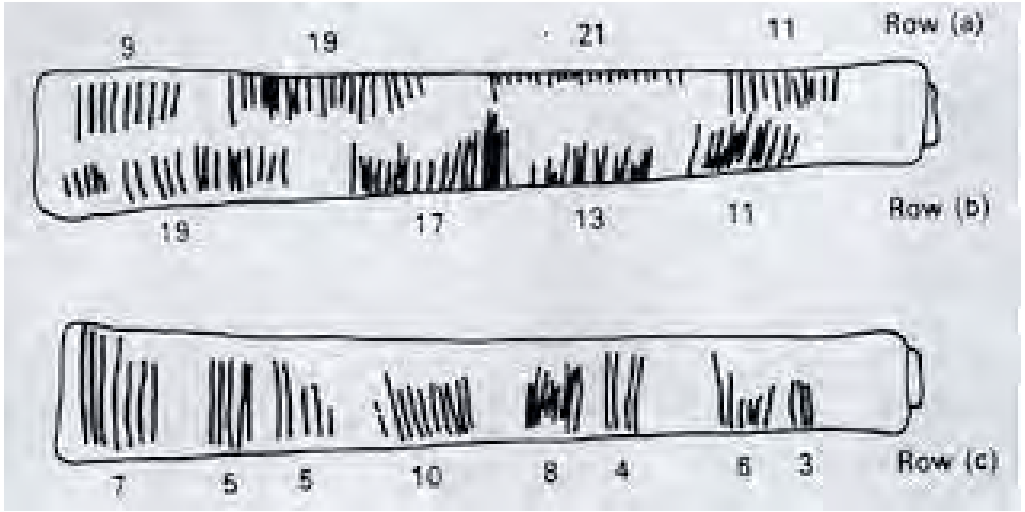
- Escapar dels depredadors amb cicles de vida inferiors.
- Evitar generar espècies híbrides.

Preguntes sense respondre (etòlegs)

- Perquè altres espècies de cigales no han seguit la mateixa estratègia?
- Què tenen d'especial el 13 i el 17?

Universitat de Girona
Càtedra Lluís A. Santaló d'Aplicacions de la Matemàtica

L'os d'Ishango, 20 000 aC (J.H. Braucourt, 1950)



Universitat de Girona
Càtedra Lluís A. Santaló
d'Aplicacions
de la Matemàtica

Localització de nombres primers

Sedàs d'Eratòstenes

	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	70
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
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130

Universitat de Girona
Càtedra Lluís A. Santaló
d'Aplicacions
de la Matemàtica

Localització de nombres primers

Sedàs d'Eratòstenes

	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	70
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
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130

Universitat de Girona
Càtedra Lluís A. Santaló
d'Aplicacions
de la Matemàtica

Localització de nombres primers

Sedàs d'Eratòstenes

	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	~~70~~
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~~
101	~~102~~	103	~~104~~	105	~~106~~	107	~~108~~	109	~~110~~
111	~~112~~	113	~~114~~	115	~~116~~	117	~~118~~	119	~~120~~
121	~~122~~	123	~~124~~	125	~~126~~	127	~~128~~	129	~~130~~

Universitat de Girona
Càtedra Lluís A. Santaló d'Aplicacions de la Matemàtica

Localització de nombres primers

Sedàs d'Eratòstenes

	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	~~70~~
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~~
101	~~102~~	103	~~104~~	105	~~106~~	107	~~108~~	109	~~110~~
111	~~112~~	113	~~114~~	115	~~116~~	117	~~118~~	119	~~120~~
121	~~122~~	123	~~124~~	125	~~126~~	127	~~128~~	129	~~130~~

Universitat de Girona
Càtedra Lluís A. Santaló d'Aplicacions de la Matemàtica

Localització de nombres primers

Sedàs d'Eratòstenes

	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~~	~~70~~
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~~
101	~~102~~	103	~~104~~	~~105~~	~~106~~	107	~~108~~	109	~~110~~
~~111~~	~~112~~	113	~~114~~	115	~~116~~	~~117~~	~~118~~	119	~~120~~
121	~~122~~	~~123~~	~~124~~	125	~~126~~	127	~~128~~	~~129~~	~~130~~

Universitat de Girona
Càtedra Lluís A. Santaló d'Aplicacions de la Matemàtica

Localització de nombres primers

Sedàs d'Eratòstenes

	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~~	~~70~~
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~~
101	~~102~~	103	~~104~~	~~105~~	~~106~~	107	~~108~~	109	~~110~~
~~111~~	~~112~~	113	~~114~~	~~115~~	~~116~~	~~117~~	~~118~~	119	~~120~~
121	~~122~~	~~123~~	~~124~~	~~125~~	~~126~~	127	~~128~~	~~129~~	~~130~~

Universitat de Girona
Càtedra Lluís A. Santaló d'Aplicacions de la Matemàtica

Localització de nombres primers

Sedàs d'Eratòstenes

	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~~	~~70~~
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~~
101	~~102~~	103	~~104~~	~~105~~	~~106~~	107	~~108~~	109	~~110~~
~~111~~	~~112~~	113	~~114~~	~~115~~	~~116~~	~~117~~	~~118~~	~~119~~	~~120~~
121	~~122~~	~~123~~	~~124~~	~~125~~	~~126~~	127	~~128~~	~~129~~	~~130~~

Universitat de Girona
Càtedra Lluís A. Santaló d'Aplicacions de la Matemàtica

Localització de nombres primers

Sedàs d'Eratòstenes

	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~~	~~70~~
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~~
101	~~102~~	103	~~104~~	~~105~~	~~106~~	107	~~108~~	109	~~110~~
~~111~~	~~112~~	113	~~114~~	~~115~~	~~116~~	~~117~~	~~118~~	~~119~~	~~120~~
~~121~~	~~122~~	~~123~~	~~124~~	~~125~~	~~126~~	127	~~128~~	~~129~~	~~130~~

Universitat de Girona
Càtedra Lluís A. Santaló d'Aplicacions de la Matemàtica

Localització de nombres primers

Sedàs d'Eratòstenes

	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~~	~~70~~
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~~
101	~~102~~	**103**	~~104~~	~~105~~	~~106~~	**107**	~~108~~	**109**	~~110~~
~~111~~	~~112~~	**113**	~~114~~	~~115~~	~~116~~	~~117~~	~~118~~	~~119~~	~~120~~
~~121~~	~~122~~	~~123~~	~~124~~	~~125~~	~~126~~	**127**	~~128~~	~~129~~	~~130~~

Universitat de Girona
Càtedra Lluís A. Santaló
Aplicacions
de la Matemàtica

Forats grans, forats petits ...

- $p_{31\,545} = 370\,261$ ve seguit de 111 nombres compostos.
- No existeix cap nombre primer entre 20 831 323 i 20 831 533.
- Si volem 1000 nombres consecutius compostos, fem:

$$A = 1 \cdot 2 \cdot 3 \cdots 1001$$

$$\Rightarrow \; A + N \,, \quad N = 2, 3, ..., 1001 \text{ es poden dividir per } N.$$

- ***Primers bessons***: (3,5), (5,7), (11,13), (17,19), ... (197,199), ... (48 647, 48 649), ...

$$2\,996\,863\,034\,895 \cdot 2^{1\,290\,000} \pm 1 \quad (09/2016)$$

té 388 342 dígits decimals (*Twin Prime Search-Prime Grid*)

- Hi ha 808 675 888 577 436 parelles primers bessons $< 10^{18}$.

Conjectura dels primers bessons (James Maynard, Terence Tao)

Hi ha infinites parelles de primers bessons.

Tres qüestions importants

1. Donat $N \in \mathbb{N}$, és primer o és compost?
2. Fixat $N \in \mathbb{N}$, quants primers hi ha per sota N?
3. Fixat $k \in \mathbb{N}$, qui és el primer p_k?

(Fàcil)

1. $N = 2021$ és primer? No. Falla la divisió $2021 \div 43 = 47$.
2. Quants primers hi ha per sota 10 000? N'hi ha 1229.
3. Qui és p_{2022} ? $p_{2022} = 17\,581$.

(Difícil)

1. $N = 456\,984\,127\,154\,789\,612\,654\,783\,695\,477$ és primer?
   No. $N = 424\,093 \cdot 1\,077\,556\,401\,908\,990\,746\,498\,489$.
2. Quants primers hi ha per sota 10^{100}?
3. Qui és p_k si $k = 10^{50}$?

Universitat de Girona
Càtedra Lluís A. Santaló d'Aplicacions de la Matemàtica

A la recerca d'un patró

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59 ...

Leonhard Euler
(1707-1783)

- $p(x) = x^2 - x + 41$, $x = 0, 1, 2...40$.
- $p(x) = x^2 - 79x + 1601$, $x = 0, 1, 2...79$.
- $\exists$ infinits primers $4n + 3$.
- Quants primers $4n + 1$?
- $\zeta(2) = \pi^2/6,\ \zeta(4) = \pi^4/90,\ \ldots$

"Els matemàtics han intentat en va fins el dia d'avui descobrir una mica d'ordre en la successió dels nombres primers, i tenim raons per creure que és un misteri on la ment humana no hi podrà penetrar mai."

Universitat de Girona
Càtedra Lluís A. Santaló d'Aplicacions de la Matemàtica

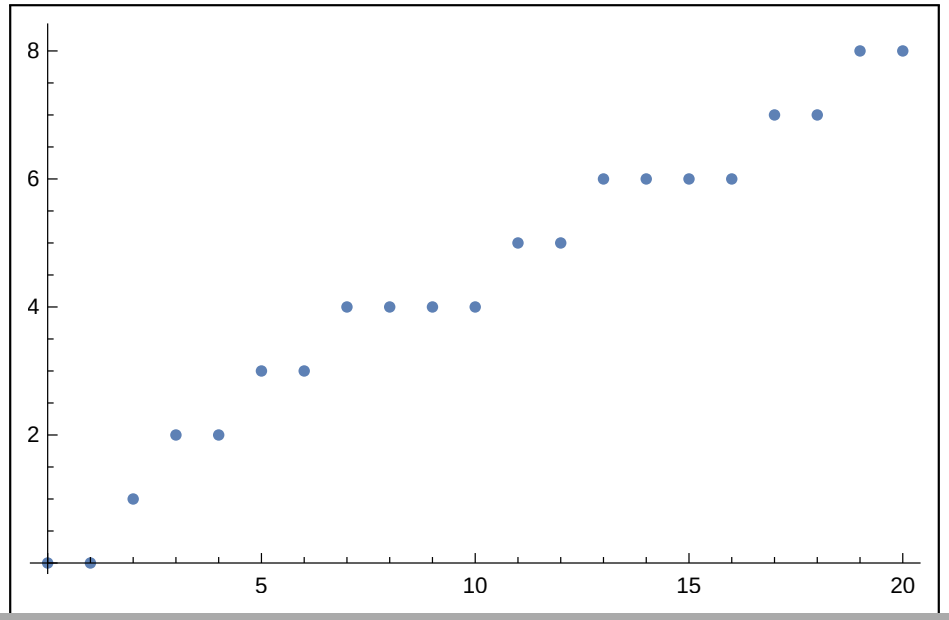
Canvi d'orientació

⚠ **Com estan distribuïts els nombres primers?**

$$\pi(x) = \#\{1 < p \leq x \ / \ p \text{ primer}\} \quad , \ \forall x \geq 0$$

x	0	1	2	3	4	5	6	7	8	9	10	11
$\pi(x)$	0	0	1	2	2	3	3	4	4	4	4	5

x	12	13	14	15	16	17	18	19	20	21	22	23
$\pi(x)$	5	6	6	6	6	7	7	8	8	8	8	9



Universitat de Girona
Càtedra Lluís A. Santaló d'Aplicacions de la Matemàtica

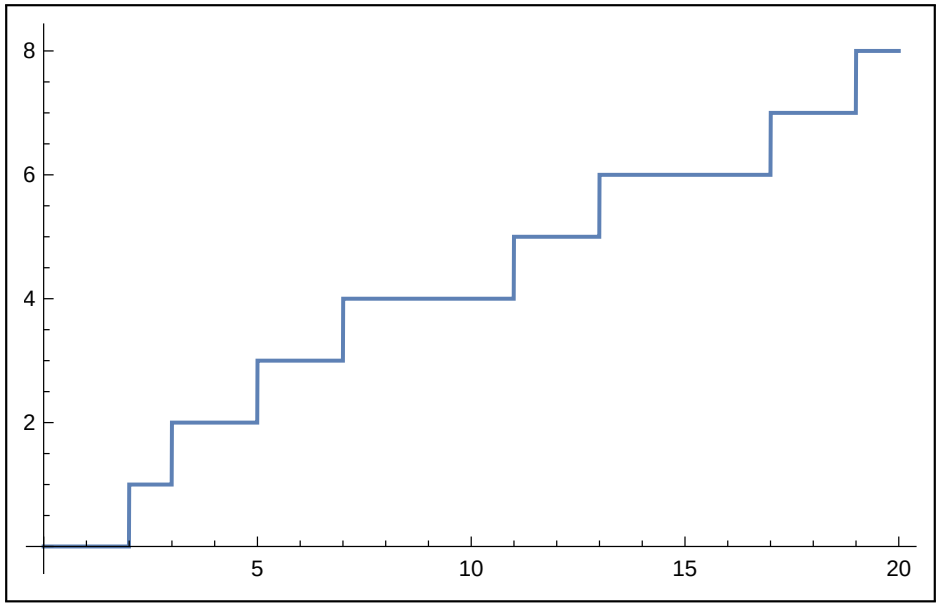
Canvi d'orientació

⚠ **Com estan distribuïts els nombres primers?**

$$\pi(x) = \#\{1 < p \leq x \ / \ p \text{ primer}\} \quad , \ \forall x \geq 0$$

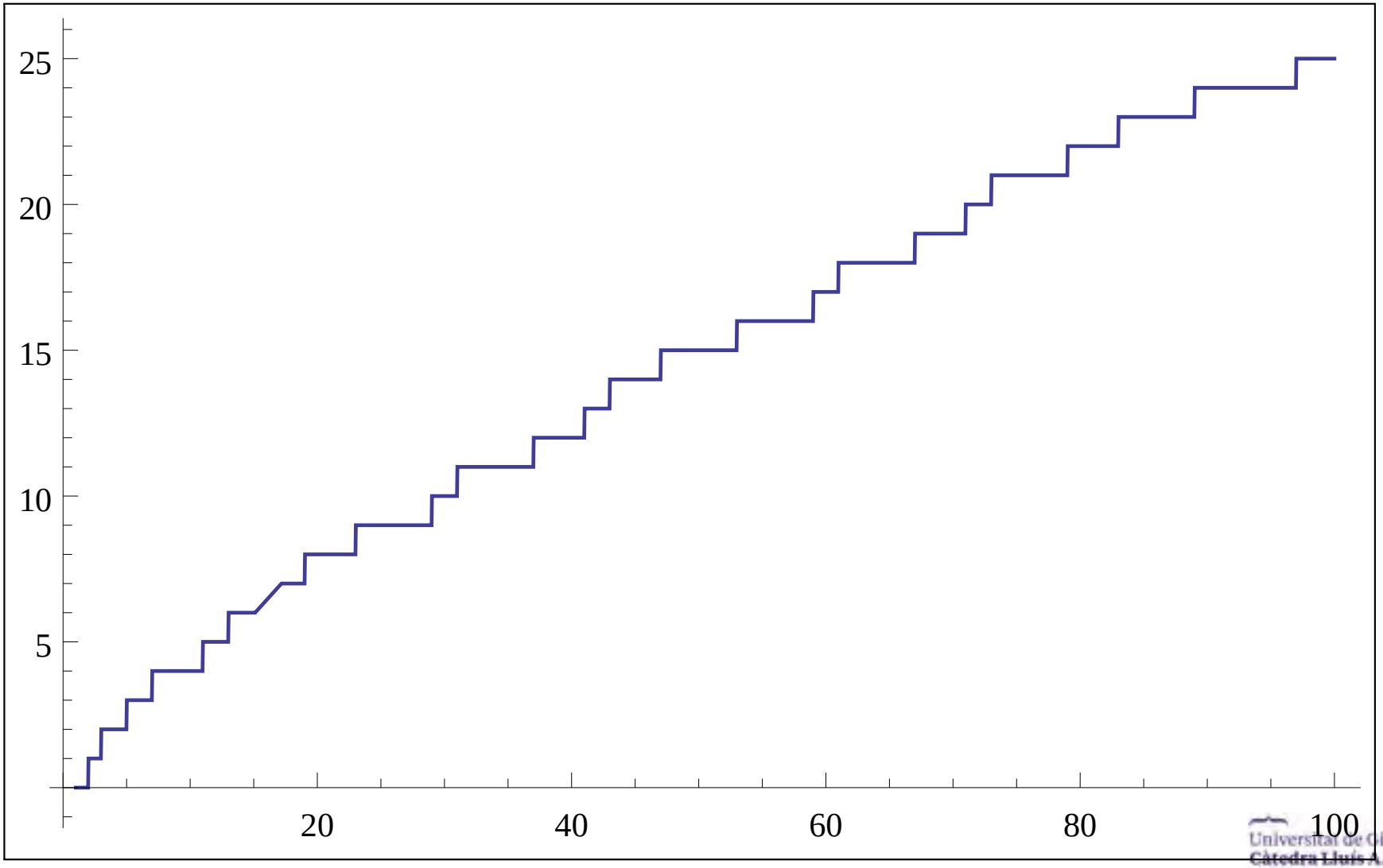
x	0	1	2	3	4	5	6	7	8	9	10	11
$\pi(x)$	0	0	1	2	2	3	3	4	4	4	4	5

x	12	13	14	15	16	17	18	19	20	21	22	23
$\pi(x)$	5	6	6	6	6	7	7	8	8	8	8	9



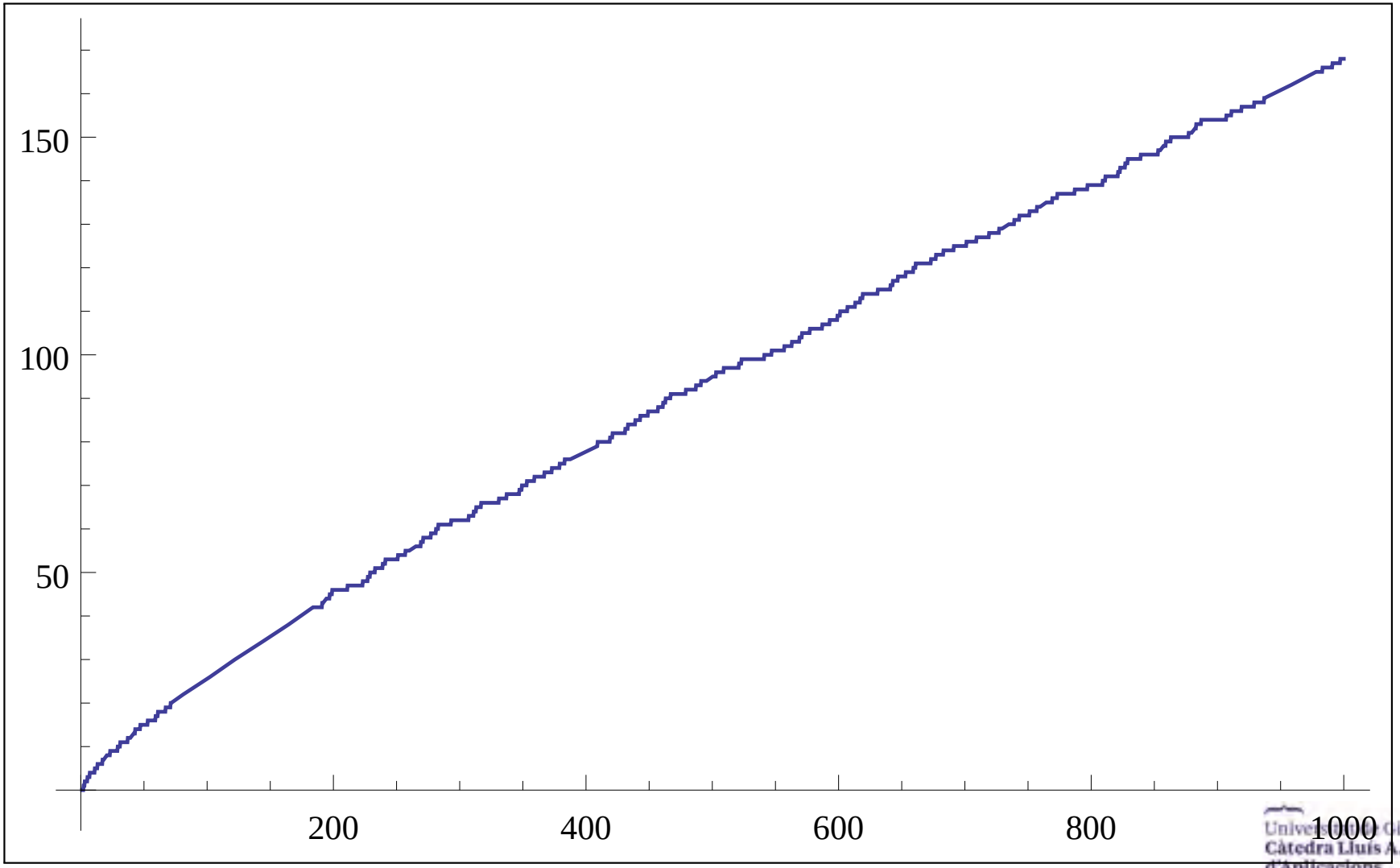
Universitat de Girona
Càtedra Lluís A. Santaló d'Aplicacions de la Matemàtica

Comportament de $\pi(x)$



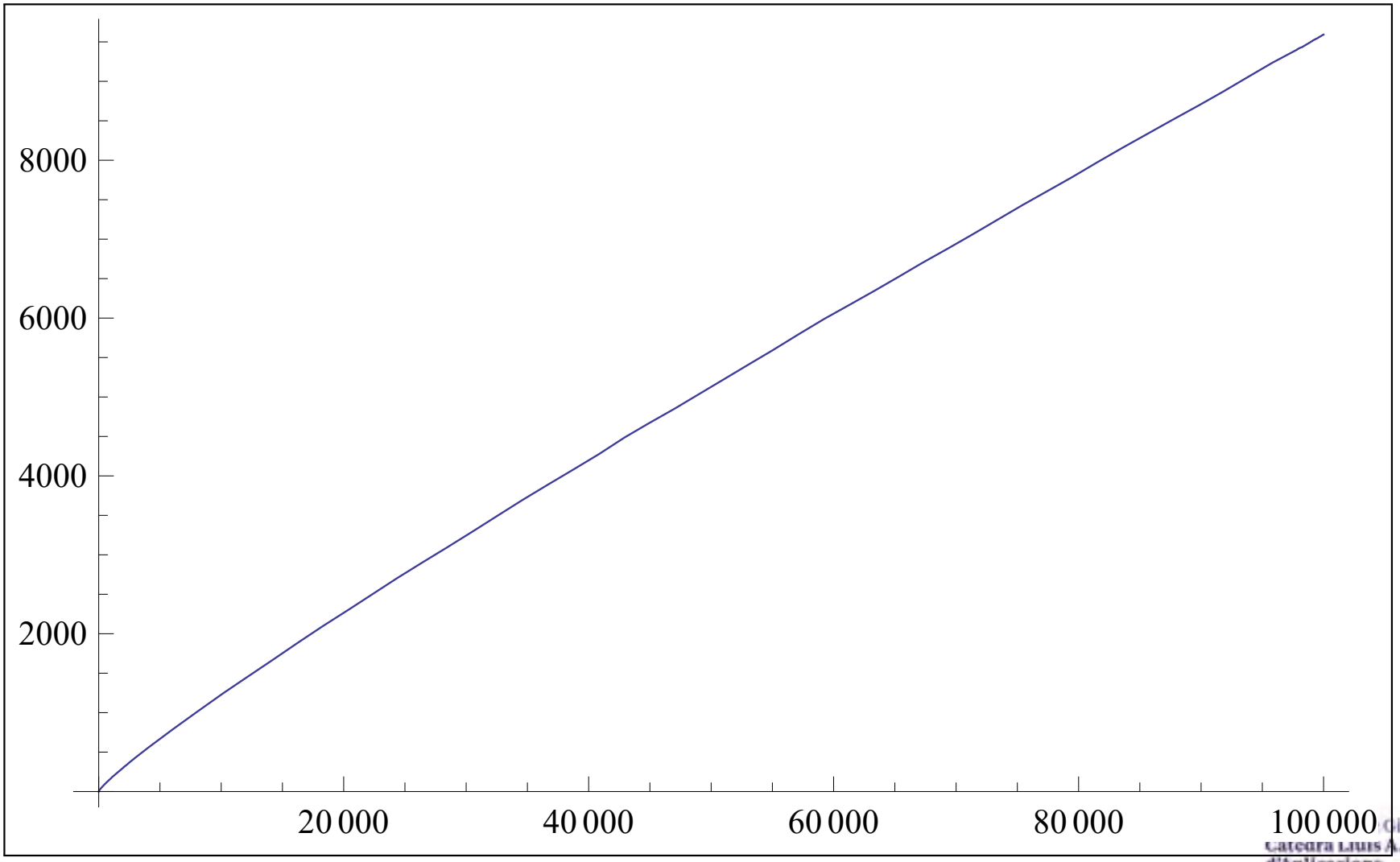
Universitat de Girona
Càtedra Lluís A. Santaló
d'Aplicacions
de la Matemàtica

Comportament de $\pi(x)$



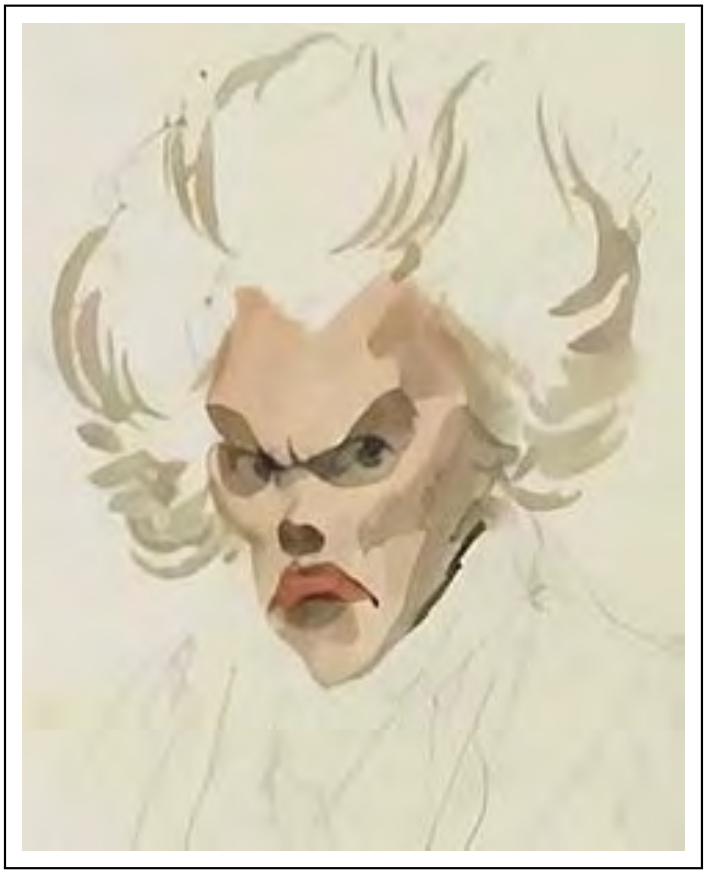
Universitat de Girona
Càtedra Lluís A. Santaló
d'Aplicacions
de la Matemàtica

Comportament de $\pi(x)$



Girona
Càtedra Lluís A. Santaló
d'Aplicacions
de la Matemàtica

Aproximació de Legendre



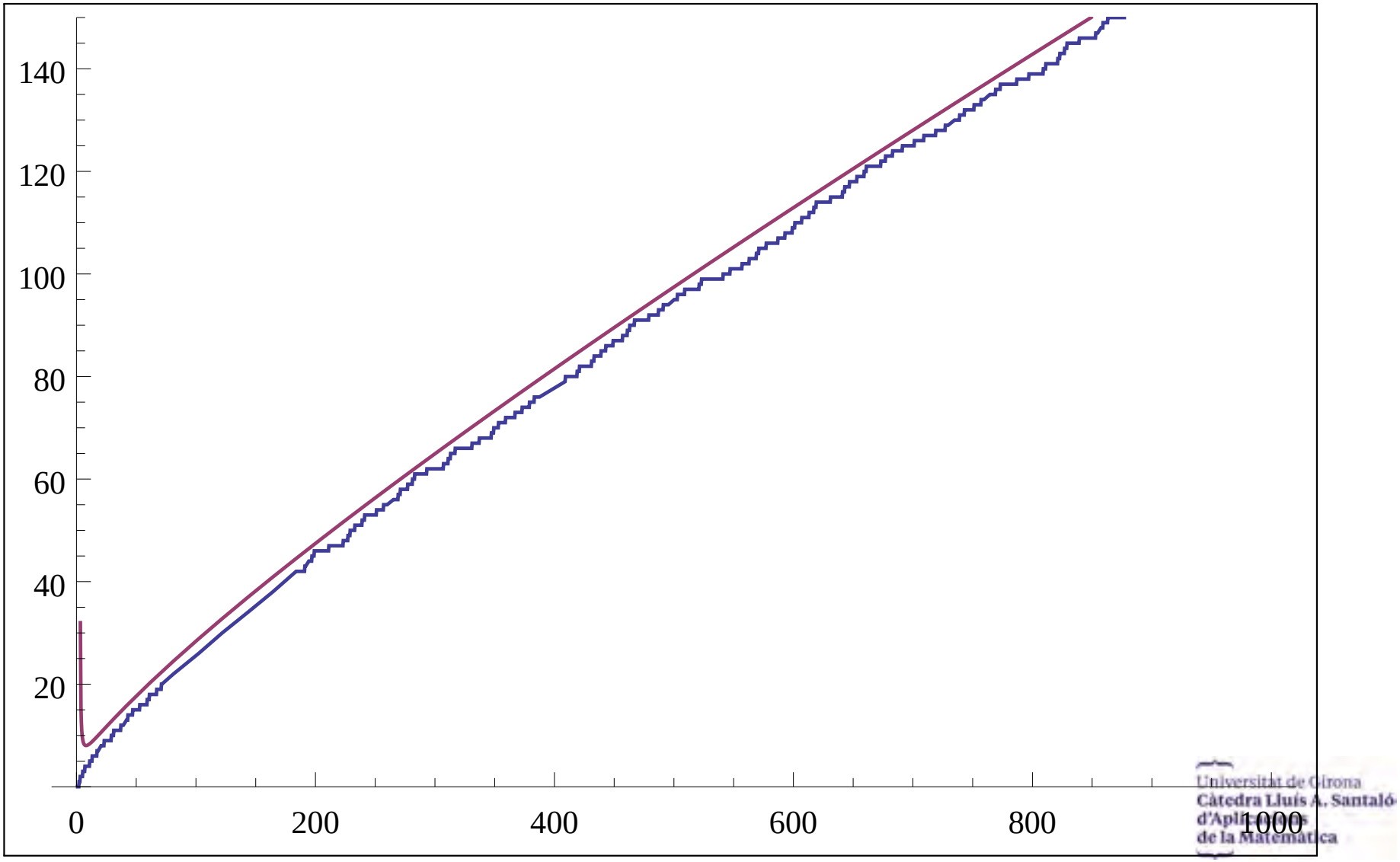
$$\pi(x) \approx F(x) = \frac{x}{\log x - 1.08366}$$

"Essai sur la théorie des nombres" (1808)

Adrien-Marie Legendre
(1752-1833)

Universitat de Girona
Càtedra Lluís A. Santaló d'Aplicacions de la Matemàtica

Aproximació de Legendre



Aproximacions de Gauss

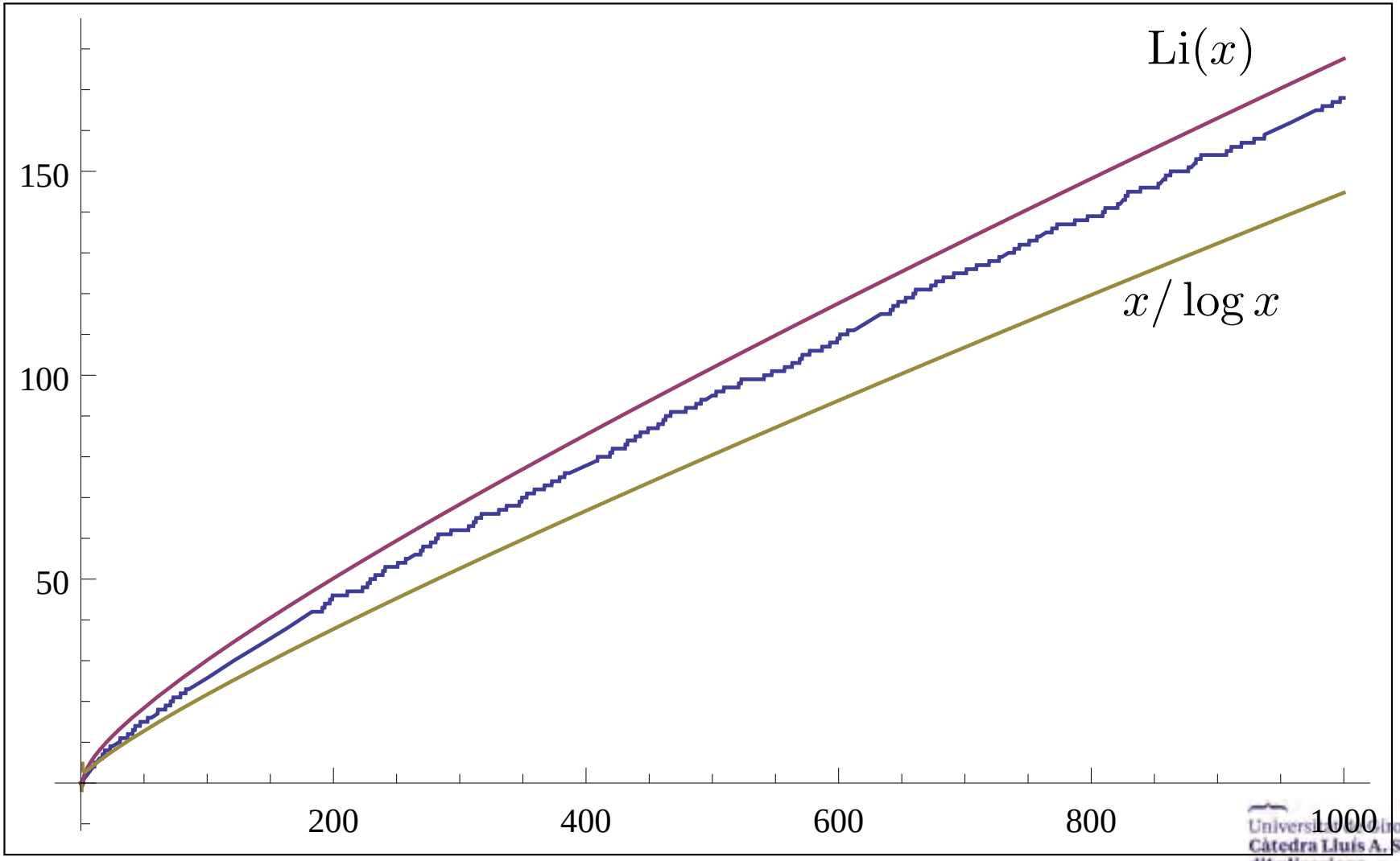
Carl Friedrich Gauss
(1777-1855)

$$\pi(x) \approx \frac{x}{\log x} \quad (\sim 1793)$$

$$\pi(x) \approx \mathrm{Li}(x) = \int_2^x \frac{dt}{\log t} \quad (\sim 1832)$$

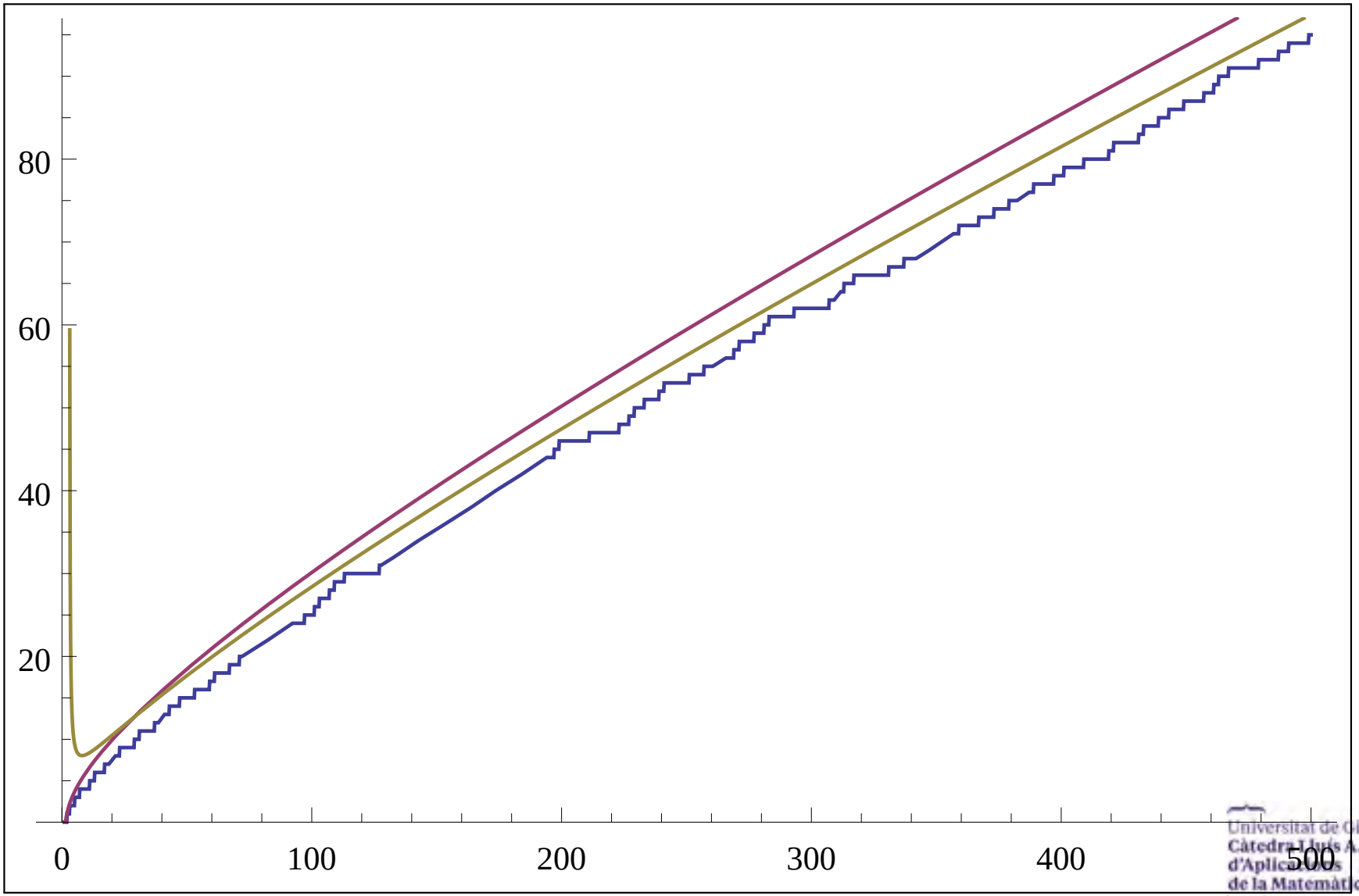
Universitat de Girona
Càtedra Lluís A. Santaló
d'Aplicacions
de la Matemàtica

Aproximacions de Gauss



Universitat de Girona
Càtedra Lluís A. Santaló
d'Aplicacions
de la Matemàtica

Gauss *versus* Legendre



Gauss *versus* Legendre

x	$\pi(x)$	$F(x)$	$\mathrm{Er}(F(x))(\%)$	$\mathrm{Li}(x)$	$\mathrm{Er}(\mathrm{Li}(x))(\%)$
10^2	25	28.3969	13.59	30.1261	20.5
10^3	168	171.7005	2.2026	177.61	5.72
10^4	1229	1230.5147	0.123247	1246.14	1.39463
10^5	9592	9588.403	-0.0375	9629.81	0.394183
10^6	78 498	78 543.2	0.057581	78 627.5	0.164972
10^7	664 579	665 139.7	0.084369	664 918.	0.05101
10^8	5 761 455	5.768×10^6	0.1136	5.762×10^6	0.013104
10^9	50 847 534	5.092×10^7	0.1376	5.084×10^7	0.003276
10^{10}	455 052 511	4.557×10^8	0.151738	4.551×10^8	0.000767
10^{11}	4 118 054 813	4.125×10^9	0.158939	4.118×10^9	0.000369

$$\pi(x) \approx \frac{x}{\log x}$$

Universitat de Girona
Càtedra Lluís A. Santaló d'Aplicacions de la Matemàtica

Primers en una successió aritmètica

Exemple

S_1 : 6, 15, 24, 33, 42 ... $\quad a_n = 9n - 3 \;\Rightarrow\; a_n = 3(3n-1)$

S_2 : 4, **13**, 22, **31**, 40 ... $\quad a_n = 9n - 5 \ni \{13, 31, 67, 103, 139, ...\}$

Peter G. Lejeune Dirichlet (1805-1859)

Teorema de Dirichlet (1837)

Si $\mathrm{Mcd}(a,b) = 1$, aleshores la successió aritmètica $an + b$, $n \in \mathbb{N}$, conté infinits nombres primers.

Exemples

- $\exists$ infinits primers $4n + 1$ (Euler).
- $\exists$ infinits primers $5n + 11$.
- $\exists$ infinits primers $8n + 15$.

Aritmètica clàssica $\mapsto$ **Teoria Analítica de Nombres**

El treball de Riemann

Georg Friedrich
Bernhard Riemann
(1826-1866)

Monatsberichte der Berliner Akademie, novembre de 1859, pp. 145-153.

"Über die Anzahl der Primzahlen unter einer gegebenen Grösse"

("Sobre la quantitat de nombres primers per sota d'un nombre donat")

⚠ **Fórmula exacta per a $\pi(x)$** ⚠

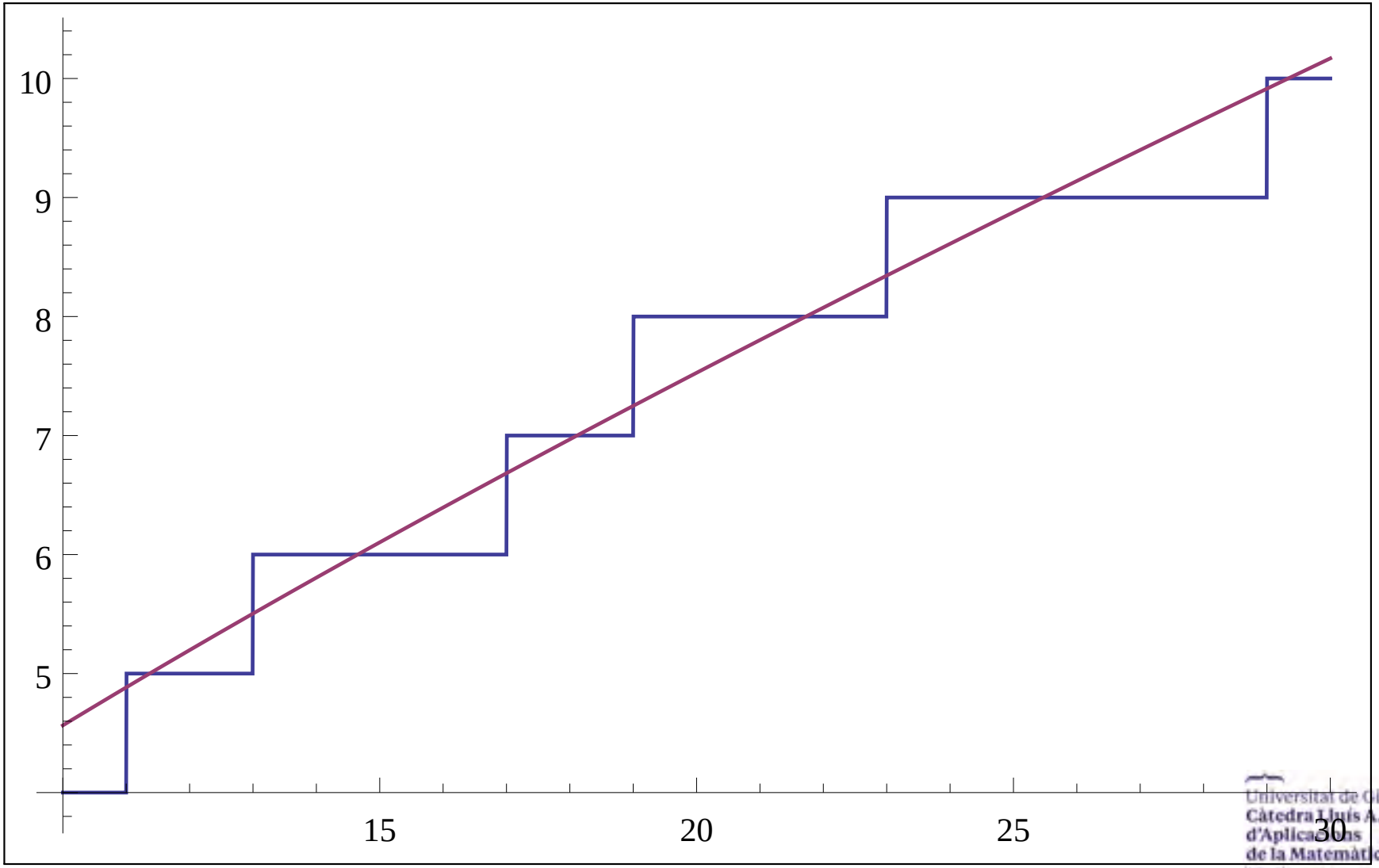
$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}\,, \qquad s = \sigma + i\,t \in \mathbb{C}, \quad \mathrm{Re}(s) > 1$$

$$\pi(x) = \text{Terme principal} + \text{Terme corrector}$$

Universitat de Girona
Càtedra Lluís A. Santaló d'Aplicacions de la Matemàtica

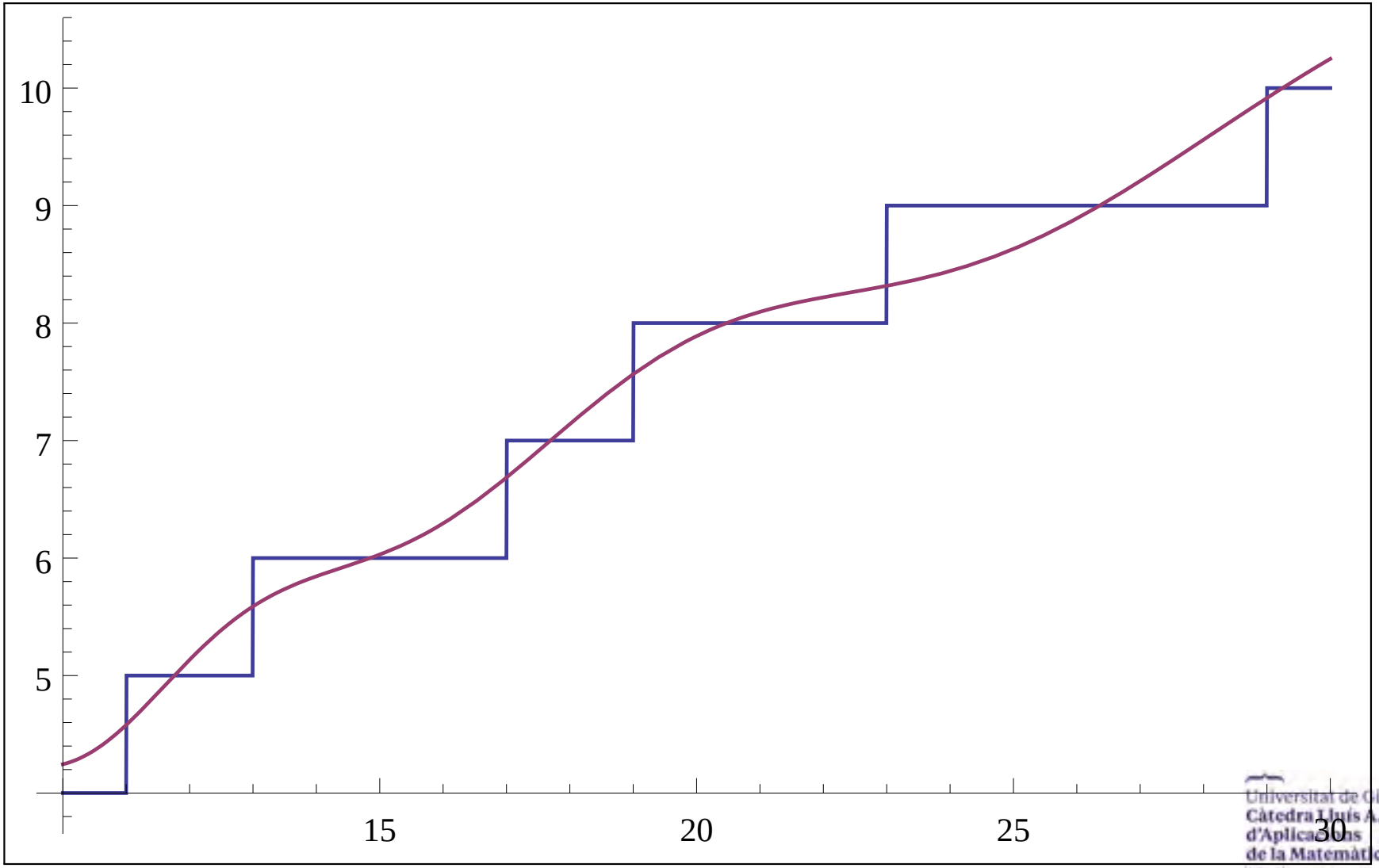
Sembla que Riemann té raó...

$$\pi(x) \approx \text{Terme principal } (\mathrm{Ri}(x))$$



Sembla que Riemann té raó...

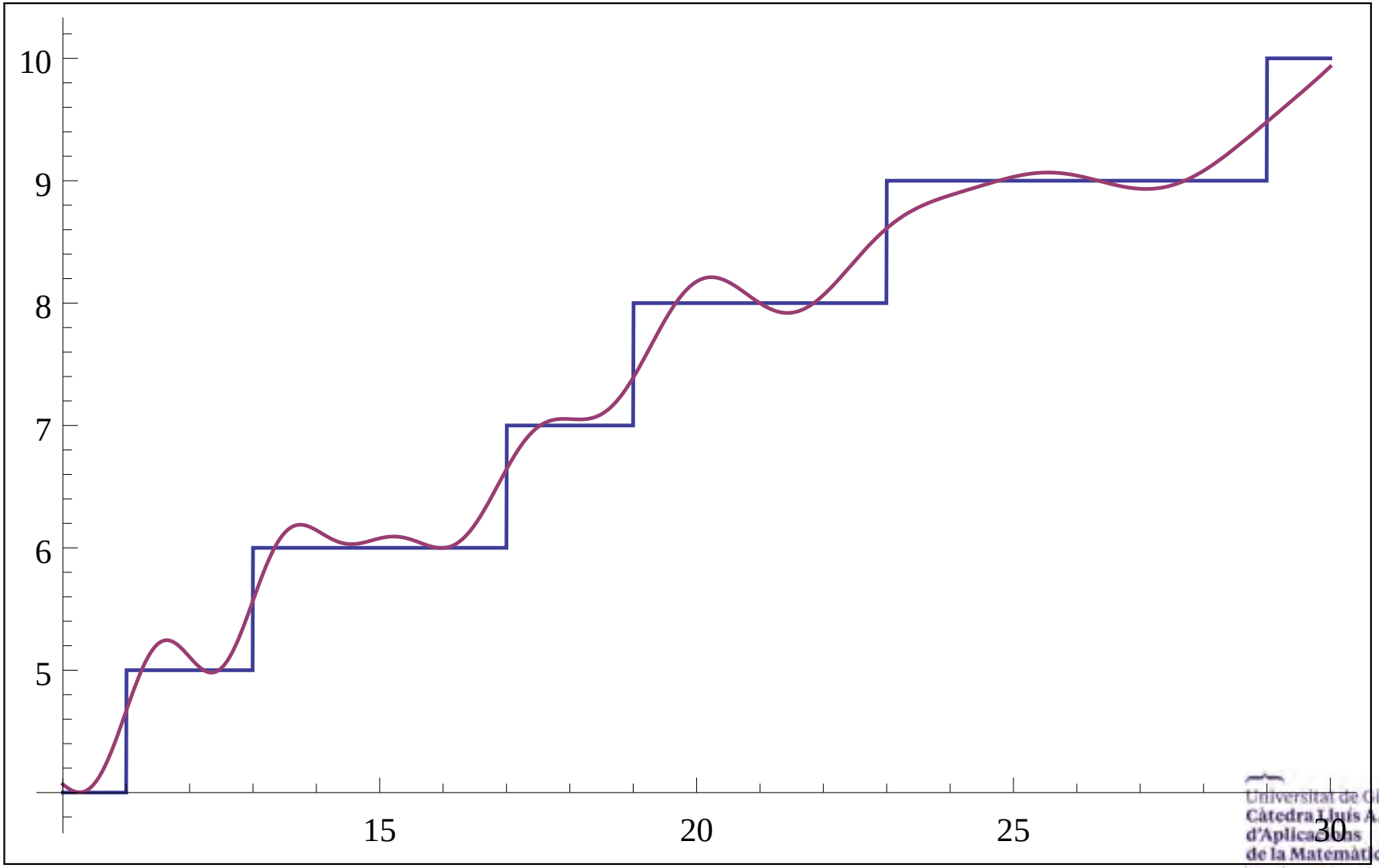
$\pi(x) \approx$ Terme principal (Ri(x))+Terme corrector (1 zero no trivial)



Universitat de Girona
Càtedra Lluís A. Santaló d'Aplicacions de la Matemàtica

Sembla que Riemann té raó...

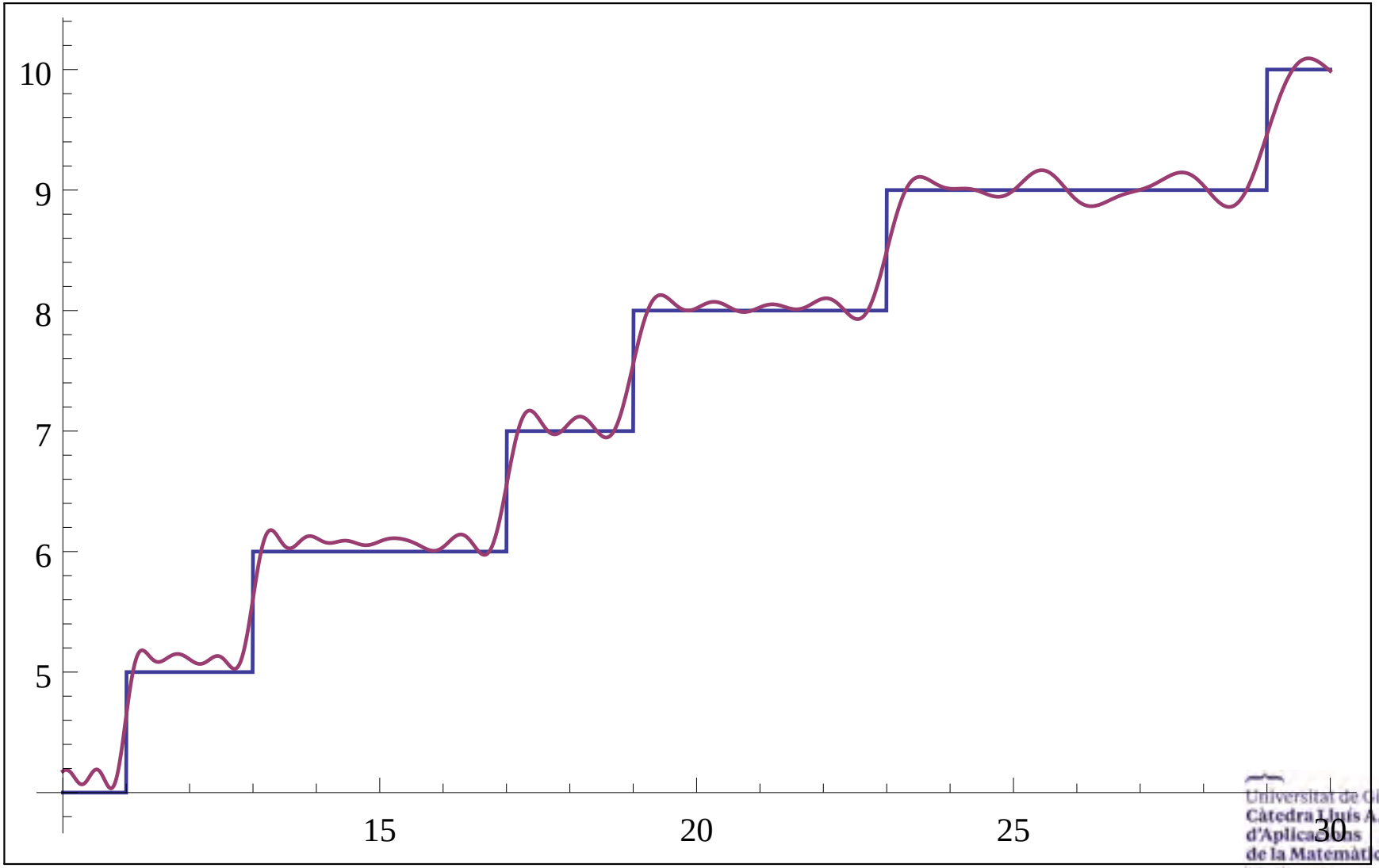
$\pi(x) \approx$ Terme principal (Ri(x))+Terme corrector (10 zeros no trivials)



Universitat de Girona
Càtedra Lluís A. Santaló d'Aplicacions de la Matemàtica

Sembla que Riemann té raó...

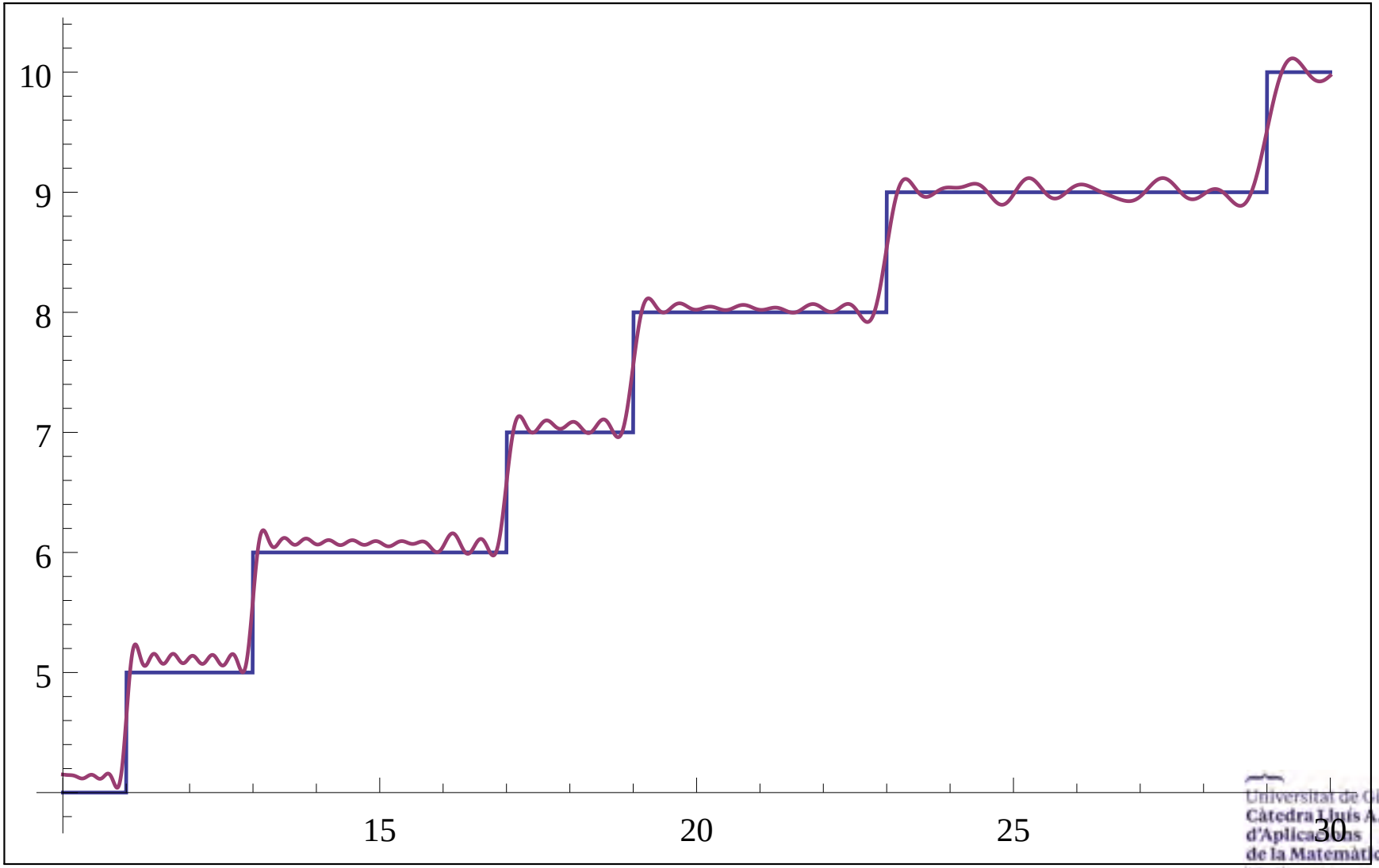
$\pi(x) \approx$ Terme principal (Ri(x))+Terme corrector (50 zeros no trivials)



Universitat de Girona
Càtedra Lluís A. Santaló d'Aplicacions de la Matemàtica

Sembla que Riemann té raó...

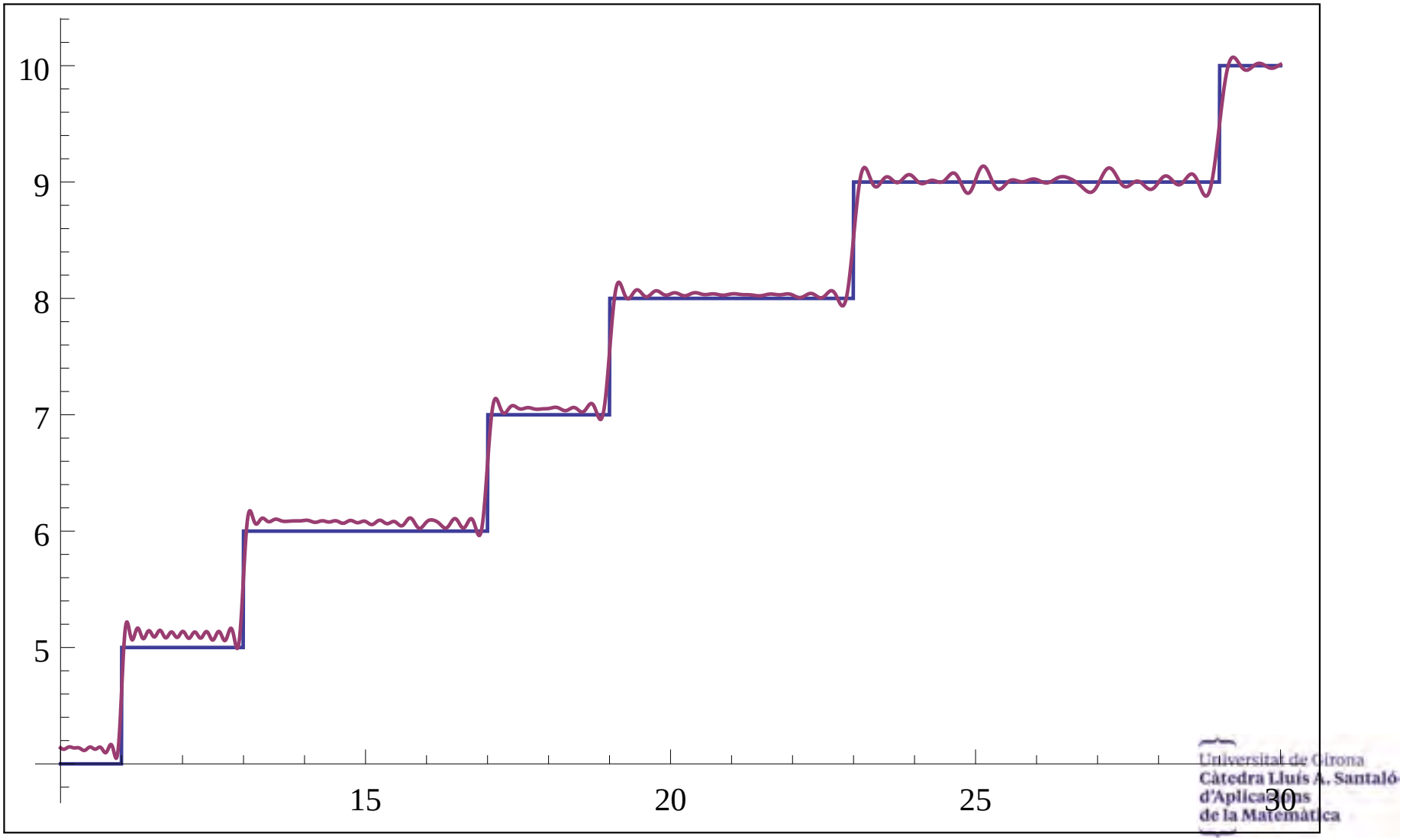
$\pi(x) \approx$ Terme principal (Ri(x))+Terme corrector (100 zeros no trivials)



Universitat de Girona
Càtedra Lluís A. Santaló d'Aplicacions de la Matemàtica

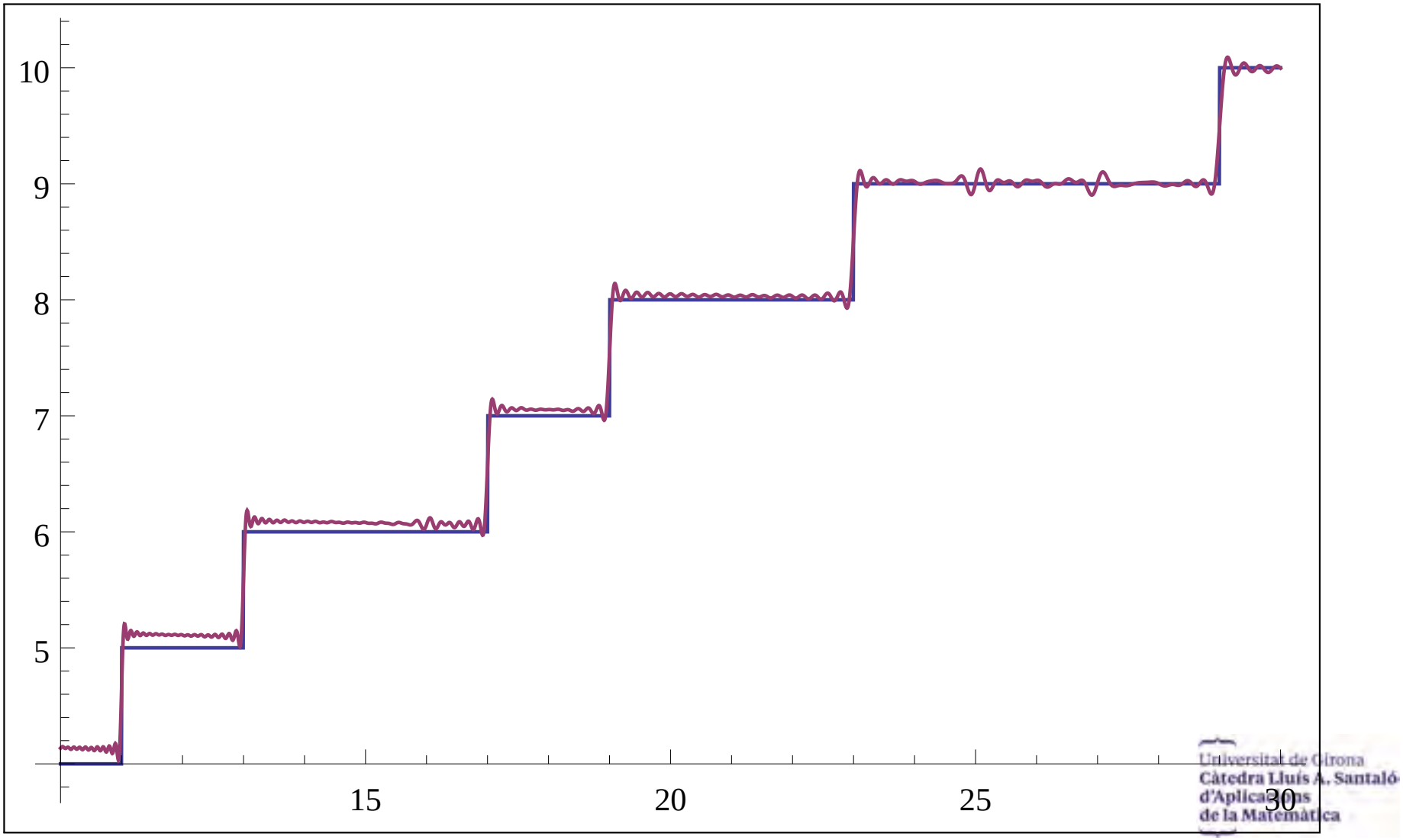
Sembla que Riemann té raó...

$\pi(x) \approx$ Terme principal (Ri(x))+Terme corrector (200 zeros no trivials)



Sembla que Riemann té raó...

$\pi(x) \approx$ Terme principal (Ri(x))+Terme corrector (400 zeros no trivials)



Entendre el treball de Riemann

- 1896. J. Hadamard i C. de la Vallée Poussin. *PNT*.
- 1900. D. Hilbert. *Els 23 problemes de Hilbert*.

Universitat de Girona
Càtedra Lluís A. Santaló
d'Aplicacions
de la Matemàtica

Entendre el treball de Riemann

8. Problems of Prime Numbers.

Essential progress in the theory of the distribution of prime numbers has lately been made by Hadamard, de la Vallée-Poussin, Von Mangoldt and others. For the complete solution, however, of the problems set us by Riemann's paper "Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse," it still remains to prove the correctness of an exceedingly important statement of Riemann, viz., *that the zero points of the function* $\zeta(s)$ *defined by the series*

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots$$

all have the real part $\frac{1}{2}$, except the well-known negative integral real zeros. As soon as this proof has been successfully established, the next problem would consist in testing more exactly Riemann's infinite series for the number of primes below a given number and, especially, *to decide*

David Hilbert (1862-1943)

"Si em desperto d'aquí a 500 anys, el primer que demanaré és: –Algú ha demostrat la Hipòtesi de Riemann?"

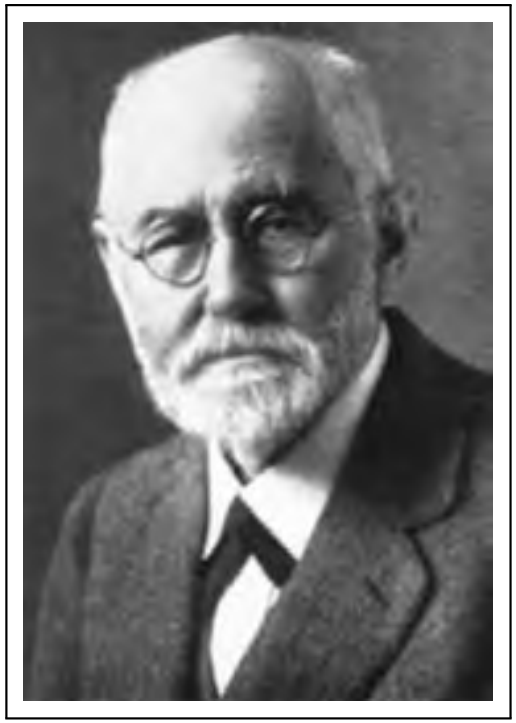
Universitat de Girona
Càtedra Lluís A. Santaló d'Aplicacions de la Matemàtica

Entendre el treball de Riemann

- 1896. J. Hadamard i C. de la Vallée Poussin. *PNT*.
- 1900. D. Hilbert. *Els 23 problemes de Hilbert*.
- 1896-1932. Demostrant els "serrells" deixats per Riemann.

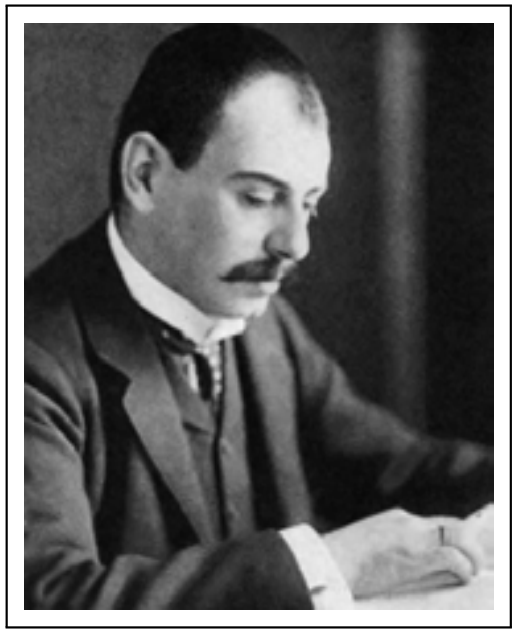
Universitat de Girona
Càtedra Lluís A. Santaló
d'Aplicacions
de la Matemàtica

Entendre el treball de Riemann



H. Von Mangoldt

(1854-1925)



E. Landau

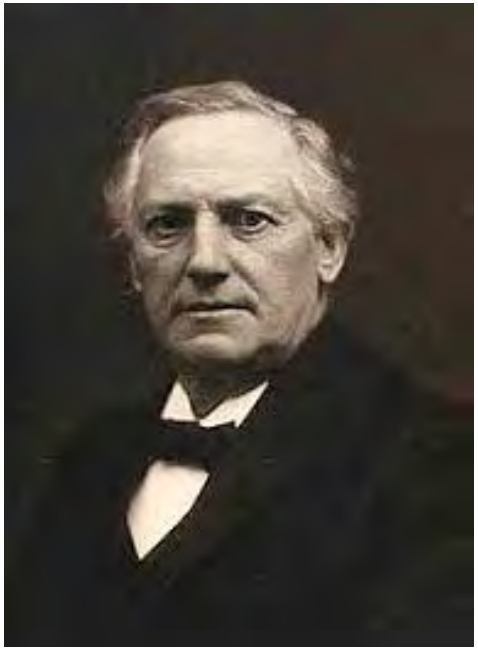
(1877-1938)

H. Bohr

(1887-1951)

Universitat de Girona
Càtedra Lluís A. Santaló
d'Aplicacions
de la Matemàtica

Entendre el treball de Riemann



J.P. Gram

(1850-1916)

G.H. Hardy

(1877-1945)

J.E. Littlewood

(1885-1977)

Universitat de Girona
Càtedra Lluís A. Santaló
d'Aplicacions
de la Matemàtica

Entendre el treball de Riemann

- 1896. J. Hadamard i C. de la Vallée Poussin. *PNT*.
- 1900. D. Hilbert. *Els 23 problemes de Hilbert*.
- 1896-1932. Demostrant els "serrells" deixats per Riemann.
- 1932-Actualitat. De l'amenaça a la confirmació computacional.

Universitat de Girona
Càtedra Lluís A. Santaló
d'Aplicacions
de la Matemàtica

Entendre el treball de Riemann

C.L. Siegel

(1896-1981)

A.M. Turing

(1912-1954)

D.H. Lehmer

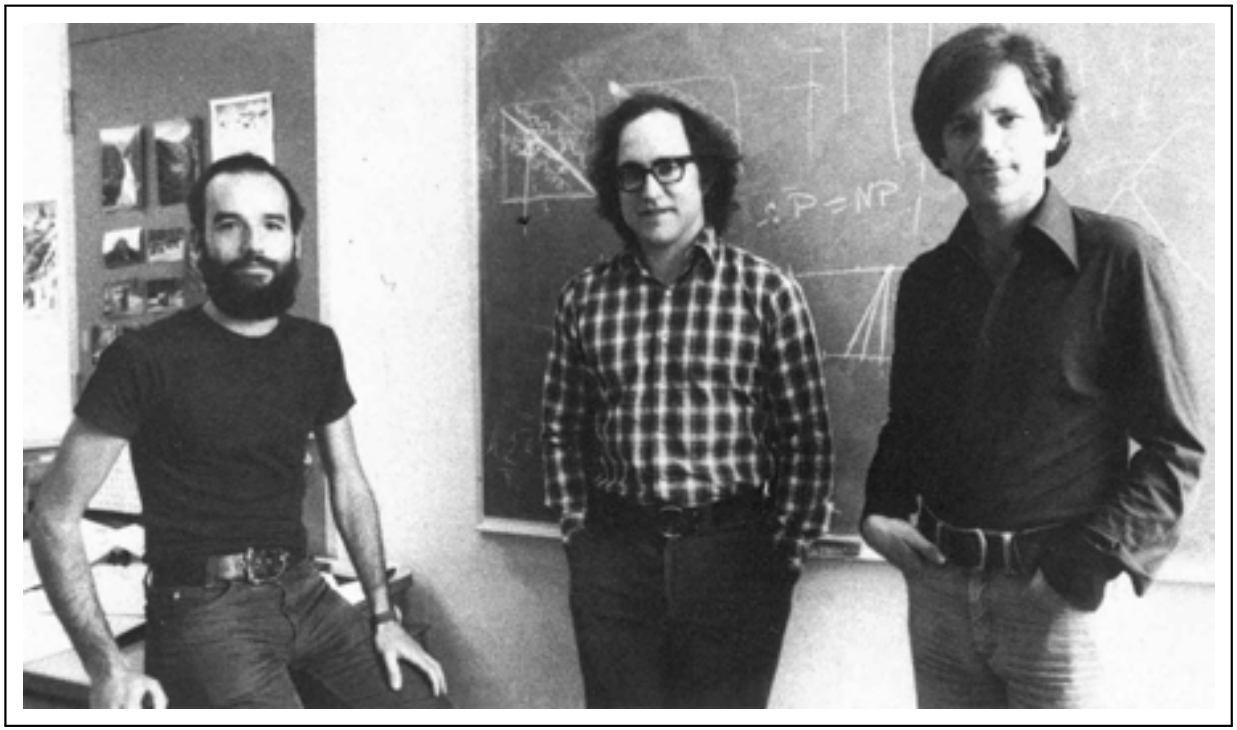
(1905-1991)

Universitat de Girona
Càtedra Lluís A. Santaló
d'Aplicacions
de la Matemàtica

Entendre el treball de Riemann

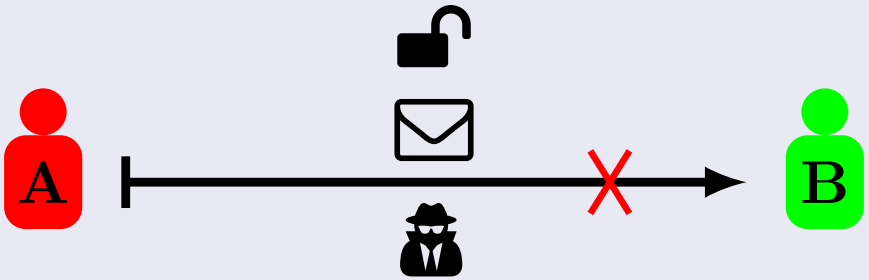
Any	n	Autor
1859(?)	3	B. Riemann (publicats per C.L. Siegel el 1932)
1903	15	J.P. Gram
1914	79	R.J. Backlund
1925	138	J.I. Hutchinson
1935	195	E.C. Titchmarsh
1936	1 041	E.C. Titchmarsh, L.J. Comrey
1953	1 104	A.M. Turing
1956	15 000	D.H. Lehmer
1956	25 000	D.H. Lehmer
1958	35 337	N.A. Meller
1966	250 000	R.S. Lehman
1968	3 500 000	J.B. Rosser, J.M. Yohe, L. Schoenfeld
1977	40 000 000	R.P. Brent
1979	81 000 001	R.P. Brent
1982	200 000 001	R.P. Brent, J. van de Lune, H.J.J. te Riele, D.T. Winter
1983	300 000 001	J. van de Lune, H.J.J. te Riele
1986	1 500 000 001	J. van de Lune, H.J.J. te Riele, D.T. Winter
2001	10 000 000 000	J. van de Lune (sense publicar)
2004	900 000 000 000	S. Wedeniwski
2004	10 000 000 000 000	X. Gourdon i P. Demichel

Per què són tan importants els nombres primers?

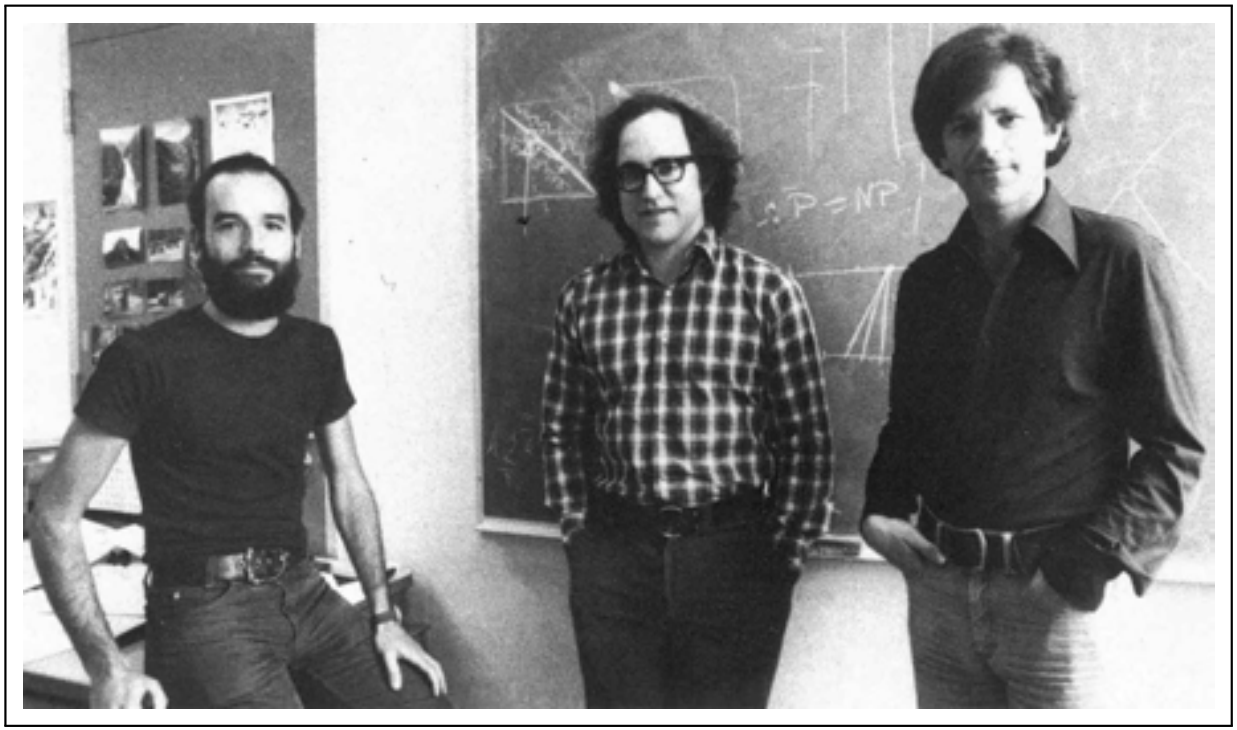


Adi Shamir (1952-), Ronald Rivest (1947-), Leonard Adleman (1945-)

Sistema criptogràfic de clau pública *RSA* (1977)



Per què són tan importants els nombres primers?



Adi Shamir (1952-), Ronald Rivest (1947-), Leonard Adleman (1945-)

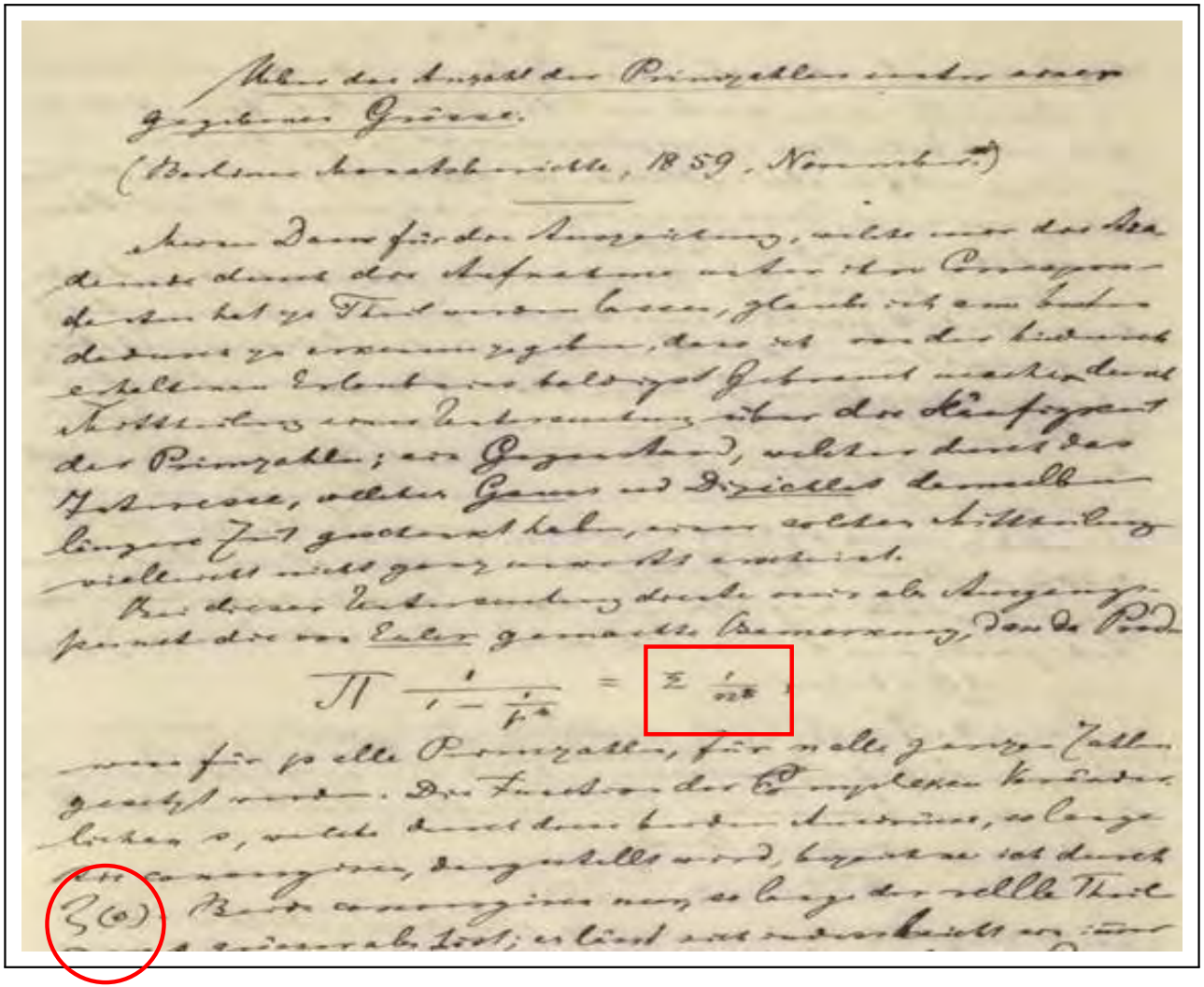
Sistema criptogràfic de clau pública *RSA* (1977)

Per què és segur *RSA*?

1. Tenim prou primers de 200 dígits?
   Sí. $\pi(10^{201}) - \pi(10^{200}) \geq 1.94352 \times 10^{198}$.
2. Si coneixem la clau pública, per què no podem calcular la clau privada?
   Necessitem factoritzar un nombre compost de 400 dígits que és producte de dos primers de 200 dígits.
3. Tenim algorismes eficients per factoritzar nombres?
   No, i els nostres ordinadors mai no seran prou ràpids.
4. Existeix un algorisme eficient?
   No ho sabem. Respondre aquesta pregunta val un altre 1 000 000 \$ (Problema *P versus NP*) .
5. Canviaria la situació amb un altre tipus d'ordinadors?
   Sí. S'ha demostrat (nivell teòric) que amb un *ordinador quàntic* el problema de factoritzar és de classe *P*.

Universitat de Girona
Càtedra Lluís A. Santaló d'Aplicacions de la Matemàtica

Moltes gràcies per la vostra atenció



Primera pàgina del manuscrit

Über die Anzahl der Primzahlen unter einer gegebenen Grösse

Universitat de Girona
Càtedra Lluís A. Santaló d'Aplicacions de la Matemàtica