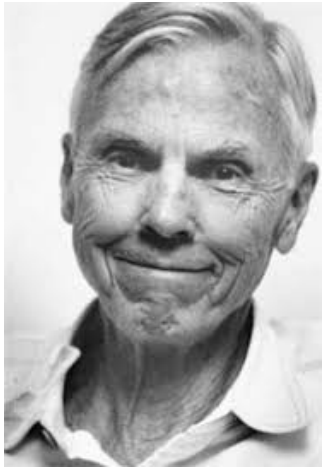
Una breu història dels nombres primers: d'Euclides a Tate

Xerrada a càrrec de Francesc Fité (Universitat de Barcelona)

Euclides (325 a.C.-265 a.C.)
Alexandria, Antiga Grècia



John Tate (1925-2019)
Harvard, USA

Nombres primers

Un **nombre primer** és un nombre diferent de 1 que:

només és divisible per 1 i per ell mateix.

Els nombres primers més petits són:

2, 3, 5, 7, 11, 13, 17, 19, ...

Tot nombre enter s'expressa com a producte de nombres primers:

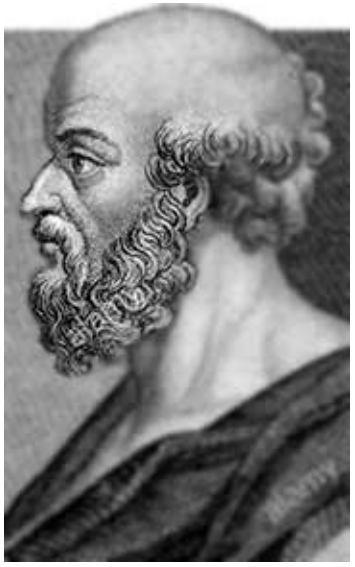
Els nombres primers són els àtoms dels nombres enters.

La **teoria de nombres** és la branca de les matemàtiques que s'encarrega de l'estudi dels nombres enters. L'estudi dels nombres primers és essencial.

L’alba de la teoria de nombres

La teoria de nombres neix a l’Antiga Grècia.

Euclides (s. IV a.C.)
Alexandria



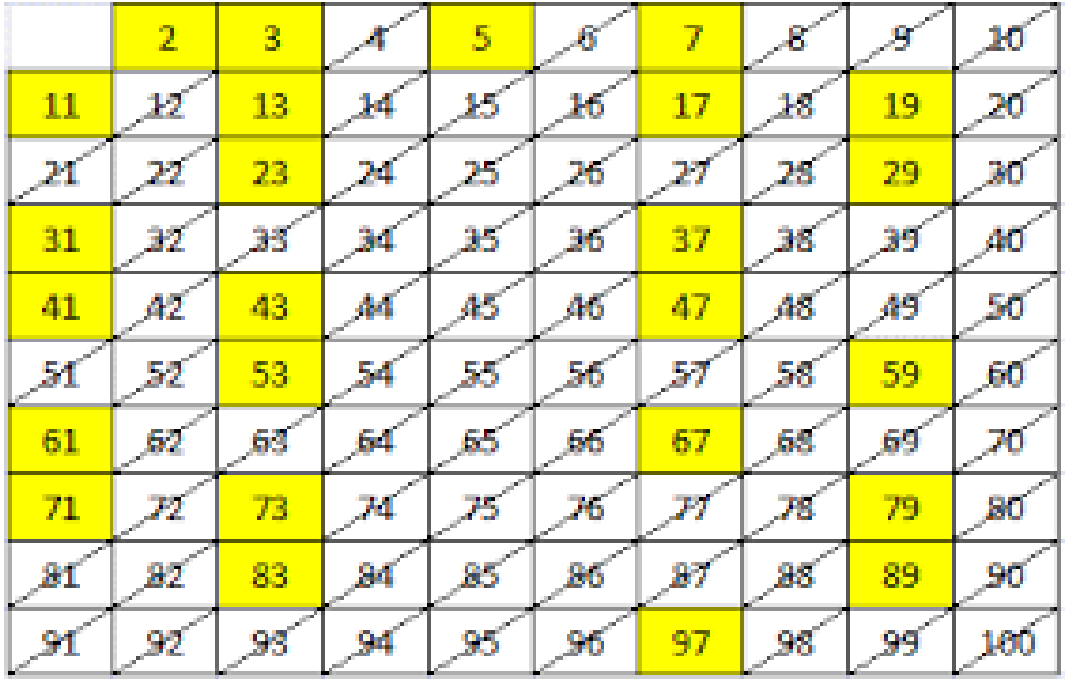
Eratòstenes (s. III a.C.)
Cirene, Alexandria

Diofant (s. III)
Alexandria

Antiga Grècia

Garbell d'Eratòstenes

És un mètode per trobar els nombres primers fins a un cert nombre.



	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

Primer descartem els múltiples de 2.

Ens trobem el 3.

Descartem els múltiples de 3.

Ens trobem el 5.

Descartem els múltiples de 5.

Ens trobem el 7.

Els nombres que no han quedat descartats són justament els primers fins a 100 !

Què és una demostració?

A l'institut aprenem a **calcular**, a **aplicar** fórmules, ...

Aprenem a **demostrar**? Què significa **demostrar**?

Demostrar consisteix en deduir la veritat d'una afirmació a partir de veritats òbvies i de les regles de la lògica.

Euclides va demostrar que existeixen **infinits** nombres primers.

Ho va fer a partir de la següent veritat òbvia:

Si un primer divideix dos nombres, divideix la seva diferència.

Per exemple, 3 divideix 9 i 15. Aleshores 3 també divideix 6.

Infinitud de primers

Demostració

Veurem que donats uns quants primers, sempre se'n pot trobar un de diferent.

Anomenem p_1, p_2, p_3, ..., p_n aquests primers donats.

Considerem el seu producte $P= p_1 \times p_2 \times p_3 \times ... \times p_n$.

Si P+1 és un nombre primer, ja hem trobat un primer diferent.

Si P+1 no és primer, aleshores existeix un primer $q<P+1$ que divideix P+1. Aquest primer q és diferent dels primers donats, ja que altrament dividiria P i P+1, i per tant també dividiria la seva diferència (P+1)-P=1, cosa que no pot ser.

Grans nombres primers

Malgrat ***conèixer l'existència*** d'infinits nombres primers, ***trobar*** nombres primers grans és complicat.

El primer més gran conegut és

$$2^{82.589.933} - 1$$

Té més de 24 milions de dígits.

Va ser trobat el 2018 pel projecte col·laboratiu GIMP (Great Internet Mersenne Prime Search) que reuneix matemàtics i informàtics d'arreu del món (més al taller!).

Així doncs, ***els grans primers són com els grans amors****:*

sabem que existeixen, però trobar-los pot ser una empresa difícil.

Un salt a la història

Durant l'Edat Mitjana, Europa queda sumida en un període de foscor.

Fermat (1601-1665)
Occitània

Euler (1707-1783)
Suïssa

Germain (1777-1831)
França

Des Diofant (s. III) a Fermat (s. XVII) no hi ha avanços significatius en la comprensió dels nombres primers. Grans avenços arriben al s. XVIII.

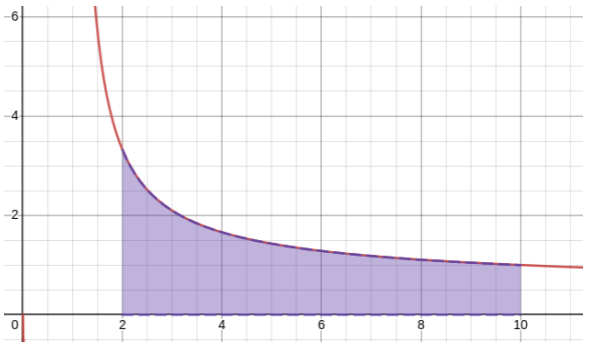
El geni de Gauss

Amb 15 anys, Gauss introdueix les funcions següents:

1) $\pi(x)$ = nombre de primers menors que x.

Per exemple, $\pi(6) = 3$.

2) Li(x) = area sota 1/log(x) entre 2 i x.



$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\log(t)}$$

Gauss (1777-1855)
Alemanya

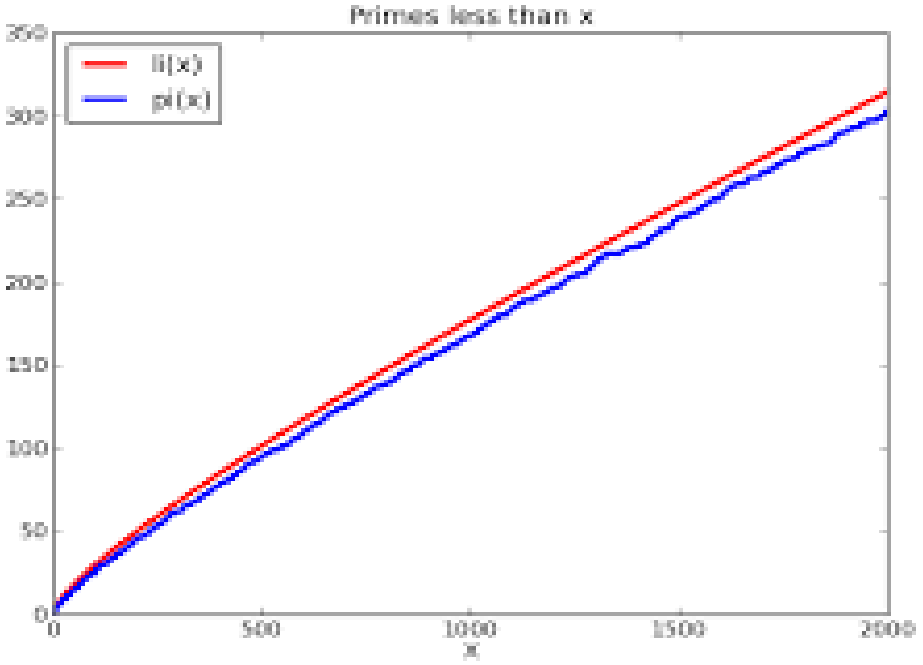
Calcular $\pi(x)$ és **complicat** si x és gran amb o sense calculadora.

Calcular Li(x) és **senzill** amb qualsevol calculadora i per x qualsevol.

Li(x) versus π(x)

El 1792 Gauss calcula π(x) per a molts valors de x i observa π(x) es pot aproximar bé per la funció Li(x):

x	π(x)	Li(x)
10	4	5.12
10^2	25	29.08
10^3	168	176.56
10^4	1229	1245.09
10^5	9592	9628.76
10^6	78498	78626.50
10^7	664579	664917.35
10^8	5761455	5762208.33
10^9	50847534	50849233.91



Teorema del nombre primer

Hadamard i de la Vallée Poussin demostren:

Teorema del nombre primer (1896)

Per la majoria de valors de x, Li(x) i $\pi(x)$ tenen el mateix nombre de xifres i comencen per la mateixa xifra.

Hadamard (1865-1963)
França

De la Vallée Poussin
(1866-1962)
Bèlgica

Hipòtesi de Riemann

De fet, esperem que encara més sigui cert:

Hipòtesi de Riemann (1859)

Per la majoria de valors de x, la primera meitat de les xifres de Li(x) i $\pi(x)$ coincideixen.

No obstant, fins a data d'avui, **no es coneix** una demostració d'aquesta afirmació!

La Fundació Clay ofereix un 1.000.000 $ a aquella persona que en pugui donar una demostració!

Riemann (1826-1866)
Alemanya

Von Koch (1870-1924)
Suècia

Quan 2 i 2 no són 4

Pregunta

Quina hora serà 5 hores després de les 22:00? I 2 hores després?

L'**Aritmètica modular** és l'aritmètica de les hores. Escrivim:

$$22 + 5 = 3 \text{ (mòdul 24)}$$

Diem que 27 és ***congruent*** amb 3 mòdul 24.

Això que hem fet per 24, ho podem fer per qualsevol número:

$$3 + 2 = 5 = 1 \text{ (mod 4)}$$

$$2 + 2 = 0 \text{ (mod 4)}$$

El que hem fet per la +, ho podem fer per altres operacions:

$$3 \times 3 = 9 = 5 = 1 \text{ (mod 4)}$$

Divisió modular

Com podem dividir en l'aritmètica modular? Quant és 4/3 (mod 5)?

Idea

Primer calcularem 1/3 (mod 5) i després multiplicarem per 4.

Observeu que

$$3 \times (1/3) = 1 \pmod 5$$

$$3 \times 2 = 6 = 1 \pmod 5$$

Deduïm que $1/3 = 2 \pmod 5$. Per tant,

$$4/3 = 4 \times (1/3) = 4 \times 2 = 8 = 3 \pmod 5$$

Arrel quadrada modular

De manera semblant ens podem preguntar quant és:

$$\sqrt{2} \pmod 7$$

Observem que:

$$\sqrt{2} \times \sqrt{2} = 2 \pmod 7$$

$$3 \times 3 = 2 \pmod 7$$

Per tant deduïm que:

$$\sqrt{2} = 3 \pmod 7$$

Gauss (1777-1855)
Alemanya

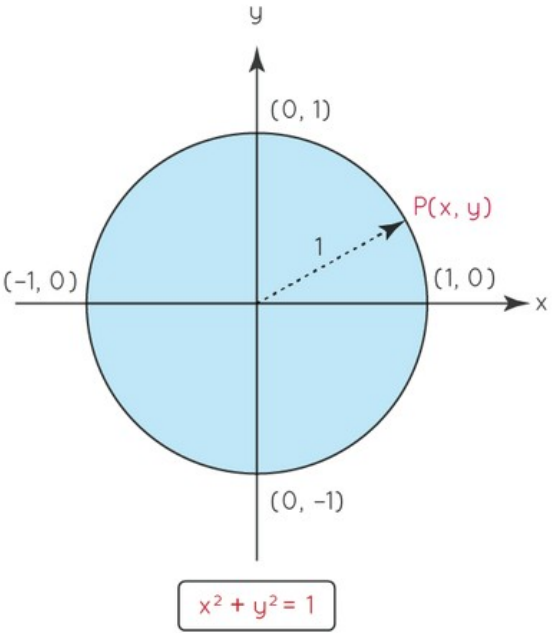
Gauss va ser l'inventor de l'aritmètica modular.

Geometria modular

L'equació del cercle de radi 1 centrat a l'origen del **pla real** és $x^2 + y^2 = 1$.

Podem pensar que $x^2 + y^2 = 1$ defineix un cercle en el **pla (mod 5)**.

El pla (mod 5) són els punts (x, y), on x i y poden prendre només els valors 0,1,2,3,4.

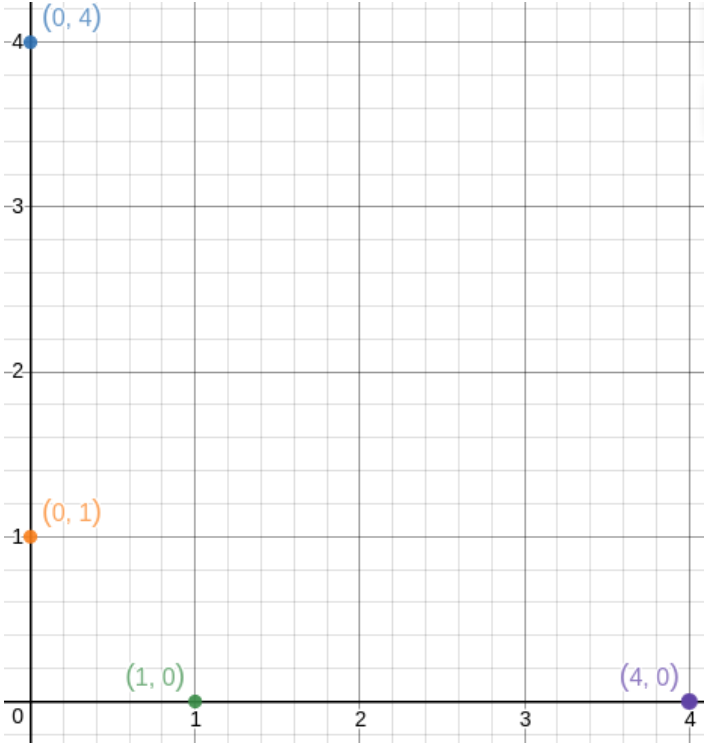


El cercle de radi 1 en el pla mòdul 5

$0^2 + 1^2 = 1 \pmod 5$
$0^2 + 4^2 = 1 \pmod 5$
$1^2 + 0^2 = 1 \pmod 5$
$0^2 + 4^2 = 1 \pmod 5$

El cercle de radi 1 només té 4 punts al pla mòdul 5.

Certament, no sembla un cercle...



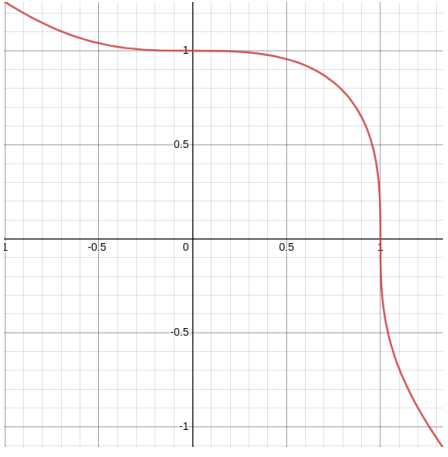
Corbes al pla mòdul un primer

Com hem fet amb 5, podem considerar el pla mòdul 7, 11, 13, 17,...

Com hem fet amb el cercle, podem considerar una **corba** qualsevol.

Una **corba** és una equació que relaciona les coordenades x i y.

El **grau** d'una corba és el grau de l'equació que la defineix.



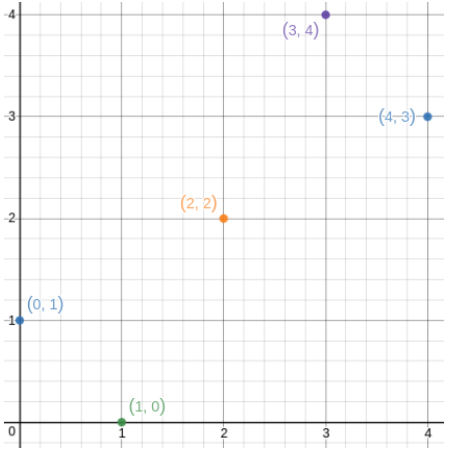
Dibuix de la corba

$C : x^3 + y^3 = 1$

Al pla real, esquerra.

Al pla (mod 5), dreta.

Grau(C)=3.



Teorema de Weil

Recordatori

El cercle $x^2 + y^2 = 1$ al pla (mod 5) té 4 punts.

La cúbica $x^3 + y^3 = 1$ al pla (mod 5) té 5 punts i al pla (mod 31) en té 33.

Teorema de Weil (1948)

Prenem un primer p qualsevol i una corba C al pla (mod p) qualsevol. Aleshores C té aproximadament p punts.

Weil (1906-1998)
França

Les corbes al pla (mod p) són de gran importància en la ***criptografia***.

La criptografia és una disciplina entre la teoria de nombres i la informàtica que s'encarrega de la codificació de missatges per tenir comunicacions segures.

Hipòtesi de Sato i Tate

Prenem una corba C.

Direm que un primer p és:

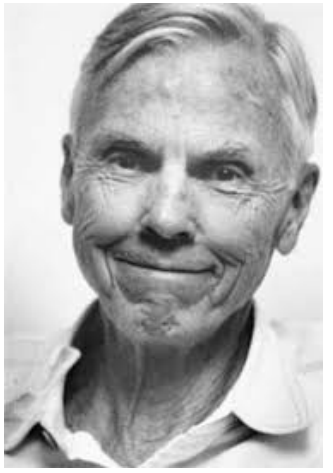
excessiu si el nombre de punts de C al pla (mod p) és > p + Grau(C).

defectiu si el nombre de punts de C al pla (mod p) és < p - Grau(C).

Hipòtesi de Sato i Tate (1965)

La proporció de primers excessius és la mateixa que la proporció de primers defectius.

A data d'avui, **no es coneix** una demostració d'aquesta afirmació!

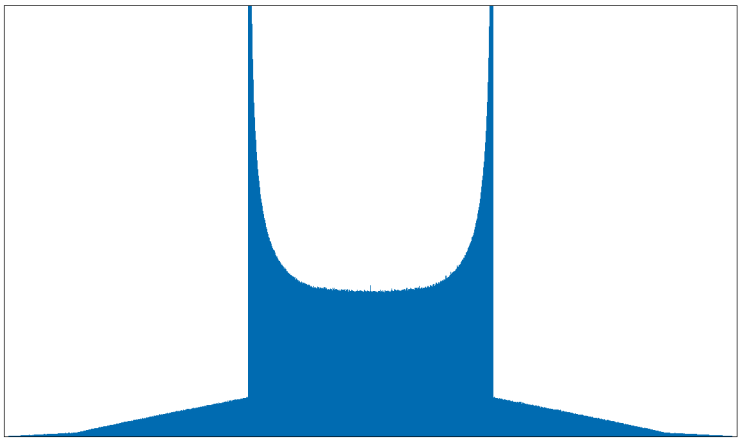


John Tate
(1925-2019), USA

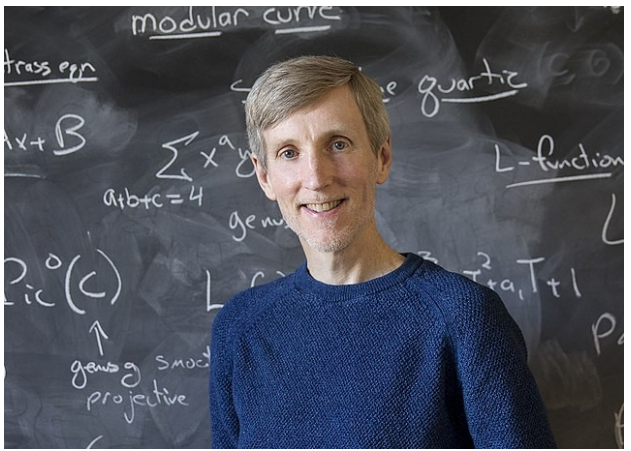
Mikio Sato
(1928-), Japó

Verificació amb ordinadors

S'ha utilitzat els ordinadors per verificar la validesa d'aquesta hipòtesi.
L'histograma de sota fa referència a la corba $y^2 - x^5 = x^3 + 2x$.



Primers defectius Primers excessius



Andrew Sutherland, USA

La simetria respecte l'eix central reflecteix que: Proporció(defectius) = Proporció(excessius).

Queden moltes pàgines per escriure...

La hipòtesi de Sato i Tate s'ha demostrat per corbes de grau < 4.

Richard Taylor (1962-), Anglaterra

Ana Caraiani (1985-), Romania

Els matemàtics i matemàtiques continuen cercant una demostració vàlida per graus 4, 5, 6, 7, 8, ...

Una breu història dels nombres primers: d'Euclides a Tate

Moltes gràcies per la vostra atenció!

Espero que us hagi interessat.