# Cartografia dels nombres primers

Xavier Xarles

21 de Març de 2026

# Què és un nombre primer?

**Definició**

Un nombre natural $p$ és **primer** si només té dos divisors positius:

- 1
- ell mateix ($p$)

**Remarca**

El nombre 1 no és un nombre primer. Això és important ja que sinó no tindríem que tot nombre factoritza de manera **única** com a producte de primers.

Si un nombre té més divisors s'anomena **nombre compost**.

# Exemples de nombres primers

Alguns dels primers nombres primers són:

$$2, 3, 5, 7, 11, 13, 17, 19, 23$$

$$29, 31, 37, 41, 43, ...$$

# Teorema fonamental de l'aritmètica

**Enunciat**

Tot nombre natural $n > 1$ es pot escriure com a producte de nombres primers.

Aquesta descomposició és **única** excepte per l'ordre dels factors. Podem escriure per tant de manera única com

$$n = p_1^{r_1} \cdots p_s^{r_s}$$

on $p_1 < p_2 < \cdots < p_r$ són primers i $r_1, \ldots, r_s \geq 1$.

# Perquè és pot fer?

Que hi ha una descomposició és fàcil:

- Si el nombre $n$ és primer, ja està.
- Si no ho és, llavors hi ha nombres $1 < m < n$ que divideixen $n$.
- Prenem el més petit $1 < p < n$ que divideix $n$.
- Aquest nombre $p$ ha de ser primer, ja que si no ho fos, tindria un divisor $1 < d < p$, que per tant també divideix $n$ i és més petit que $p$, i per tant $p$ no seria el més petit.
- El nombre $n$ és $n = p \cdot m$ amb $1 < m < n$.
- Repetim el procediment amb $m$.
- Com que el nombre $m$ és més petit, al repetir el procediment algun dia acabarem.

# Perquè és única?

La raó fonamental és perquè els nombres primers verifiquen que
**Lema d'Euclides:**
Si $p$ és un nombre primer, i $p$ divideix $n \cdot m$, llavors $p$ divideix $n$ o $p$ divideix $m$.

Com que, si $p$ i $q$ són primers, i $p$ divideix $q$, llavors $p = q$, podem anar veient que els nombres primers que van apareixen a la descomposició són únics.

# Com saber si un nombre és primer?

**Criteri pràctic**
Un nombre $p$ és primer si no és divisible per cap nombre primer $q$ menor o igual que $\sqrt{p}$.

Si $p$ no és primer, llavors $p = n \cdot m$, on $1 < n \leq m < p$.
Llavors

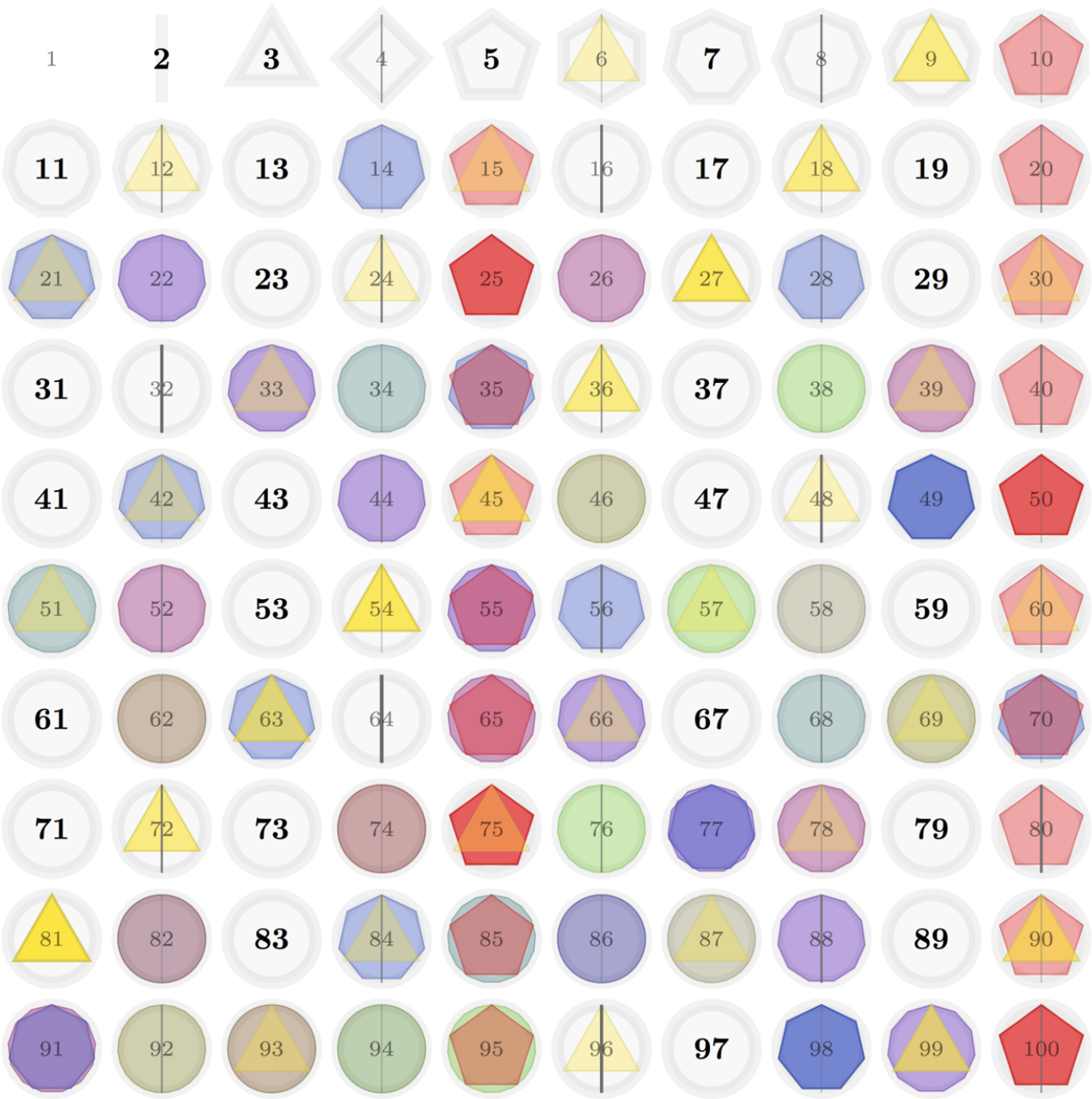
$$p = n \cdot m \geq n \cdot n = n^2.$$

Per tant

$$\sqrt{p} \geq n.$$

**Exemple** Per saber si un nombre de dues xifres és primer, només cal veure si és divisible per 2, 3, 5 o 7.

Figura: Eratostenes.



# Hi ha infinits nombres primers?

Veurem que si tenim un conjunt finit $S = \{p_1, \ldots, p_s\}$ de nombres primers, llavors hi ha un nombre primer que no està al conjunt.

Considerem el nombre

$$N = p_1 \cdots p_s + 1$$

(producte de tots els elements de $S$ més 1).

Aquest nombre és més gran que 1, i per tant algun nombre primer $q$ el divideix.

Aquest nombre $q$ no és igual a cap dels nombres $p_i$, ja que els $p_i$ no divideixen $N$:

Com que $p_i$ divideix a $N - 1 = p_1 \cdots p_s$, si $p_i$ dividis a $N$ llavors dividiria a la resta $N - (N - 1) = 1$, que no pot ser.

Per exemple, si prenem $S = \{2, 3, 5, 7\}$, llavors $N = 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$, i el nombre primer $q$ és 211.

Si prenem $S = \{2, 3, 5, 7, 11, 13\}$, llavors
$N = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031$ que no és un nombre primer, però $q = 59$ el divideix i si que ho és $30031 = 59 \cdot 509$.

# Quants nombre primer hi ha?

Gauss es va dedicar a calcular quants nombres primers hi havia fins a nombres grans (fins a 3 milions).

Fent aquest càlculs s'en va adonar que de nombres primers fins a $n$ n'hi havia aproximadament $\frac{n}{\log(n)}$ (on log vol dir logaritme natural o neperià).

Per exemple, fins a 3 mil·lions hi ha 216816 nombres primers, i

$$\frac{n}{\log(n)} = \frac{3000000}{\log(3000000)} \approx 201153$$

De fet, és encara millor prendre

$$\int_1^n \frac{dx}{\log(x)} = 216971$$

| Unter | gröſses Primzahlen | Integral $\int \frac{dn}{\log n}$ | Differ | Ihre Formel | Abweich. |
|---|---|---|---|---|---|
| 500 000 | 41 556 | 41606,4 | +50,4 | 41596,9 | +40,9 |
| 1000 000 | 78 501 | 78627,5 | +126,5 | 78672,7 | +171,7 |
| 1500 000 | 174 112 | 114263,1 | +151,1 | 114374,0 | +264,0 |
| 2000 000 | 148883 | 149054,8 | +171,8 | 149233,0 | +350,0 |
| 2500 000 | 183016 | 183245,0 | +229,0 | 183495,1 | +479,1 |
| 3000 000 | 216745 | 216970,6 | +225,6 | 217308,5 | +563,6 |

Dass Legendre sich auch mit diesem Gegenstande beschäftigt hat, war mir nicht bekannt; auf Veranlassung Ihres Briefes habe ich in seiner Theorie des Nombres nachgesehen, und in der zweiten Ausgabe einige darauf berügliche Seiten gefunden, die ich früher übersehen (oder seitdem vergessen) haben muſs. Legendre gebraucht die Formel

$$\frac{n}{\log n - A}$$

wo $A$ eine Constante sein soll, für welche er $1.08366$ setzt. Nach einer flüchtigen Rechnung finde ich danach in obigen Fällen die Abweichungen

$-23,3$
$+42,2$
$+68.1$
$+92.8$
$+159,1$
$+167.6$

Diese Differenzen sind noch kleiner als die mit dem Integral, sie scheinen aber bei zunehmendem n ~~stärker~~ schneller zu wachsen als diese, so daſs leicht möglich wäre, daſs bei viel weiterer Fortsetzung jene die letztern übertrafen. Um Zählung und Formel in Übereinstimmung zu bringen müſste man respective anstatt $A = 1{,}08366$ setzen

$1.09040$
$1.07682$
$1.07582$
$1.07529$
$1.07179$
$1.07297$

# Probabilitat o densitat dels nombres primers

La manera que tenim d'interpretar el que va conjecturar Gauss és que la probabilitat que un nombre $n$ sigui primer és $\frac{1}{\log(n)}$.

Per exemple, si agafo un nombre de 10 xifres, quina és la probabilitat que sigui primer?

O millor, si agafo 100 nombres de 10 xifres a l'atzar, quants d'ells seran nombres primers?

$$\frac{100}{\log(10^{10})} = \frac{100}{10\log(10)} = \frac{10}{\log(10)} \approx 4.3$$

Experiment amb sagemath: Ho podeu provar a sagecell.sagemath.org

```
M = []
for i in range(100):
    L = [ZZ.random_element(10^9+1,10^10) for _ in range(100)]
    M.append(sum(1 for n in L if n.is_prime()))
sum(M)/100.
```

# El teorema dels nombres primers

Llavors, la quantitat de nombres primers menors que $n$ hauria de ser aproximadament

$$\sum_{m=2}^{n} \frac{1}{\log(m)} \approx \int_2^n \frac{dx}{\log(x)} \approx \frac{n}{\log(n)}$$

EL 1896, utilitzant idees del Riemann, dos matemàtics francesos van demostrar que la intuïció del Gauss era correcte.

**Teorema:** (Hadamard, de la Vallée Poussin)
Si diem $P(n) =$ quantitat de nombres primers menors que $n$, llavors

$$P(n) \approx \int_2^n \frac{dx}{\log(x)} \approx \frac{n}{\log(n)}$$

# El teorema dels nombres primers

$$P(10^{28}) = 1575892692759734104127395 98$$

$$\frac{10^{28}}{28\log(10)} = 1551051721083042241611747 1,042$$

$$\int_2^{10^{28}} = 1575892692759748381583999 70,696$$

# Infinitud de certs tipus de primers

1. Tots els nombres primers, excepte el 2, són de la forma $4m+1$ o $4m-1$. N'hi ha infinits de cada tipus?
2. Tots els nombres primers, excepte el 3, són de la forma $3m+1$ o $3m-1$. N'hi ha infinits de cada tipus?
3. Tots els nombres primers, excepte el 2 i el 3, són de la forma $6m+1$ o $6m-1$. N'hi ha infinits de cada tipus?
4. Tots els primers, excepte el 2 i el 5, acaben en 1, o en 3, o en 7 o en 9 (expressats en base 10). N'hi ha infinits de cada tipus? .

# Primers fins a un mil·lió

Hi ha 78498 nombres primes menors d'un mil·lió.

1. 39175 son de la forma $4n+1$ i 39323 de la forma $4n-1$.
2. 39231 son de la forma $6n+1$ i 39266 son de la forma $6n-1$.
3. Si mirem com acaben, de fet tenim que n'hi ha 19617, 19665, 19621 i 19593 acabats en 1, 3, 7 i 9, respectivament.

# Teorema de Dirichlet

El 1826 Dirichlet va demostrar que hi ha infinits primers en cadascun dels casos. De fet va demostrar un resultat molt més general:

Per a cada base $b > 1$, hi ha infinits primers acabats en el dígit $a$ si i només si $a$ i $b$ són primers entre si.

Dit d'una altra manera, si $a$ i $b$ són primers entre si, hi ha infinits primers de la forma $a + bn$, on $n$ és un natural.

A més, hi ha la mateixa proporció de primers entre tots els possibles dígits en base $a$.

Per tant, la meitat dels primers son de la forma $4n + 1$, i l'altra meitat de la forma $4n - 1$.

I una quarta part dels primers acaba en 1, ídem en 3, ídem en 7 ídem en 9.

# Primers donats per polinomis

Hi ha moltes conjectures sobre els nombres primers. Comencem per les conjectures sobre primers de formes diferents.

1. Hi ha infinits primers de la forma $n^2 + 1$ (conjectura de Landau) (n'hi ha 840 valors de n fins a 10000 que surt primer)
2. Hi ha infinits primers de la forma $n^2 + 2$ (d'aquest n'hi ha 445)
3. Hi ha infinits primers de la forma $n^2 + 3$ (d'aquests n'hi ha 711)
4. Hi ha infinits primers de la forma $n^2 + n + 1$ (n'hi ha 1409 valors de n fins a 10000 que surt primer).
5. Hi ha infinits primers de la forma $n^3 + 2$ (d'aquests n'hi ha 519).

Però en canvi no n'hi ha infinits de la forma $n^3 + 1$, ni n'hi ha infinits de la forma $n^2 + n + 2$.

# Que li cal a un polinomi per donar infinits primers?

Perquè $n^3 + 1$ no dona infinits primers? Perquè

$$n^3 + 1 = (n + 1)(n^2 - n + 1)$$

i per tant sempre és producte de dos nombres (o més).

Per tant una condició que cal és que el polinomi no factoritzi (com a polinomi) en producte de dos o més polinomis: que sigui irreductible.

# Que li cal a un polinomi per donar infinits primers?

El polinomi $n^2 + n + 2$ és irreductible, però resulta que tots els seus valors són parells!

Un altre exemple més difícil de veure és $n^3 + 2n + 3$: resulta que tots els valors són sempre múltiples de 3.

Finalment, hi ha una condició sobre el coeficient de grau més gran: ha de ser positiu ja que sinó el polinomi només prendrà un nombre finit de valors positius.

# Bunyakovsky

**Conjectura:**
Prenem $p(x)$ un polinomi amb coeficients enters, irreductible, de manera que el coeficient de grau més gran sigui positiu i que no hi hagi cap nombre primer $p$ que divideixi tots els valors.

Llavors hi ha infinits primers de la forma $p(n)$ variant $n \geq 1$.

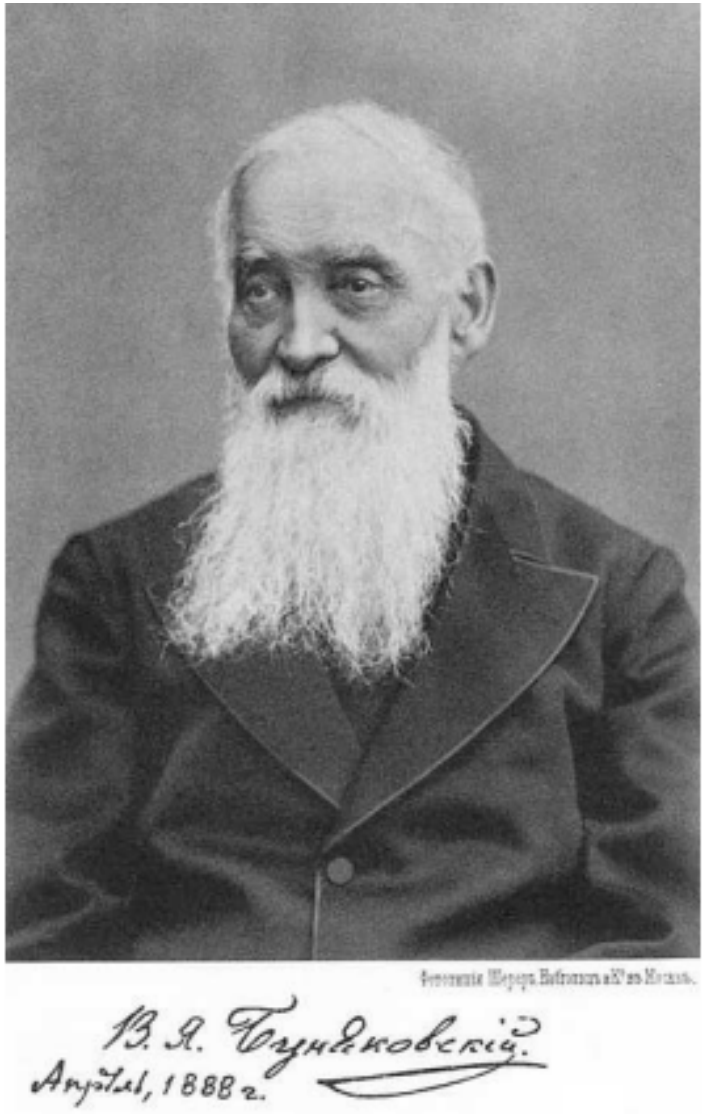



Figura: Viktor Yakovlevich Bunyakovsky (1804–1889)

# Quants n'hi ha? Heurística

Si la probabilitat que un nombre $n$ sigui primer és $\frac{1}{\log(n)}$, llavors la probabilitat que un nombre $n^2+1$ sigui primer hauria de ser

$$\frac{1}{\log(n^2+1)} \approx \frac{1}{\log(n^2)} = \frac{1}{2\log(n)}$$

Ara bé, si fem el càlcul fins a 1 mil·lió amb el cas $n^2+1$ surt que hi ha 54110 valors de $n$ tal que $n^2+1$ és primer, però $\int_2^{1000000} \frac{dx}{2\log(x)}$ surt 39313; si fem el quocient entre un i l'altre surt $1,37638$.
Això és perquè cal multiplicar per un factor que indiqui quants dels nombres són múltiples d'algun primer.

# Quants n'hi ha? Heurística millorada

Si $f(x)$ és un polinomi, i $p$ és un nombre primer, denotem per

$$\omega_f(p) := \#\{1 \leq m \leq p \mid f(m) \text{ és múltiple de } p\}.$$

Per exemple, $\omega_f(p) = p$ si i només si $f(n)$ és sempre divisible per $p$
Si $f(x) = x$, llavors $\omega_x(p) = 1$, doncs només hi ha un nombre divisible per $p$ (el $p$).
En canvi, si $f(x) = x^2 + 1$, llavors $\omega_f(p) = 1$ si $p = 2$, i és 2 o 0 la meitat de les vegades (per exemple $\omega_f(3) = \omega_f(7) = \omega_f(11) = 0$, i $\omega_f(5) = \omega_f(13) = 2$).
Com que volem tenir en compte tot els primers, prendre el següent producte infinit:

$$C_f := \prod_{p \text{ primer}} \frac{p - \omega_f(p)}{p - 1}$$

Observeu que si $f(n)$ és sempre divisible per un nombre primer $p$, llavors $C_f = 0$.

# Conjectura (Bateman- Horn)

Sigui $f$ un polinomi amb coeficients enters, irreductible i amb coeficients principal positiu. Llavors

$$\#\{2 \leq m \leq n \mid f(n) \text{ és primer } \} \approx \frac{C_f}{\deg(f)} \sum_{m=2}^{n} \frac{1}{\log(m)}$$

$$\approx \frac{C_f}{\deg(f)} \int_2^n \frac{dx}{\log(x)} \approx \frac{C_f}{\deg(f)} \frac{n}{\log(n)}$$

Per exemple, si calculem quan val (aproximadament) la constant $C_f$ per $f(x) = x^2 + 1$, surt que $C_f = 1,37281$, que quadra amb el que ens ha sortit abans.

Si ho fem amb $n^2 + 2$, aquí tenim que $w_f(p) = 2$ si $p = 3$, 11, 17, i $w_f(p) = 2$ si $p = 5$, 7, 13... La constant surt $C_f \approx 0.7132$.
Això explica perquè hi havia gairebé el doble de $n$'s tals que $n^2 + 1$ és primer que tal que $n^2 + 2$ és primer.

Finalment, el cas $n^2 + n + 1$ és encara més radical, doncs en surten el doble que en altres casos doncs $w_f(2) = 0$ (quan si és de la forma $n^2 + a$ per algun $a$ surt $w_f(2) = 1$); això fa que surti el doble del que surt en els casos $n^2 + a$ (per exemple, el cas $a = 3$).

# Altres conjectures: primers bessons

Una altre de les conjectures famoses diu que hi ha infinits primers $p$ tals que $p+2$ és primer. Diem que $(p, p+2)$ són primers bessons.
Per exemple, $(3,5)$, $(5,7)$, $(11,13)$, $(17,19)$, i molts altres.

De la mateixa manera, es pot generalitzar a hi ha infinits primers $p$ tals que $p+4$, o infinits primers $p$ tals que $p+6$, o fins i tot que hi ha infinits primers $p$ tals que $p+2$ i $p+6$ son primer.

Però no hi ha infinits primers $p$ tals que $p+2$ i $p+4$ són primers, ja que si $p>3$ és primer, llavors o $p+2$ o $p+4$ és múltiple de 3.

# Quants n'hi ha? Heurística

Podem fer un anàlisi similar al que hem fet abans per decidir quants nombres $n$ compleixen que $n$ i $n+2$ són primers alhora?

La idea és que el fet que $p$ i $p+2$ siguin primers poden ser considerats successos independents (no és ben bé cert, clar).

Llavors hem d'esperar que la probabilitat que $n$ i $n+2$ són primers alhora ha de ser el producte

$$\frac{1}{\log(n)}\frac{1}{\log(n+2)} \approx \frac{1}{(\log(n))^2}$$

# Conjectura explícita pels primers bessons

**Conjectura:**

$$\#\{3 \leq m \leq n \mid m \text{ i } m+2 \text{ són primers}\} \approx C_2 \frac{n}{(\log(n))^2}$$

on

$$C_2 = 2 \prod_{p \geq 3 \text{ primer}} \left(1 - \frac{1}{(p-1)^2}\right).$$

# Conjectura general de Bateman i Horn (1962)

Suposem que tenim $f_1(x)$, ..., $f_r(x)$ polinomis diferents amb coeficients enters, irreductibles i amb coeficient principal positiu. Llavors

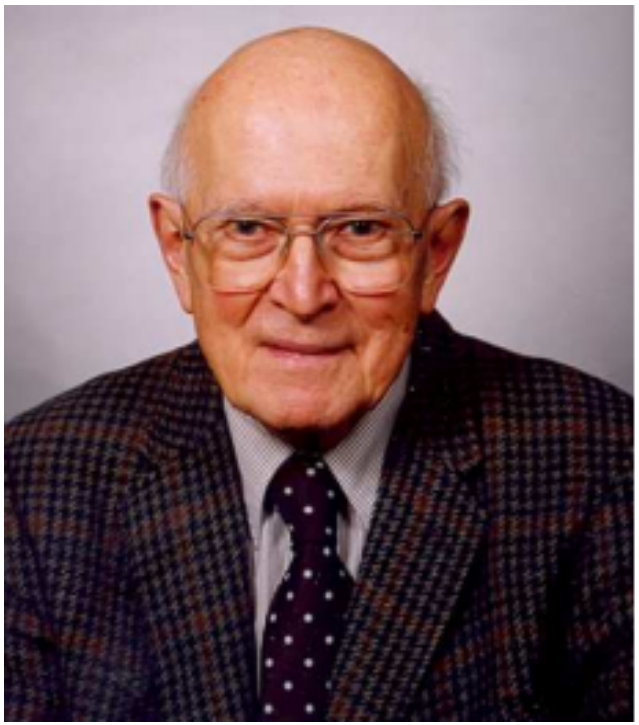
$$\#\{m \leq n \mid f_i(m) \text{ són primers per a tot } i = 1, \ldots, r\} \approx C_{f,r} \frac{n}{(\log(n))^r}$$

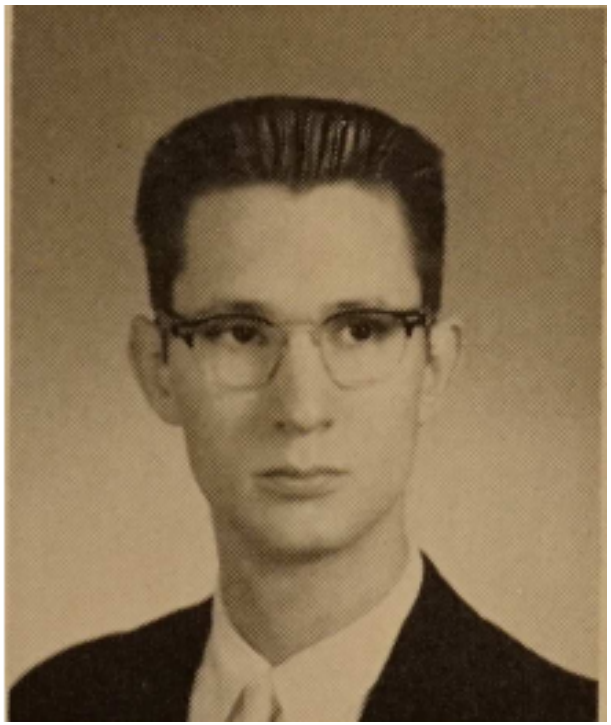
on

$$C_{f,r} := \prod_{p \text{ primer}} \left(1 - \frac{1}{p}\right)^{-r} \left(1 - \frac{w_f(p)}{p}\right)$$

on $f = f_1(x) \cdots f_r(x)$.

# Bateman i Horn





# Comparació amb els altres casos

Quan tenim només un polinomi, llavors $r = 1$, i surt que

$$C_{f,1} := \prod_{p \text{ primer}} \left(1 - \frac{1}{p}\right)^{-1} \left(1 - \frac{w_f(p)}{p}\right) =$$

$$= \prod_{p \text{ primer}} \left(\frac{p-1}{p}\right)^{-1} \left(\frac{p - w_f(p)}{p}\right) = \prod_{p \text{ primer}} \left(\frac{p - w_f(p)}{p-1}\right)$$

Quan tenim primers bessons, llavors $f(n) = n(n+2)$, i $w_f(2) = 1$, $w_f(p) = 2$ per a tot $p > 2$ primer. Per tant

$$C_{f,1} := \left(1 - \frac{1}{2}\right)^{-2} \left(1 - \frac{1}{2}\right) \prod_{p>2 \text{ primer}} \left(1 - \frac{1}{p}\right)^{-2} \left(1 - \frac{2}{p}\right) =$$

$$2 \prod_{p>2 \text{ primer}} \left(1 - \frac{1}{(p-1)^2}\right)$$

# Encara més conjectures: La conjectura de Goldbach

La conjectura famosa conjectura de Goldbach ens diu que tot nombre parell $> 2$ és suma de dos nombres primers.

De fet el Goldbach va conjecturar que tot nombre senar $> 7$ és suma de tres nombres primers, i va ser Euler qui va dir que probablement era cert el cas parell.

Aquesta darrera conjectura, per cert, ja s'ha demostrat recentment (el darrer pas el va fer un matemàtic peruà, Harald Helfgott, el 2013).

# Conjectura de Goldbach explícita

Hardy i Littlewood van conjecturar entre altres coses una fórmula pel nombre de maneres d'escriure un nombre parell $2n$ com a suma de dos primers. La conjectura diu que

$$\#\{p \leq n \mid p \text{ i } 2n-p \text{ son primers}\} = C_2 \left( \prod_{\substack{p>2 \text{ primer} \\ \text{que divideix } n}} \frac{p-1}{p-2} \right) \left( \frac{n}{(\log(n))^2} \right)$$

on $C_2$ és la constant que ja ha sortit al fer els primers bessons.

# Exemples

Si la conjectura de Hardy i Littlewood és correcte, podem esperar que amb nombres de mides similars, si $n$ és divisible per pocs primers llavors hi haurà menys maneres de fer-ho, i si és divisible per molts primers, n'hi haurà moltes.

Per exemple, si $n = 3 \cdot 5 \cdot 7 \cdot 11 = 1155$, llavors hi ha 114 parelles de primers $(p, q)$ tals que $p + q = 2n$ i $p \leq q$.

Si $n = 2^{10} = 1024$, llavors hi ha només 25 parelles de primers $(p, q)$ tals que $p + q = 2n$ i $p \leq q$.

Fins i tot si $n = 2^{11} = 2048$, hi ha només 53 parelles de primers $(p, q)$ tals que $p + q = 2n$ i $p \leq q$, menys de la meitat que el primer cas.

Moltes gràcies.