Desemmascarant els primers

Xavier Xarles

26 de Febrer del 2020

Els 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,

...

Primers Cosmològics (tan grans com estrelles hi ha a l'Univers)

$$218494118322706961732497$$

...

Primers Cosmològics (tan grans com partícules hi ha a l'Univers)

$$701463029369816474487648159898930073518561408552885045933638771327708804178323780296 77$$

...

Els nombres primers

Primers Criptogràfics!

971994546612005453879011741856132098756872659412125436153896
650743682428158316273110641914693801591269920797279063619671289810650570814935218321894916693479985714000482517807890429567252249595994432758983356682610636423361212601652357364400909396979939595375368811969578908955154959716792729419202815689276782426915252563462581129003594111248818253385972979766410749460849781050122095713202417268917718271494162992639697922253828252713373198601628971283206494771598749878554344248663537350882261773491

...

El nombre primer més gran (!)

$$2^{74207281} - 1 = 1^{(74.207.281 \text{ dígits } \dots)}1$$

escrit en binari.

Els primers són molt útils

És clar que els nombres primers són un pilar fonamental de les matemàtiques i que apareixen per tot arreu.

D'altra banda, els nombres primers grans s'utilitzen en la forma més extesa d'encriptació (de clau p+blica): el RSA. Per exemple, en la majoria de webs segures.

En l'actualitat es recomana que les claus RSA es construeixin amb nombres primers de més de 500 xifres decimals.

Mites sobre els primers

- Hi ha gent que compra primers grans.
- No hi ha mètodes bons per a trobar primers.
- Els primers són encara molt misteriosos.
- No coneixem realment com són els primers ja que hi ha moltes conjectures sobre ells.

Com saber si un nombre gran és primer

El Garbell d'Eratòstenes ens diu que un nombre és primer si no és divisible per cap (primer) més petit que la seva arrel quadrada.

NO SERVEIX DE RES (si el nombre té més de 60 xifres).
Hauríem de fer 10^{30} divisions. Si fem un mil·ló de divisions per segon, ens caldran 10^{24} segons. Però l'Univers té menys de 10^{21} segons!

Necessitem un mètode molt més ràpid.

Com saber si un nombre gran no és primer

És molt més fàcil veure que un nombre **no** és primer.

Sols cal tenir una propietat que verifiquin els nombres primers...
encara que hi hagi alguns nombres no primers que la verifiquin!

Pierre de Fermat 1601-1665

Petit Teorema de Fermat (18 d'octubre del 1640)

Si p és un nombre primer, i a és un nombre enter, aleshores

$$p \text{ divideix } a^p - a.$$

Pseudoprimers de Fermat

Un nombre n és un pseudoprimer de Fermat en base a si n és primer amb a i

$$a^{n-1} \equiv 1 \pmod{n}.$$

Hi ha molts compostos que no són pseudoprimers en base a.

Exemple

Si $n = 1635082058672300883899426002639999371369121606063247$
Aleshores
$2^{n-1} \equiv 139909189869604910587546742214976487961388480370558 6 \pmod{n}$
De fet
$n = 28986825866865994545282377 \times 56407764899202574427372311$

Podem fer-ho de manera eficient?

Ara tenim un "mètode" per descartar nombres n que no són primers

- Escollim un nombre a l'atzar a.
- Mirem si és pseudoprimer amb base a.
- Si surt que no, sabem que n és compost.
- Si surt que sí, repetim el procediment fins a convèncer-nos que potser és primer.

Es pot fer a la pràctica i en un temps acceptable aquest càcul?
Com ho podem fer per a calcular el residu de dividir a^{n-1} entre n quan n és un nombre enorme?

Càlcul de residus

El primer punt clau és adonar-nos que no cal calcular a^{n-1} i després el residu de dividir entre n; aquest nombre és enorme, i no ens hi cabria a la mèmoria de l'ordinador. El que podem fer és anar calculant els residus de les operacions intermèdies.
Això és gràcies a que és el mateix multiplicar dos nombres i calcular el seu residu de dividir entre n, que calcular primer els residus de dividir entre n cada nombre i després fer el producte.
D'aquesta manera mai ens caldrà treballar amb nombres més grans que n^2.
L'aritmètica amb els residus s'anomena aritmètica modular, i va ser desenvolupada per Carl Friedrich Gauss en el seu llibre *Disquisicions Aritmètiques* (hi ha traducció al català).

Exemple: l'aritmética dels rellotges

Imaginem que els metges d'un hospital decideixen fer torns de 7 hores.

Si el primer torn comença a les 00:00 hores, a quina hora començarà el torn número tres mil?

Una manera de calcular-ho és multiplicar 7 per 3000, i després calcular el residu de dividir-lo entre 24.

Una altra manera és calcular el residu de dividir 3000 entre 24, que és 0, ja que 24 divideix 3000. Per tant el residu buscat és 0, i per tant tornarà a ser les 12 de la nit.

Exponenciació binaria

Es pot calcular $a^n \pmod{n}$ molt ràpid (lineal en els nombres de bits de n).

- $Resultat = 1$
- Mentre $n > 1$
- Si n és senar
- $Resultat = Resultat \times a$
- $n = n - 1$
- $a = a^2$
- $n = n/2$
- $Resultat$

Algorisme per a trobar nombres primers industrials

Si volem un nombre primer n de N xifres decimals

1. Escollim un nombre n a l'atzar amb N xifres decimals.
2. Escollim un nombre a l'atzar a (menor que n).
3. Si a^{n-1} no és $\equiv 1 \pmod{n}$, tornem a 1.
4. Si ho és, n és un primer **industrial**.

Nombres de Carmichael

Hi ha nombres n que compleixen que són pseudoprimers per a tot a primer amb n, però no són primers.

$1105 = 5 \cdot 13 \cdot 17$

$1729 = 7 \cdot 13 \cdot 19$

$2465 = 5 \cdot 17 \cdot 29$

$2821 = 7 \cdot 13 \cdot 31$

$6601 = 7 \cdot 23 \cdot 41$

$8911 = 7 \cdot 19 \cdot 67$

N'hi ha infinits.

Pseudoprimers Forts

Podem millorar el criteri utilitzant que, mòdul un nombre primer, un nombre que el seu quadrat és congruent a 1 ha de ser congruent a ± 1. O sigui

$$\text{Si } a^2 \equiv 1 \pmod{p} \text{ i } p \text{ és primer, aleshores } a \equiv \pm 1 \pmod{p}.$$

Donat n primer senar, escrivim $n - 1 = 2^s \cdot d$ amb d senar. Aleshores, si a és un enter primer amb n,

- O bé $a^d \equiv 1 \pmod{n}$
- o bé

$$a^{2^r \cdot d} \equiv -1 \pmod{n}$$

per algun $0 \leq r \leq s - 1$.

Un nombre senar que passi el criteri anterior es diu que és un pseudoprimer fort en base a.

Algorisme millorat per a trobar nombres primers industrials

Si volem un nombre primer n de N xifres decimals

1. Escollim un nombre n a l'atzar amb N xifres decimals.
2. Escollim un nombre a l'atzar a (fins a 1000, per exemple).
3. Si n no és un pseudoprimer fort en base a, anem a 1.
4. Si ho és, n és un primer industrial fort.

Com d'efectiu es el mètode?

Quina és la probabilitat de trobar un nombre primer de n xifres?

Conjectura de Gauss

La probabilitat que un nombre de n xifres sigui primer és

$$\frac{1}{n\log(10)}$$

El Teorema dels nombres primers

Teorema (dels nombres primers)

(Jacques Hadamard i Charles Jean de la Vallée-Poussin)
Si denotem $\pi(x)$ la quantitat de nombres primers menors que x, aleshores $\pi(x) \sim \frac{x}{\log(x)}$ per $x \to \infty$.

Per tant, aproximadament, la probabilitat que un nombre menor que x sigui primer és $1/\log(x)$ (sempre que $x > 2$).

Així, com que $\log(10^{500}) \approx 1150$, la probabilitat que un nombre de 500 xifres sigui primer és aproximadament d'una entre 1150 (o de 575 si només agafem agafem senars).

Fixeu-vos que al doblar les xifres la probabilitat "només"es divideix per 2. Per tant si volem un amb 1000 xifres, ens caldrà aplicar el mètode amb senars sols unes 1150 vegades.

Com trobar nombres a l'atzar

Com ho fa l'ordinador per a trobar nombres "a l'atzar"?

Durant molt temps el que es feia era utilitzar funcions que donaven nombres **que semblaven** a l'atzar.

Aquests nombres s'anomenen nombres pseudo-aleatoris.

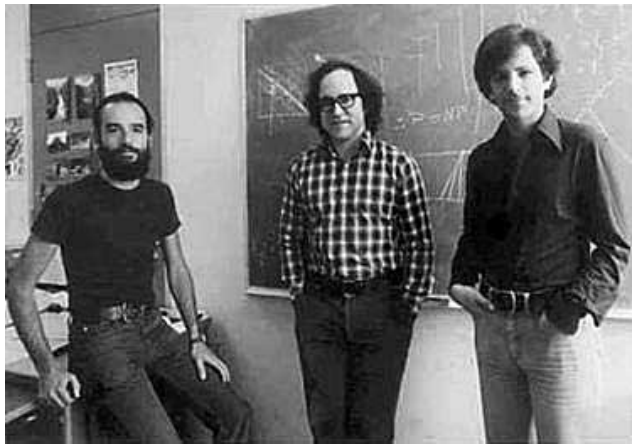
El problema que tenen és que de fet són deterministes; algù els podria reproduir!

Com trobar nombres a l'atzar

A l'actualitat hi ha varies eines per generar nombres a l'atzar

- Utilitzant informació exterior a l'ordinador, com el temps que es triga en apretar una tecla.
- Hi ha pàgines web que utilitzen informació no predictible, com la informació atmosfèrica: www.random.org
- Utilitzant efectes quàntics, com per exemple a random.irb.hr
- Utilitzant ordinadors quàntics. Ara per ara no està accessible.

Com es fan servir els nombres primers criptogràfics: RSA



Quan ens connectem a una pàgina segura fem servir normalment RSA.
RSA=Ron Rivest, Adi Shamir and Leonard Adleman

Es basa en que no hi ha métodes prou ràpids per a factorizar nombres grans (de 1000 xifres, productes de dos nombres primers d'unes 500 xifres).

Com es fan servir els nombres primers criptogràfics: RSA

Desenvolupat quatre anys abans per Clifford Cocks quan treballava per una agència de comunicacions del Regne Unit.

No es va saber fins que es va desclassificar el 1997.

No compris mai un nombre primer

Si utilitzes un nombre primer conegut per algú per construir la teva clau RSA, la teva clau és insegura.

Només podem confiar si els dos nombres que utilitzem els hem trobat nosaltres i **realment** a l'atzar.

El 2013, a Taiwan, es van poder factorizar fins a 184 claus RSA perquè els nombres primers havien estat generats amb un programa que de tant en tant en repetia.
L'únic que van fer va ser calcular el màxim comú divisor de parelles de tot de claus RSA fins que en van trobar alguna que no donava 1.

Multiplicar és fàcil, factoritzar és molt difícil!

Per multiplicar dos nombres es triga un temps que depèn de manera lineal del nombre de xifres.

Però per factoritzar un nombre que és producte de dos de mida similar, el temps que es triga depèn en forma exponencial del nombre de xifres.

El millor mètode per a factoritzar grans nombres (a l'atzar) és l'anomenat "Garbell general dels cossos de nombres".

El rècord!

El rècord absolut de factorització d'un nombre RSA (públic!) és del Novembre del 2019 amb 240 xifres decimals.

$$
\begin{aligned}
&124620366781718784065835044608106590434820374651678805754818788883289666801188210855036039570272508747509864768438458621054865537970253930571891217684318286362846948405301614416430468066875699415246993185704183030512549594371372159029236099\\
&=\\
&509435952285839914555051023580843714132648382024111473186660296521821206469746700620316443478873837606252372049619334517\\
&\times\\
&244624208838318150567813139024002896653802092578931401452041221336558477095178155258218897735030590669041302045908071447
\end{aligned}
$$

Van caldre uns 900 anys de computació.

Com demostrar que un nombre és primer.

Teorema (Lucas)

Donat $n > 1$ enter, si existeix un enter $a > 1$ tal que $a^{n-1} \equiv 1 \pmod{n}$ i per a tot primer p dividint $n-1$ $a^{(n-1)/p}$ no és $\equiv 1 \pmod{n}$, aleshores n és primer.

De fet sols cal veure-ho per suficients primers: pels primers dividint m de manera que $n - 1 = md$, amb $m > \sqrt{n}$.(Pocklington)
Determinar el nombres primers que divideixen $n-1$ pot ser molt díficil!

El problema de veritat és saber factoritzar, no trobar primers!

Certificats de primalitat

Si després de 3 mesos de càlculs per a saber si un nombre és primer l'ordinador respon SI utilitzant el teorema anterior, això és una **demostració** que és primer?

Si ens escriu la factorització de $n-1$, la llista de primers que el divideixen, i els a's utilitzats, qualsevol ordinador ho pot comprovar en qüestió de milisegons. Potser caldrà escriure això mateix pels primers en la llista de primers anteriors.

Això és un certificat de primalitat.

Un exemple de certificat

Considerem $n = 6271$.
Aleshores $n - 1 = 11 \cdot 19 \cdot 30$ i $30 < \sqrt{n} \approx 71$.
Ara $d_1 := (n-1)/11 = 570$ i $d_2 := (n-1)/19 = 330$.
Calculem

$$2^{d_1} = 2^{570} \equiv 4365 \pmod{6271}$$

$$2^{d_2} = 2^{330} \equiv 5016 \pmod{6271}$$

mentre que

$$2^{n-1} \equiv 1 \pmod{6271}$$

Per tant 6271 és primer.

Els primers són P

Els mètodes anteriors per a veure que un nombre és primer són molt lents i, el que és pitjor, augmenten exponencialment amb les xifres de n.
Hi ha mètodes que són en temps polinomial, o sigui que augmenten polinomialment amb les xifres de n.

Teorema de Miller

Si un nombre n és pseudoprimer fort en base a per a tot $2 \leq a \leq 2(\ln(n))^2$, aleshores és primer.
Si la conjectura generalitzada de Riemann és certa.

Teorema AKS

Hi ha un algorisme (determinista) que en temps polinomial determina si un nombre és primer.

A cops la Certesa

Ens oculta la Veritat