5. Quan 1+1 no són dos. El DNI electrònic.

Hom coneix aquell refrany popular que diu que "dos més dos són quatre", com una manera de reafirmar que la certesa del que s'acaba de dir no té cap dubte. Però això en matemàtiques no sempre és cert, en particular quan no podem fer feina amb un nombre infinit de valors.

En el llenguatge de l'amor pareix que tampoc no regeixen las lleis universals de l'*Àlgebra* i de l'*Aritmètica*, ja que en el amor 1+1 és *infinit* mentre que 2–1 és *cero* (Segons *Lope de Vega*; el, o la, que ha estimat i ha sofert la pèrdua del seu amor ho sap bé). I si hi ha fills 1+1=3, 4, 5... I és que l'amor és inefable i no solament està més allà de l'À*lgebra* i de l'*Aritmètica*, sinó que, parafrasejant a *Nietzche* està inclús més allà del be i del mal.

I en la lògica binària usada en els ordinadors, 1+1= 0. I així ens va de bé. I si tinguéssim que fer feina amb lògica ternària, les operacions que faríem serien:

$+_3$	**0**	**1**	**2**
0	0	1	2
1	1	2	**0**
2	2	0	**1**

Això vol dir que fer feina amb un sistema de només tres números {0,1,2} i la suma entre ells és **el valor la resta de la seva divisió per tres** (com es pot comprovar en la taula anterior: **$2+_3 2$=resta(4/3)=1**).
Aquesta operació s'expressa com: **$a+_3 b$ =a+b mòd 3.**

Nota: Observar que en l'aritmètica mòdul 3:

$-2 = 1$, ja que $2+_3 1 = 0$
$½ = 2$, ja que $2 \cdot_3 2 = 1$.

5.1 Aritmètica modular

Aquesta aritmètica es refereix a la manera de comptar com en els rellotges. Quan a les 10 del matí començam una passejada i ens dura 6hores, farem 10+6=16; però usualment direm: hem arribat a les 4 de l'horabaixa (de fet hem dividit 16 per 12 i ens hem quedat amb la resta de la divisió). D'altra manera, si diem que hem arribat al lloc a les 4 de l'horabaixa i hem trigat 6 hores en fer l'excursió, ràpidament deduirem que s'havia començat a les 10 del matí (4-6=10?).

Aqueta aritmètica del rellotge es diu, normalment "**aritmètica mòdul 12**" i es treballa en el conjunt Z_{12}={0,1,2,3,4,5,6,7,8,9,10,11}, que són els possibles restes de divisió de qualsevol número sencer per 12. Així, 29 i 5 són el mateix número a Z_{12}, la qual cosa s'expressa: **29 mòd 12 = 5** (ja que al dividir 29 per 12 ens dona de resto 5).

En aquest conjunt Z_{12} podem sumar, restar i multiplicar (dividir ja són figues d'un altre paner!. Només podrem dividir si fem l'aritmètica modular amb un nombre primer, com ara el cas de fer mòdul 3).

Operativa modular

Z_n= Enters mòd n = {restes de divisió per n} = {0,1,2,3…,n-1}

(a op b) mòd n = [(a mòd n) op (b mòd n)] mòd n, on op={+,·}

*Exemple***:** suma amb n=12
(23 +19) mòd 12 = 42 mòd 12 = **6**
[(23 mòd 12) + (19mòd 12] mòd 12 =
[11 + 7] mòd 12 = 18 mòd 12 = **6**

Exemple: producte amb n=12
(23 ·19) mòd 12 = 437 mòd 12 = **5**
[(23 mòd 12) + (19mòd 12)] mòd 12=
[11 · 7] mòd 12 = **5**

Com restarem?....; tenint en compte que **-a mòd 12= (12-a) mòd 12**

Exemple: resta amb n=12
(34 - 19) mòd 12 = 15 mòd 12 = **3**
[(34 mòd 12) - (19mòd 12] mòd 12 =
[10 +(-7 mòd 12)] mòd 12 = [10 + (12-7)] mòd 12 = 15 mòd 12 = **3**

Veurem aquest tipus d'operacions per calcular codis numèrics (ref: *Article:* ***Códigos numéricos para la vida*** *(Suma$^+$, febrer 2008, pp.43-54),* ***Jesús Beato Sirvent, IES Bahía de Cádiz, Cádiz),*** usats en la vida quotidiana, al qual estem acostumats, però no hi parem massa atenció.

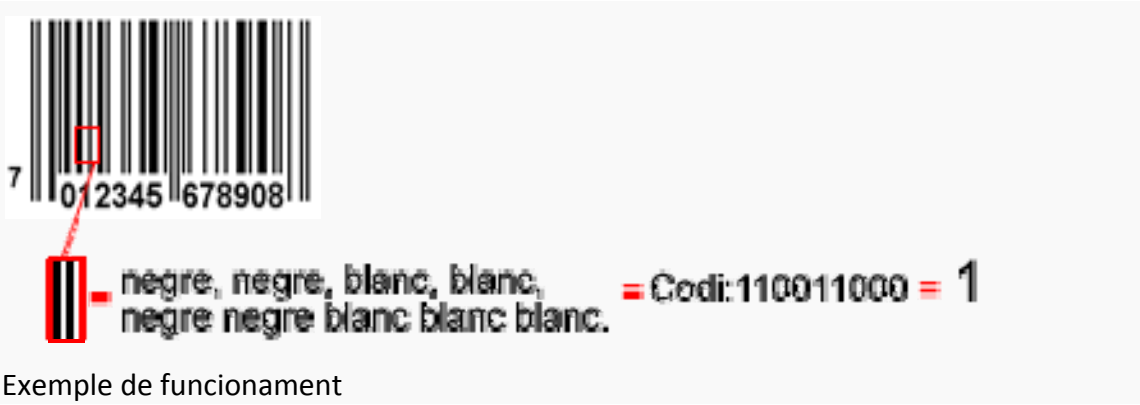
Tals codis seran, per exemple:

1. El càlcul del dígit de control d'un xec bancari, on s'utilitza el sistema {0,1,2,3,4,5,6}, amb l'operació $+_7$.
2. El càlcul de la lletra de control del DNI, on s'utilitza el sistema {0,1,2,3,...,22}, amb l'operació $+_{23}$
3. El codi de barres dels productes del mercat, on s'utilitza el sistema el sistema {0,1,2,3,...,9}, amb l'operació $+_{10}$

El **codi de barres** és un sistema d'identificació numèrica adaptat per tal de poder ser llegit ràpidament mitjançant un sistema òptic-electrònic, bàsicament per rajos làser. Aquest conegut sistema d'identificació va ser patentat a l'any 1949, però la generalització del codi de barres tal i com el coneixem, no va arribar fins al 1977. La idea està inspirada en el codi Morse, però en aquest cas el senyal que conté la informació és lluminós en comptes d'acústic.

Aquest codi està construït a partir d'una seqüència de senyals que varien en el temps de durada. Una combinació d'aquests senyals curts i llargs dóna lloc a una lletra o a un número.

De forma similar, els codis de barres no són altra cosa que un conjunt de bandes blanques i negres de diferent gruix. Un cop processada la informació digitalment, el blanc serà traduït per un 0 i el negre per un 1. Cada número del codi està constituït per set dígits binaris (al dibuix: codi), que, tot i definir només deu números (del 0 al 9), podrien donar lloc a un total de 128 combinacions.



Exemple de funcionament

La lectura es du a terme mitjançant un feix de llum làser. El làser surt del lector i recorre la superfície del codi a gran velocitat. Les bandes negres absorbeixen totalment la llum que arriba, mentre que les blanques la reflecteixen de nou cap al lector. A més de detectar la llum que arriba, el lector conté un cronòmetre intern que li permet quantificar el temps d'arribada o absència de llum i relacionar-ho així amb una banda més ampla o més prima. Finalment, els zeros i uns de les zones blanques i negres són traduïts als números del codi.

El codi de barres més usat en l'actualitat és el EAN-13, i conté 13 dígits. Aquest codi s'expressa: $\mathbf{a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}a_{11}a_{12}\text{-}c}$ de manera que a_i i c són valors a {0,1, 2,..., 9}.

El significat dels dígits és:

a1a2 indiquen el país on s'ha sol·licitat el codi (el prefix d'Espanya és 84).
a3a4a5a6a7 representen el codi assignat a l'empresa.
a8a9a10a11a12 representen el codi assignat al producte
c és el dígit de control.

El càlcul del dígit de control c, a partir dels dotze dígits es fa:

1. Calcular S: S= (a1+a3+a5+a7+a9+a11)+3(a2+a4+a6+a8+a10+a12)
2. S'agafa la resta de dividir S entre 10

Aleshores: Si R = 0 => c = 0
Si R ≠ 0 => c=10-R

És a dir, es sumen els valors senars, amb els triple dels valors parells, i el símbol de control és el que li falta per arribar a la següent desena.

La primera patent de codi de barres va ser registrada el 7 d'octubre de 1952 com a mètode per identificar els vagons de ferrocarril.

El 1961 apareix el primer escàner fix de codis de barres que llegia barres de colors vermell, blau, blanc i negre identificant vagons de ferrocarrils.

El 1967 l'Associació de Ferrocarrils d'Amèrica del Nord aplicà codis de barres pel control de trànsit d'embarcaments. El projecte no va durar molt per manca d'un adequat manteniment de les etiquetes que contenien els codis.

El 1969, el làser fa la seva aparició i a començaments dels 70 van aparèixer les primeres aplicacions industrials però només per maneig d'informació i al a control de arxius en organismes militars el 1971. La seva aplicació es va difondre per a control de documents en biblioteques i troba la seva major aplicació en els bancs de sang, on un mitjà d'identificació i verificació automàtica eren indispensables.

L'any 1973 s'anuncia el codi UPC. (*Universal Product Code*) que es convertiria en l'estàndard de identificació de productes. D'aquesta manera la actualització automàtica d'inventaris permetia una millor i més oportuna compra i abastiment de béns. Europa es fa present amb la seva pròpia versió d'UPC El 1976, el codi EAN (*European Article Number*).

El primer sistema patentat de verificació de codis de barres per mitjà de làser apareix al mercat el 1978. Apareix la norma ANSI que especifica les característiques tècniques dels codis de barres i el primer codi bidimensional.

El 1990 es publica l'especificació ANSI X3.182, que regula la qualitat d'impressió de codis de barres lineals. En aquest mateix es presenta el codi bidimensional..

Codi de barres de dues dimensions (*Semacode*)

El tipus de codis bidimensionals que en l'actualitat tenen un major desenvolupament són els codis QR (*Quick Response*)que consisteixen en matrius de dades bidimensionals. Amb els codis QR, dupliquem la dimensió d'un codi de barres, es a dir es com un codi que s'ha de llegir no nomes horitzontalment com en el cas dels codis de barres sinó que al mateix temps s'ha de fer verticalment, això fa que la quantitat de informació que poden emmagatzemar sigui molt superior a la dels convencionals codis de barres.

Els codis QR els va crear la companyia japonesa Denso-wave l'any 1994, per això avui en dia al Japó ja són molt comuns.

Un exemple d'utilització pot ser: vas caminant pel carrer i trobes un anunci publicitari d'algun producte que t'agradi, simplement fent una foto amb el teu mòbil del codi QR, tindràs accés a tota la informació del producte, pagina web del fabricant, on comprar, preu, etc.

Si als anys 50 es va viure la revolució dels codis de barres, que van implantar-se arreu per la seva forma ràpida i senzilla d'accedir a la informació, ara es hora que és l'hora dels codis QR substituint, poc a poc, els codis de barres i aportant-nos molta mes informació.

Capacitat d'emmagatzemar dades del codi QR:

- Dades numèriques 7089 caràcters.
- Dades Alfanumèriques 4296 caràcters.
- Dades Binàries (8) bits 2953 bytes
- Kanjis/kanas (caràcters japonesos) 1817 caràcters

5.2 El DNI electrònic.

Amb l'arribada de la Societat de la Informació i la generalització de l'ús d'Internet es fa necessari adequar els mecanismes d'acreditació de la personalitat a la nova realitat i disposar d'un instrument eficaç que traslladi al món digital les mateixes certeses amb les quals operem cada dia en el món físic i que, essencialment, són:

- Acreditar electrònicament i de forma indubtable la identitat de la persona.

- Firmar electrònicament documents, atorgant-los una validesa jurídica equivalent a la qual els proporciona la firma manuscrita.

Per a respondre a aquestes noves necessitats neix el Document Nacional d'Identitat electrònic (DNIe), similar al tradicional i la principal novetat de la qual és que incorpora un petit circuit integrat (xip), capaç de guardar de forma segura informació i de processar-la internament.

La informació que conté el xip són, bàsicament les dades de filiació del titular, la imatge digitalitzada de la fotografia, la imatge digitalitzada de la firma manuscrita, la plantilla de la impressió dactilar dels dits índex de cada ma, un certificat qualificat per a autenticació i un altre per la firma, un certificat electrònic de l'autoritat emissora i el parell de claus criptogràfiques (públiques i privades) associades al titular. El fet que hi hagi dos certificats és per què el ciutadà pugui diferenciar les activitats d'autenticació i de firma electrònica.

Les claus criptogràfiques són números calculats basats en nombres primers molt grans (centenars de xifres), amb certes propietats que ens permeten la confidencialitat i la integritat de la informació, al mateix temps que l'autenticació de l'usuari que l'emet.

Per a poder incorporar aquest xip, el Document Nacional d'Identitat canvia el seu suport tradicional (cartolina plastificada) per una targeta de material plàstic, dotada de noves i majors mesures de seguretat. A aquesta nova versió del Document Nacional d'Identitat ens referim com DNI electrònic.

El DNI electrònic no conté informació relativa a dades personals distintes a les que apareixen impresos en la pròpia targeta, ni dades sanitàries, ni fiscals, ni judicials, ni penals, ni infraccions de tràfic, ..., de moment.

En la mesura que el DNI electrònic vagi substituint al DNI tradicional i s'implantin les noves aplicacions, podrem utilitzar-lo per a:

- Realitzar compres signades a través d'Internet.
- Fer tràmits complets amb les Administracions Públiques a qualsevol hora i sense haver de desplaçar-se ni fer cues
- Realitzar transaccions segures amb entitats bancàries
- Accedir a l'edifici on treballem
- Utilitzar de forma segura el nostre ordinador personal
- Participar en interaccions en Internet amb la certesa que el nostre interlocutor és qui diu ser

Qüestió: Però, i com podem firmar electrònicament per tal de garantir la identitat amb la mateixa validesa jurídica que ens proporciona la firma manuscrita?

Resposta: Utilitzant la de clau criptogràfica de firma, guardada en el xip del DNIe.

Les claus criptogràfiques i la firma electrònica.

De manera senzilla, a través d'un exemple, veurem cóm funciona. La idea és basada en propietats dels números primers que va descobrir el matemàtic i físic Suís (el mateix pare dels *sudokus*), *Leonard Euler(1707-1783).*

Cada usuari fa:

1. Tria dos números primers: p i q. Els guarda ben guardats, i calcula $n=p\cdot q$ que no té cap problema en fer públic.
2. Calcula $\phi=(p-1)\cdot(q-1)$, i el guarda ben guardat.
3. Agafa un valor e, que tothom pot conèixer, i calcula d que és l'invers de e mòdul ϕ. Guarda d, ben guardat.
4. La clau pública és (n,e), mentre que la clau privada és (d,n).
5. La firma electrònica de l'usuari es basa en (d,n)

   Per firmar m, farà: **$s= m^d$ mòd n**. Evidentment, això només ho podrà fer qui coneix d.
   Qui rep m i s, pot verificar qui l'ha enviat. Cerca el valor públic **e**, i fa: **s^e mòd n**. Si el resultat coincideix amb m, dóna la verificació per bona; sinó la rebutja.
   Euler assegura que, tal com hem construït les coses, $[(m)^d \text{ mòd } n]^e \text{mòd } n = m$

On és la trampa?. Que només pot calcular d, qui coneix ϕ, i ϕ només el pot calcular qui coneix p i q.

Un exemple (amb números petits, és clar).

1. Tria dos números primers: 23 i 31. Els guarda ben guardats, i calcula $n=23\cdot31=713$, que no té cap problema en fer públic.
2. Calcula $\phi=22\cdot30=660$, i el guarda ben guardat.
3. Agafa un valor e=7, que tothom pot conèixer, i calcula d que és l'invers de e mòdul ϕ. Guarda **d=283**, ben guardat.
4. La clau pública és (7, 713), mentre que la clau privada és **(283,713).**
5. La firma electrònica de l'usuari es basa en **(283,713).**

Suposem que vol firmar el valor m=10, aleshores farà

s= m^d mòd n = 10^{283} mòd 713 = 412.

Envia **m=10** i **s= 412**

Qualsevol pot verificar la firma de m, fent**:** 412^7 mòd 713 que és **= 10**

Com que el resultat coincideix amb m, la dona per bona

Encara que tot sembli senzill, parlarem un poc de les dificultats i de les solucions per fer feina, de manera efectiva, amb números tan grans.

.