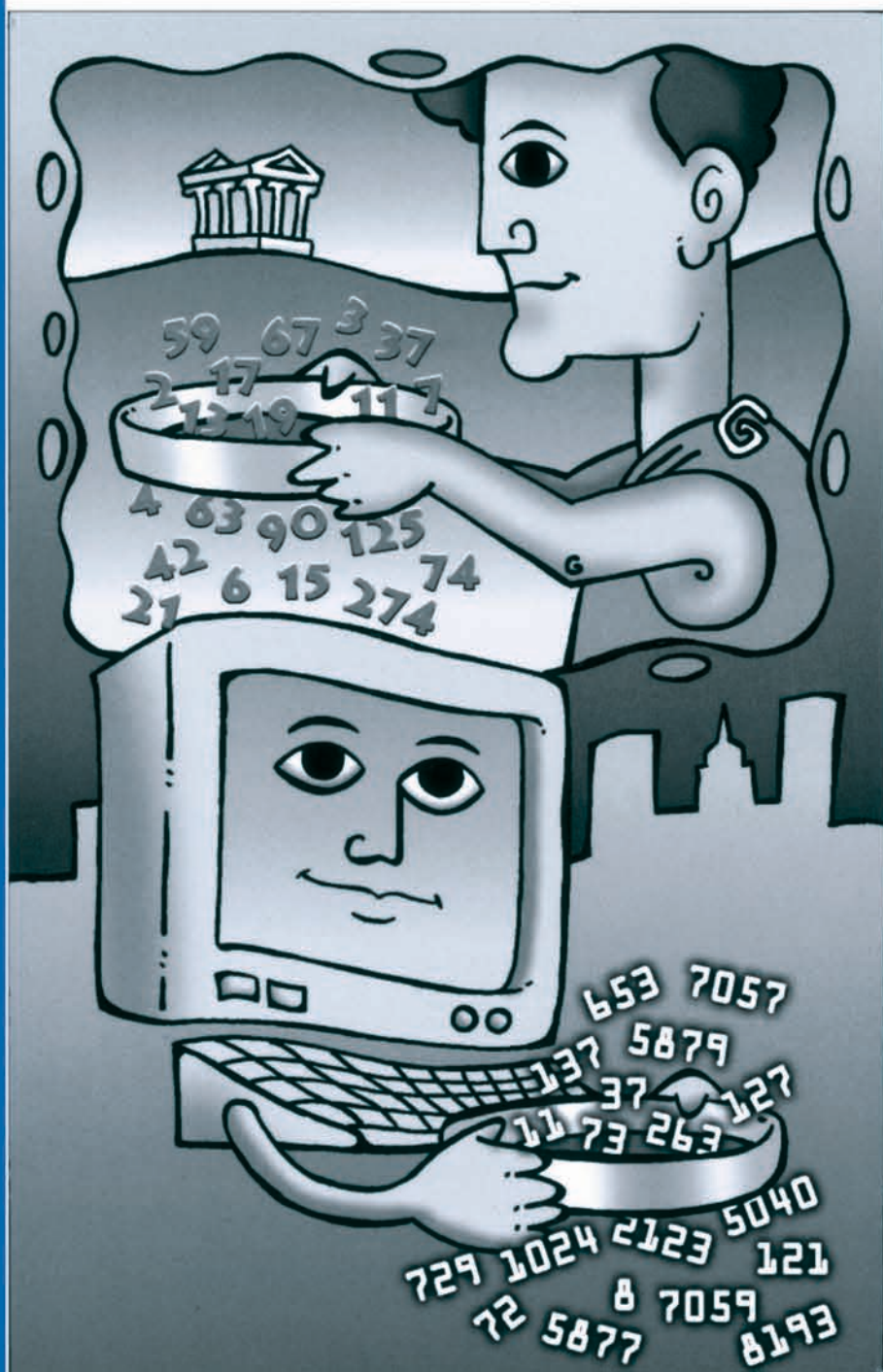


Aritmètica

Artur Travesa



Contingut

	Pàg.
INTRODUCCIÓ	1
CAPÍTOL I: ELS NOMBRES ENTERS	7
§1: La divisió euclidiana	9
§2: Representació dels nombres enters	14
§3: La suma en multiprecisió	19
§4: La multiplicació en multiprecisió	27
§5: La divisió entera en multiprecisió	31
§6: Algoritme binari d'exponenciació	38
§7: Complementos i exercicis	42
CAPÍTOL II: DIVISIBILITAT I NOMBRES PRIMERS ...	47
§1: Múltiples i divisors	47
§2: L'algoritme d'Euclides	52
§3: Nombres primers	60
§4: El teorema fonamental de l'Aritmètica	67
§5: Distribució de primers	72
§6: El teorema de Chebychev	79
§7: Complementos i exercicis	84
CAPÍTOL III: CONGRUÈNCIES	89
§1: Definició i propietats bàsiques	89
§2: El calendari	93
§3: Congruències lineals	101
§4: El teorema xinès del residu	110
§5: L'aritmètica modular	113

§6: El teorema de Goldbach	123
§7: Complementos i exercicis	125
CAPÍTOL IV: ARRELS PRIMITIVES	133
§1: La funció phi d'Euler	133
§2: Els teoremes de Fermat i d'Euler	139
§3: Arrels primitives	141
§4: Existència d'arrels primitives	147
§5: Aplicacions	152
§6: Connexió de línies telefòniques	159
§7: Complementos i exercicis	165
CAPÍTOL V: CONGRUÈNCIES QUADRÀTIQUES	169
§1: Congruències polinòmiques	169
§2: Congruències quadràtiques	176
§3: El símbol de Legendre	177
§4: La llei de reciprocitat quadràtica	184
§5: El símbol de Jacobi	190
§6: Càlcul d'arrels quadrades	196
§7: Complementos i exercicis	203
CAPÍTOL VI: PRIMERITAT	207
§1: Intentem la divisió	207
§2: Nombres pseudoprimers i nombres de Carmichael	210
§3: Test de Solovay–Strassen	216
§4: Nombres fortament pseudoprimers	221
§5: Test de Miller–Rabin	233
§6: Complementos i exercicis	235
CAPÍTOL VII: CERTIFICATS DE PRIMERITAT	239
§1: Càlcul d'arrels primitives	239
§2: Certificat de Pocklington-Lehmer	244
§3: Nombres de Fermat	248
§4: Nombres de Mersenne	252
§5: Prova del criteri de Lucas-Lehmer	256
§6: Complementos i exercicis	261

CAPÍTOL VIII: FACTORITZACIÓ (I)	265
§1: Intentem la divisió	265
§2: Mètode de Fermat	271
§3: Bases de factors	275
§4: Fraccions continuades	281
§5: Mètode de Brillhart-Morrison	288
§6: Mètode rho de Pollard	290
§7: Complementos i exercicis	295
 CAPÍTOL IX: FACTORITZACIÓ (II)	299
§1: Mètode $p-1$ de Pollard	299
§2: Corbes el·líptiques	305
§3: Mètode de factorització de Lenstra	312
§4: Anàlisi del mètode	317
§5: El garbell quadràtic	323
§6: El garbell quadràtic multipolinòmic	329
§7: Complementos i exercicis	332
 CAPÍTOL X: EQUACIONS DIOFANTINES	337
§1: Equacions diofantines lineals	337
§2: L'equació pitagòrica	343
§3: Interpretació geomètrica	346
§4: El mètode del descens	350
§5: Ternes d'Euler i Fermat	352
§6: Sumes de quadrats	357
§7: Complementos i exercicis	366
 REFERÈNCIES	371
 ÍNDEX TERMINOLÒGIC	375

Congruències

Sovint solem agrupar en una mateixa definició objectes o conceptes diferents per raons de ciclicitat. Per exemple, del tercer dia de cada setmana en diem dimecres; encara que tots els dimecres són dies diferents, els agrupem en un nou concepte. El llenguatge de les congruències, desenvolupat per Gauss a final del segle XVIII, proporciona una eina còmoda per al tractament d'aquests fenòmens i està íntimament relacionat amb la divisibilitat. Dediquem aquest capítol al seu estudi i al d'algunes aplicacions pràctiques.

§1. Definició i propietats bàsiques

Comencem amb la definició de congruència entre dos nombres enters mòdul un altre nombre enter.

1.1. Definició. Sigui N un nombre enter. Donats nombres enters a , b , direm que a és congru a b mòdul N , i escriurem $a \equiv b \pmod{N}$, si, i només si, $a - b$ és múltiple de N . En altres paraules, a és congru a b mòdul N si, i només si, $a - b$ pertany a l'ideal de $\mathbb{Z}$ generat per N . En particular, dir que $a \equiv 0 \pmod{N}$ és el mateix que dir que a és múltiple de N ; o sigui, que a pertany a l'ideal generat per N .

1.2. Exemples. En el cas que el mòdul és $N = 0$, la congruència $a \equiv b \pmod{0}$ és equivalent a la igualtat $a = b$, ja que l'únic múltiple de 0 és 0. Si el mòdul és $N = \pm 1$, les congruències $a \equiv b \pmod{1}$ i $a \equiv b \pmod{-1}$ se satisfan per a tota parella de nombres enters a , b , perquè qualsevol nombre enter és múltiple de 1 i de -1 .

1.3. Observació. En el cas que $N \neq 0$, dir que $a \equiv b \pmod{N}$ és el mateix que dir que a i b donen el mateix residu en fer la divisió entera per N .

En efecte, siguin $a = Nq_1 + r_1$ i $b = Nq_2 + r_2$ les divisions enteres de a i de b entre N ; llavors, dir que $a \equiv b \pmod{N}$ és dir que $a - b$ és múltiple de N ; o, equivalentment, que la diferència $(a - b) - N(q_1 - q_2) = r_1 - r_2$ és múltiple de N ; i, com que $0 \leq |r_1 - r_2| < |N|$, això equival a dir que $r_1 = r_2$. $\square$

El signe $\equiv$ que es fa servir per a indicar les congruències fa pensar en el signe d'igualtat. Certament, aquests dos símbols tenen moltes propietats comunes. En particular, escriurem $a \not\equiv b \pmod{N}$ per a indicar que a i b no són congrus mòdul N . La demostració de la proposició següent, en què s'estableixen propietats de les congruències anàlogues a les de la igualtat, es deixa com a exercici per al lector.

1.4. Proposició. *Sigui N un nombre enter. La relació de congruència mòdul N és una relació d'equivalència; és a dir, si a , b , c són nombres enters qualssevol, se satisfan les propietats següents:*

- (a) *Reflexiva:* $a \equiv a \pmod{N}$;
- (b) *Simètrica:* si $a \equiv b \pmod{N}$, aleshores $b \equiv a \pmod{N}$; i
- (c) *Transitiva:* si $a \equiv b \pmod{N}$ i $b \equiv c \pmod{N}$, aleshores $a \equiv c \pmod{N}$. $\square$

Les relacions de congruència són compatibles amb les operacions aritmètiques de sumar i multiplicar en $\mathbb{Z}$; de fet, la seva gran importància es deriva d'això.

1.5. Proposició. *Siguin a, b, c, d, N nombres enters. Se satisfan les propietats següents:*

- (a) *Si $a \equiv b \pmod{N}$, aleshores $a + c \equiv b + c \pmod{N}$.*
- (b) *Si $a \equiv b \pmod{N}$, aleshores $ac \equiv bc \pmod{N}$.*
- (c) *Si $a \equiv b \pmod{N}$ i $c \equiv d \pmod{N}$, aleshores $a + c \equiv b + d \pmod{N}$.*
- (d) *Si $a \equiv b \pmod{N}$ i $c \equiv d \pmod{N}$, aleshores $ac \equiv bd \pmod{N}$.*

DEMOSTRACIÓ. La demostració de la propietat (a) és immediata, ja que $(a+c)-(b+c) = a-b$. Per a veure la propietat (b) només cal observar que si $a-b$ és múltiple de N , llavors $(a-b)c = ac-bc$ també ho és. Demostrem les altres dues; suposem que $a-b$ i $c-d$ són múltiples de N ; aleshores, la seva suma $(a+c)-(b+d)$ és múltiple de N , i això demostra (c), i la combinació lineal $(a-b)c+b(c-d) = ac-bd$ també ho és, fet que demostra (d). $\square$

1.6. Corol·lari. *Siguin a, b, N nombres enters i sigui $f(X) := a_0 + a_1X + \dots + a_nX^n$ un polinomi qualsevol de coeficients enters $a_0, \dots, a_n$. Si $a \equiv b \pmod{N}$, aleshores $f(a) \equiv f(b) \pmod{N}$.*

DEMOSTRACIÓ. Si tenim en compte les propietats de **1.5**, és suficient demostrar que per a tot nombre natural $k \geq 2$ és $a^k \equiv b^k \pmod{N}$. I això és senzill, ja que $a^k - b^k = (a-b)(a^{k-1} + a^{k-2}b + \dots + ab^{k-2} + b^{k-1})$, de manera que si $a-b$ és múltiple de N , també ho és $a^k - b^k$. $\square$

A tall d'il·lustració de la gran utilitat que té el llenguatge de les congruències, i malgrat que només n'hem demostrat algunes (poques) propietats, que ensenyen que la congruència és semblant a la igualtat, podem donar-ne immediatament una aplicació important.

1.7. Proves de divisibilitat per 9 i per 3. *Sigui $N = a_0 + a_110 + a_210^2 + \dots + a_r10^r$ l'expressió decimal d'un nombre enter N . Aleshores, N és múltiple de 9, respectivament, de 3, si, i només si, la suma de les seves xifres, $a_0 + a_1 + \dots + a_r$, també ho és.*

DEMOSTRACIÓ. En efecte, com que $10 \equiv 1 \pmod{9}$, obtenim que $10^k \equiv 1^k = 1 \pmod{9}$, de manera que $N \equiv a_0 + a_1 + \dots + a_r \pmod{9}$. Per tant, la congruència $N \equiv 0 \pmod{9}$ equival a la congruència $a_0 + a_1 + \dots + a_r \equiv 0 \pmod{9}$. La mateixa demostració serveix canviant el mòdul 9 per 3. $\square$

Un criteri de divisibilitat per 11 per a nombres escrits en el sistema decimal s'obté de manera anàloga; en deixem la demostració com a exercici.

1.8. Exercici. Proveu que un nombre enter $N := a_0 + a_110 + a_210^2 + \dots + a_r10^r$ és múltiple de 11 si, i només si, la suma alternada $a_0 - a_1 + a_2 - \dots +$

$(-1)^r a_r$ també ho és. Cal que els nombres a_i siguin *les xifres* decimals de n ?

1.9. Observació. El gran avantatge d'aquests criteris de divisibilitat es troba en la seva recursivitat i, sobretot, quan es vol aplicar a nombres molt grans. En efecte, per a tot nombre natural N , la suma de les seves xifres decimals és un nombre natural menor o igual que N , amb igualtat si, i només si, $0 \leq N \leq 9$; és a dir, si N consta d'una sola xifra decimal (cf. l'exercici següent). Anàlogament, el valor absolut de la suma alternada de les xifres decimals de N és un nombre natural menor o igual que N (cf. l'exercici 1.12). Per tant, podem repetir el procediment amb el nombre $a_0 + a_1 + \cdots + a_r$, o amb $\pm(a_0 - a_1 + a_2 - \cdots + (-1)^r a_r)$, segons el cas, i iterar el procediment fins que només resta una sola xifra decimal; i, en aquest cas, la propietat de divisibilitat es comprova de manera trivial.

1.10. Exercici. Demostreu que si N és un nombre natural qualsevol, la suma de les seves xifres decimals és un nombre natural menor o igual que N , amb igualtat si, i només si, N consta d'una sola xifra decimal.

1.11. Exercici. Més generalment, proveu que si N és un nombre natural qualsevol i $b > 1$ és un nombre enter, que prendrem com a base de numeració, la suma de les xifres en base b de N és un nombre natural menor o igual que N , amb igualtat si, i només si, N consta d'una sola xifra en base b .

1.12. Exercici. Demostreu que si N és un nombre natural qualsevol i $b > 1$ és un nombre enter, el valor absolut de la suma alternada de les xifres de N en base b és un nombre natural menor o igual que N , i que si hi ha igualtat és $0 \leq N < b$.

1.13. Exemple. Per quins dels tres nombres 3, 9, 11, és divisible el nombre

83675 95445 09835 94567 34568 92843 84687 12349 09623 98347 ?

Si anomenem N aquest nombre, la suma de les seves xifres decimals és el nombre 267; la suma de les xifres decimals de 267 és 15, i la suma de

les de 15 és 6, que és un nombre divisible per 3 però no per 9. Per tant, N és divisible per 3 però no ho és per 9. D'altra banda, la suma alternada de les xifres decimals de N és el nombre 25, i la de les xifres decimals de 25 és 3, que no és divisible per 11; per tant, N tampoc no és divisible per 11.

1.14. Exercici. Demostreu que tot nombre capicua tal que la seva expressió decimal consti d'un nombre parell de xifres és múltiple de 11.

1.15. Exercici. Feu programes de computador per a realitzar les proves de divisibilitat per 3, per 9 i per 11, per a nombres escrits en notació decimal.

1.16. Exercici. De manera semblant a les proves de divisibilitat per 9 i per 11 per a nombres escrits en el sistema decimal de numeració, establiu una prova de divisibilitat per $b - 1$ i una de divisibilitat per $b + 1$ per a nombres escrits en qualsevol base $b > 1$. Després, dissenyeu un algoritme i feu un programa de computador per a dur-les a la pràctica.

§2. El calendari

La mesura del temps es fa de manera cíclica. Això és a causa de tres fets importants: d'una banda, la periodicitat del moviment aparent de la Lluna al voltant de la Terra, que produeix les llunacions, és a dir, els intervals de temps entre dues llunes plenes consecutives. D'altra banda, la periodicitat del moviment de la Terra al voltant del Sol, que produeix els anys. Finalment, la periodicitat del moviment de rotació de la Terra, que produeix de manera natural els dies.

A l'hora de mesurar el temps, i sobretot per qüestions climàtiques, és convenient tenir en compte tots aquests fets. Però hi ha un problema molt important que cal tenir present: la quantitat de dies d'una llunació i la quantitat de dies d'un any no són nombres enters. Així, per exemple, la durada *mítjana* d'una llunació és de 29 dies, 12 hores, 44 minuts i 2.8 segons, i la durada *mítjana* d'un any tròpic (s'entén per any tròpic la mesura de temps que pren com a referència el pas pel primer punt de la constel·lació

d'Àries), de 365 dies, 5 hores, 48 minuts i 46.08 segons; és a dir, hi ha, de mitjana, 365.2422 dies per any.

A fi d'ajustar tant com es pugui la mesura del temps a aquests fets cíclics, s'han proposat molts calendaris diferents. No ens entretindrem a explicar molts tipus diferents de calendari i ens limitarem al que fem servir actualment.

La base del nostre calendari actual és el calendari julià, que propugnà l'any 45 a. de C. l'emperador romà Julius Cæsar en modificar un calendari anterior basat en un calendari egipci. Abans de la reforma juliana del calendari, els mesos s'havien batejat amb els noms *martius*, *aprilis*, *maius*, *junius*, *quintilis*, *sextilis*, *september*, *october*, *november*, *december*, *januarius* i *februarius* i tenien, alternativament, 31 i 30 dies, llevat del mes *februarius*, que era el darrer de l'any, que només tenia 29 dies per a ajustar la durada de l'any a 365 dies.

El calendari julià disposà un any de 365 dies repartits en 12 mesos, amb l'addició d'un dia cada 4 anys. Citem, com a anècdota que, a causa de la reforma juliana del calendari, i perquè Julius Cæsar va néixer en el mes de *quintilis*, el Senat romà de l'època de l'emperador Marc Antoni (l'any 44 després de Jesucrist) acordà canviar de nom el mes *quintilis* i li donà el de *julius*, en honor del propulsor del nou calendari (cf. [GEC 77]).

2.1. Observació. En aquells moments, els romans no consideraven la setmana com a unitat de mesura del temps, sinó que dividien els mesos en tres parts desiguals: de les calendes a les nones, de les nones als idus, i dels idus a les calendes del mes següent. Tenien, doncs, un calendari solar i no-lunar.

Es va produir una mala aplicació dels anys de traspàs, els que tenen 366 dies. Anys més tard, per a corregir l'error que havia provocat aquest fet, l'emperador Augustus decretà dotze anys consecutius sense que hi hagués cap any de 366 dies. Aquest fet fou causa que el Senat romà (també l'any 44 després de Jesucrist) canviés de nom el mes *sextilis* i el rebategés com a *augustus*. A més a més, perquè el mes dedicat a l'emperador Augustus tingués el mateix nombre de dies que el dedicat a Julius Cæsar, els senadors decidiren treure un dia de *februarius* i afegir-lo a *augustus*. I a fi que, amb aquesta reforma, no hi hagués tres mesos consecutius de 31 dies, modificaren

els nombres de dies dels mesos *september* i *november*, que passaren a tenir 30 dies, i els d'*october* i *december*, que passaren a tenir-ne 31. D'aquesta manera, els mesos adquiriren el nom i el nombre de dies que tenen actualment (cf. [GEC 77]). Posteriorment, l'inici de l'any es dugué al primer dia de *januarius* en lloc del primer de *martius*; per aquesta raó és el mes de febrer i no el de desembre el que es fa servir per a ajustar el nombre de dies de l'any. (Aquest fet ens plantejarà un problema suplementari més endavant.)

El calendari julià, encara que en menor mesura que calendaris anteriors, i malgrat les reformes d'Augustus, mantenia l'error que sorgeix per no tenir en compte correctament la durada de l'any mitjà. La causa és la diferència en la fracció de dia per any: de 0.25, com cregué Julius Cæsar, a 0.2422, com s'ha calculat posteriorment. Per a corregir aquest error, el Papa Gregori XIII, l'any 1582, promulgà una nova reforma del calendari. El nou calendari s'anomena, des de llavors, calendari gregorià. La reforma es basa simplement en el fet que no tots els anys que són múltiples de 4 són anys de traspàs: no ho són els anys múltiples de 100, però són també de traspàs els anys múltiples de 400. A més a més, i per a corregir el fet que en els anys d'aplicació del calendari julià hi havia hagut una diferència de 10 dies, es varen suprimir els dies 5 al 14 d'octubre de l'any 1582.

2.2. Observació. Encara subsisteix un error aproximat de 3 dies cada deu mil anys.

L'objectiu que ens proposem en aquesta secció és donar una fórmula per a calcular el dia de la setmana de qualsevol data del calendari gregorià; és a dir, fer allò que es coneix comunament amb el nom de *calendari perpetu*.

Per a això, convé començar per fer algunes consideracions prèvies. D'una banda, i com que la setmana té set dies, serà útil treballar mòdul 7. Així, doncs, donarem el valor 0 (mod 7) al diumenge, 1 (mod 7) al dilluns, 2 (mod 7) al dimarts, 3 (mod 7) al dimecres, 4 (mod 7) al dijous, 5 (mod 7) al divendres, i 6 (mod 7) al dissabte.

D'altra banda, a fi de simplificar la fórmula, i tenint en compte que els anys de traspàs s'afegeix un dia al final del mes de febrer en lloc de desembre, serà còmode considerar febrer com l'últim mes de l'any anterior; d'aquesta manera, assignarem 1 al mes de març, 2 al mes d'abril, etcètera,

fins a 10 al mes de desembre, 11 al de gener de l'any següent, i 12 al de febrer. Així, per exemple, el dia 21 de febrer de l'any 1996 és considerat com el dia 21 del mes 12 de l'any 1995.

2.3. Observació. Notem que usar aquest conveni és equivalent a pensar que l'any comença el dia 1 de març en lloc del dia 1 de gener, com es feia abans de la reforma juliana.

Tenint en compte aquest conveni, siguin d el dia del mes, m el nombre del mes, i A el nombre de l'any, que escriurem segons la igualtat $A = 100c + a$, $0 \leq a < 100$, donada per la divisió entera de A per 100.

Sigui s_A el dia de la setmana que correspon al dia 1 de març de l'any A . Anem a calcular, en primer lloc, el nombre de dies que hi ha entre aquest dia i el dia 1 de març de l'any 1600.

2.4. Observació. Prendrem 1600 com a any de referència perquè 1600 és el primer any múltiple de 400 després de la reforma gregoriana i, en conseqüència, ens serà més senzill referir-nos a aquest any que no pas a qualsevol altre a l'hora de fer el càlcul del nombre d'anys de traspàs.

Entre 1600 i l'any A hi ha hagut exactament $\left\lfloor \frac{A - 1600}{4} \right\rfloor$ anys múltiples de 4, $\left\lfloor \frac{A - 1600}{100} \right\rfloor$ anys múltiples de 100 i $\left\lfloor \frac{A - 1600}{400} \right\rfloor$ anys múltiples de 400; per tant, el nombre d'anys de traspàs entre aquests dos anys és donat per l'expressió

$$\begin{aligned} & \left\lfloor \frac{A - 1600}{4} \right\rfloor - \left\lfloor \frac{A - 1600}{100} \right\rfloor + \left\lfloor \frac{A - 1600}{400} \right\rfloor \\ &= \left\lfloor \frac{A}{4} \right\rfloor - \left\lfloor \frac{A}{100} \right\rfloor + \left\lfloor \frac{A}{400} \right\rfloor - 400 + 16 - 4 \\ &= \left\lfloor \frac{A}{4} \right\rfloor - \left\lfloor \frac{A}{100} \right\rfloor + \left\lfloor \frac{A}{400} \right\rfloor - 388 \\ &= 25c + \left\lfloor \frac{a}{4} \right\rfloor - c - \left\lfloor \frac{a}{100} \right\rfloor + \left\lfloor \frac{c}{4} + \frac{a}{400} \right\rfloor - 388 \\ &= 24c + \left\lfloor \frac{a}{4} \right\rfloor + \left\lfloor \frac{c}{4} \right\rfloor - 388, \end{aligned}$$

ja que, d'una banda, $\left\lfloor \frac{a}{100} \right\rfloor = 0$ i, de l'altra, $\frac{a}{400} < \frac{1}{4}$, de manera que $\left\lfloor \frac{c}{4} + \frac{a}{400} \right\rfloor = \left\lfloor \frac{c}{4} \right\rfloor$. Si tenim en compte que cada any té 365 dies, llevat dels

anys de traspàs, que en tenen un de més, el nombre de dies transcorreguts entre l'1 de març del 1600 i l'1 de març de l'any A el dóna l'expressió

$$365(A - 1600) + 24c - 388 + \left[\frac{a}{4}\right] + \left[\frac{c}{4}\right] = 365A + 24c - 584388 + \left[\frac{a}{4}\right] + \left[\frac{c}{4}\right].$$

Si reduïm mòdul 7, el dia de la setmana de l'1 de març de l'any A , s_A , es relaciona amb el de l'any 1600, s_{1600} , per la congruència

$$\begin{aligned} s_A &\equiv s_{1600} + A + 3c + \left[\frac{a}{4}\right] + \left[\frac{c}{4}\right] \\ &= s_{1600} + 103c + a + \left[\frac{a}{4}\right] + \left[\frac{c}{4}\right] \\ &\equiv s_{1600} + 5c + a + \left[\frac{a}{4}\right] + \left[\frac{c}{4}\right] \pmod{7}. \end{aligned}$$

El càlcul de s_{1600} es fa fàcilment si tenim en compte que el dia 1 de març del 1997 va ser un dissabte; com que el dissabte és 6 (mod 7), en substituir obtenim la congruència

$$\begin{aligned} 6 &\equiv s_{1600} + 5 \cdot 19 + 97 + \left[\frac{97}{4}\right] + \left[\frac{19}{4}\right] \\ &\equiv s_{1600} + 3 \pmod{7}, \end{aligned}$$

de manera que $s_{1600} = 3$; és a dir, l'1 de març del 1600 va ser un dimecres.

En dur aquest valor a la fórmula anterior, obtenim la fórmula definitiva per al càlcul del dia de la setmana que correspon a l'1 de març de l'any A :

$$s_A \equiv 3 + 5c + a + \left[\frac{a}{4}\right] + \left[\frac{c}{4}\right] \pmod{7}.$$

Observem que aquesta fórmula no necessita conèixer el dia de la setmana que correspon a cap data concreta, en contraposició a altres que usen el dia actual o algun altre dia per a fer la comparació.

Però ens interessa calcular el dia de la setmana de qualsevol data, no només el dia de la setmana que correspon a l'1 de març. Per a això, cal comptar el nombre de dies que hi ha entre l'1 de març i la data que volem. Si es tracta d'un dia de març, només caldrà sumar-lo a la fórmula anterior i restar 1; però si es tracta d'un dia d'abril, caldrà afegir, encara, 3, ja que març té $31 \equiv 3 \pmod{7}$ dies. I si es tracta d'un dia de maig, caldrà sumar $5 = 3 + 2$, ja que abril té $30 \equiv 2 \pmod{7}$ dies. I així successivament.

Si observem que l'increment acumulat corresponent al mes m és donat exactament pel nombre $[2.6m - 0.2] - 2$, el dia 1 del mes m de l'any $100c + a$ és donat per l'expressió

$$1 + 5c + a + \left[\frac{a}{4}\right] + \left[\frac{c}{4}\right] + [2.6m - 0.2] \pmod{7}.$$

Per tant, el dia de la setmana que correspon al dia d del mes m de l'any $100c + a$ és donat per

$$d + 5c + a + [2.6m - 0.2] + \left[\frac{a}{4}\right] + \left[\frac{c}{4}\right] \pmod{7}.$$

2.5. Exercici. Comproveu que, efectivament, l'expressió $[2.6m - 0.2] - 2 \pmod{7}$ calcula l'increment del dia de la setmana que correspon al dia 1 del mes m respecte del que correspon al dia 1 de març.

D'aquesta manera, hem obtingut el calendari gregorià perpetu. Establim el resultat en forma d'enunciat per a facilitar-ne la lectura.

2.6. Proposició. (Calendari gregorià perpetu) *El dia de la setmana que correspon al dia d del mes m de l'any $A = 100c + a$ del calendari gregorià, amb $0 \leq a < 100$, s'obté per l'expressió*

$$d + 5c + a + [2.6m - 0.2] + \left[\frac{a}{4}\right] + \left[\frac{c}{4}\right] \pmod{7},$$

on cal tenir present les notacions següents:

- (a) *Els nombres que corresponen al mes i a l'any, m , A , s'han d'escriure de manera que $m = 1$ correspon al mes de març, $m = 2$, a abril, etcètera, i considerar els mesos de gener i febrer com els mesos 11 i 12 de l'any anterior; és a dir, considerar que l'any comença el dia 1 de març en lloc del dia 1 de gener.*
- (b) *Els dies de la setmana es llegeixen de manera que diumenge és 0 $\pmod{7}$, dilluns és 1 $\pmod{7}$, etcètera, fins a dissabte, que és 6 $\pmod{7}$. □*

2.7. Exemple. Amb la hipòtesi que continuï vigent el calendari gregorià, quin dia de la setmana serà el primer dia del segle XXI?

El dia 1 de gener de l'any 2001 correspon, tenint en compte el nostre conveni, a fer $d = 1$, $m = 11$, $a = 0$, i $c = 20$. Per tant, cal calcular el nombre $1 + 5 \cdot 20 + 0 + [2.6 \cdot 11 - 0.2] + [0/4] + [20/4] \equiv 1 + 100 + 28 + 5 \equiv 1 \pmod{7}$, de manera que el primer dia de l'any 2001, segons el calendari gregorià, serà un dilluns.

2.8. Exercici. Es diu per alguns indrets que Santa Teresa d'Àvila va restar onze dies morta abans que no l'enterressin i que, mentrestant, el seu cos no es corrompia. Però la realitat històrica sembla que ensenya que, de fet, només van transcórrer deu hores entre el moment de la seva mort i el del seu enterrament. Si tenim en compte que Santa Teresa va ésser enterrada el dia 15 d'octubre del 1582 a les set del matí (aproximadament), quin dia i a quina hora va morir?

2.9. Exercici. Calculeu el dia de la setmana que correspongué al 12 d'octubre del 1492.

2.10. Observació. El calendari gregorià no ha estat adoptat per tots els països; ni, en els països en què ha estat adoptat, hi ha estat en la mateixa data. Per exemple, a Gran Bretanya ho va ser l'any 1752 i es van haver d'afegir onze dies, en lloc de deu; al Japó ho va ser l'any 1873, als països d'Europa de l'Est, el 1917, i a Grècia, el 1923.

2.11. Exercici. Encara que William Shakespeare i Miguel de Cervantes van morir, tots dos, en la mateixa data (un 23 d'abril de 1616), no van morir el mateix dia. Qui va morir primer? Quants dies abans?

2.12. Exercici. Feu una cerca bibliogràfica de la data concreta en què els diferents països van adoptar el calendari gregorià, calculeu quants dies va caldre afegir, i feu un programa de computador per a calcular el dia de la setmana de qualsevol data del calendari gregorià que tingui en compte els països als quals s'aplica.

2.13. Exercici. Tot i que el calendari oficial adoptat per l'Organització de les Nacions Unides és el calendari gregorià, hi ha alguns països que usen,

simultàniament, altres calendaris; per exemple, els calendaris àrab, hindú, jueu o xinès. Feu un programa de computador que faci la conversió de dates entre els calendaris diferents.

2.14. Exercici. Tenint en compte el calendari que es feia servir en cada instant abans de l'adopció del calendari gregorià, modifiqueu els programes dels exercicis anteriors a fi de poder calcular correctament el dia de la setmana de qualsevol data segons el calendari vigent en aquella data, i la data que correspondria segons el calendari julià-gregorià.

2.15. Observació. El calendari gregorià, a més a més de l'error de 3 dies cada deu mil anys, té altres problemes. Per exemple, els mesos no tenen tots el mateix nombre de dies, i això també succeeix amb els trimestres. En particular, a una data fixa de cada any no li correspon el mateix dia de la setmana. Notem, també, que un calendari purament lunar tampoc no seria satisfactori, ja que el nombre de dies d'una llunació no concorda bé ni amb el de les setmanes ni amb el dels mesos.

Seria desitjable —per exemple, per qüestió de festes, tant laborals com socials o religioses— que els dies de la setmana a què corresponen les mateixes dates anyals fossin els mateixos. També ho seria que els mesos tinguessin tots el mateix nombre de dies i el mateix nombre de setmanes.

Si ens adonem que 364 és divisible per 7 i per 13, concretament, que $364 = 4 \cdot 7 \cdot 13$, seria raonable que un any normal constés de tretze mesos de quatre setmanes de set dies, més un dia (o dos si l'any és de traspàs) que no corresponguessin a cap mes ni a cap setmana. De totes maneres, hi hauria el problema que no podríem dividir l'any en trimestres, i les estacions tampoc no concordarien amb mesos de l'any. De fet, s'ha proposat, però no ha tingut acceptació pràctica, l'anomenat “calendari internacional fix”. Constaria, efectivament, de tretze mesos de vint-i-vuit dies, més un dia al final de l'any; aquest dia no correspondria a cap mes. D'altra banda, els anys de traspàs, que s'inclourien com en el calendari gregorià, afegirien el dia de més al final del sisè mes. També s'ha proposat el nom de Sol per al mes que s'afegiria, i que estaria situat entre els mesos actuals de juny i juliol.