Una classe de Computació Agebraica amanida amb MateMàgia

Grau en Enginyeria Matemàtica i Física.

Assignatura de Computació Algebraica

Josep M. Brunat

16 d'octubre de 2023

1 Introducció

Tothom sap que els efectes dels il·lusionistes es basen en ocultar alguna cosa: capses amb doble fons, dues monedes fent veure que només n'hi ha una, cartes amagades a la màniga, distreure l'atenció amb alguna cosa mentre es fa l'important per al truc, etcètera. En canvi, en el que s'ha vingut a anomenar MateMàgia, tot és a la vista. L'efecte sorpresa s'obté gràcies a alguna propietat matemàtica desconeguda per l'espectador.

En el jocs que explicarem, hi ha qui el fa el paper de mag, que anomenarem Maria (amb la mateixa lletra inicial que «mag»), i qui fa el paper de públic que anomenarem Pere (amb la mateixa lletra inicial que «public»). Els jocs tenen en comú que són basats en matèries pròpies de la computació algebraica.

2 Endevinar un nombre. Teorema de Cantor i canvis de base

Joc 1. Endevinar un nombre entre 1 i 63

Maria dóna a un estudiant 6 cartrons amb el contingut que es detalla tot seguit:

1	3	5	7
9	11	13	15
17	19	21	23
25	27	29	31
33	35	37	39
41	43	45	47
49	51	53	55
57	59	61	63

2	3	6	7
10	11	14	15
18	19	22	23
26	27	30	31
34	35	38	39
42	43	46	47
50	51	54	55
58	59	62	63

4	5	6	7
12	13	14	15
20	21	22	23
28	29	30	31
36	37	38	39
44	45	46	47
52	53	54	55
60	61	62	63

8	9	10	11
12	13	14	15
24	25	26	27
28	29	30	31
40	41	42	43
44	45	46	47
56	57	58	59
60	61	62	63

16	17	18	19
20	21	22	23
24	25	26	27
28	29	30	31
48	49	50	51
52	53	54	55
56	57	58	59
60	61	62	63

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

A continuació Pere ha de pensar en secret un nombre enter N amb $1 \leq N \leq 63$, i donar a Maria els cartrons en els quals el nombre hi sigui escrit. Llavors Maria és capaç d'endevinar N.

Per explicar què hi ha darrera d'aquest joc, començarem amb un resultat de Georg Cantor[1]

Proposició 2.1 *Sigui $(b_n : n \geq 1)$ una successió d'enters positius amb $b_n \geq 2$ per tot n. Definim una nova successió $(B_n : n \geq 1)$ per $B_1 = b_1$, $B_2 = b_1 \cdot b_2$ i, en general, $B_n = b_1 \cdots b_n$. Llavors, per a cada enter $N \geq 1$ existeixen enters $a_k, \ldots, a_0$ únics tals que*

$$N = a_k B_k + a_{k-1} B_{k-1} + \cdots + a_1 B_1 + a_0, \quad a_k \neq 0, \quad 0 \leq a_i < b_{i+1}.$$

Demostració. Sigui $q_0 = N$.

Si $q_0 = N < b_1$, definim $a_0 = q_0$ i hem acabat.

Si $q_0 \geq b_1$, dividim q_0 per b_1 i obtenim q_1, a_0 únics tals que

$$q_0 = q_1 b_1 + a_0, \quad q_1 \neq 0, \quad 0 \leq a_0 < b_1.$$

Si $q_1 < b_2$, prenem $a_1 = q_1$ i tenim

$$N = q_0 = a_1 b_1 + a_0 = a_1 B_1 + a_0, \quad 0 \neq a_1 = q_1 < b_2$$

i hem acabat.

Suposem que, per a un i, existeixen $q_i, a_{i-1}, \ldots, a_0$ únics tals que $q_i \neq 0$, $0 \leq a_j \leq b_{j+1}$ per a $0 \leq j \leq i$, i

$$N = B_i q_i + a_{i-1} B_{i-1} + \cdots + a_1 B_1 + a_0,$$

Si $q_i < b_{i+1}$, prenem $a_i = q_i$ i hem acabat. Si no, dividim q_i per b_{i+1} i existeixen q_{i+1}, a_i únics tals que

$$q_i = b_{i+1} q_{i+1} + a_i, \quad q_{i+1} \neq 0, \quad 0 \leq a_i \leq b_{i+1}.$$

[1]Georg Cantor. St. Petersburg, Rússia, 1845; Halle, Alemanya, 1918.

Llavors,

$$\begin{aligned} N &= B_i(b_{i+1}q_{i+1} + a_i) + a_{i-1}B_{i-1} + \cdots + a_1B_1 + a_0, \\ &= B_{i+1}q_{i+1} + a_iB_i + a_{i-1}B_{i-1} + \cdots + a_1B_1 + a_0. \end{aligned}$$

Com que $q_0 > q_1 > \ldots$, segur que existeix un k tal que $q_k < b_{k+1}$ i, prenent $a_k = q_k$, obtenim

$$N = a_kB_k + a_{k-1}B_{k-1} + \cdots + a_1B_1 + a_0 \qquad \square$$

EXEMPLE. Posem $b_n = n$. En aquest cas, $B_n = n!$. Notem que $b_1 = 1$ i, per tant, $a_0 = 0$. Donat $N \geq 1$, existeixen enters $a_k, \ldots, a_1$ únics tals que

$$N = a_k \cdot k! + a_{k-1} \cdot (k-1)! + \cdots + a_2 \cdot 2! + a_1 \cdot 1!, \quad a_k \neq 0, \quad a_i < i+1, \quad 1 \leq i \leq k.$$

Per exemple, per al 7315, dividim pels enters successius començant pel 2 (perquè el residu a_0 de dividir per 1 és 0) i obtenim:

$$\begin{array}{rrrrrrrrrrrrrrr}
7 & 3 & 1 & 5 & \big| & 2 & & & & & & & & & \\
\cline{5-6}
1 & 3 & & & & 3 & 6 & 5 & 7 & \big| & 3 & & & & \\
\cline{6-10}
 & 1 & 1 & & & 0 & 6 & & & 1 & 2 & 1 & 9 & \big| & 4 \\
\cline{10-11}
 & & 1 & 5 & & & 0 & 5 & & & 0 & 1 & 9 & 3 & 0 & 4 & \big| & 5 \\
\cline{13-14}
 & & & \mathbf{1} & & & & 2 & 7 & & & & \mathbf{3} & & 0 & 4 & 6 & 0 & \big| & 6 \\
\cline{15-16}
 & & & & & & & & \mathbf{0} & & & & & & \mathbf{4} & 0 & 0 & 1 & 0 & \big| & 7 \\
\cline{17-18}
 & & & & & & & & & & & & & & & & & \mathbf{0} & \mathbf{3} & & \mathbf{1}
\end{array}$$

Així,

$$7315 = 1 \cdot 7! + 3 \cdot 6! + 4 \cdot 4! + 3 \cdot 3! + 1. \qquad \|$$

El cas més emprat del resultat de Cantor és el cas que la successió dels b_n és constant. Aleshores s'obte el següent:

Corol·lari 2.2 *Sigui $b \geq 2$ un enter. Donat un enter $N \geq 1$ existeixen enters $a_k, \ldots, a_0$ únics tals que*

$$N = a_kb^k + a_{k-1}b^{k-1} + \cdots + a_1b + a_0, \quad a_k \neq 0, \quad 0 \leq a_i \leq b, \ 0 \leq i \leq k.$$

DEMOSTRACIÓ. Només cal prendre $b_n = b$ a la proposició de Cantor. Amb això, $B_n = b^n$ i s'obté el resultat. $\square$

Si, amb la notació del corol·lari anterior, $N = a_kb^k + a_{k-1}b^{k-1} + \cdots + a_1b + a_0$, els nombres $a_k, \ldots, a_0$ es diuen les *xifres* de N en base b, i s'escriu $N = (a_k \ldots a_0)_{b)}$; amb xifres concretes les xifres no es posen entre parèntesi. Com és evident, usualment escrivim els nombres en base 10 sobreentenent la base.

EXEMPLE. Escrivim el nombre 135 en base 3. Les xifres són els residus de les divisions successives per 3, més l'últim quocient, el que resulta ser menor que $b = 3$:

$$\begin{array}{rrrrrrrrr}
1 & 4 & 2 & \big| & 3 & & & & \\
 & 2 & 2 & & 4 & 7 & \big| & 3 & \\
 & & \mathbf{1} & & 1 & 7 & & 1\ 5 & \big| \ 3 \\
 & & & & \mathbf{2} & & & \mathbf{0} & 5 \ \big| \ 3 \\
 & & & & & & & & \mathbf{2}\ \ \mathbf{1}
\end{array}$$

Així, $135 = 1 \cdot 3^4 + 2 \cdot 3^3 + 0 \cdot 3^3 + 2 \cdot 3 + 1$ i $135 = 12021_{3)}$ ‖

Si la base b és més gran que 10, sovint les «xifres» 10, 11, etc. es substitueixen per lletres.

El programa `d2b` admet per entrada dos enters (n, b) i retorna la llista de les xifres de n en base b. Per exemple `d2b(135,3)` retorna `[1,2,0,2,1]`. El programa `b2d` fa el procés invers, per exemple `b2d([1,2,0,2,1],3)` retorna `135`.

```
def d2b(n,b):
     q=n
     res=[]
     while q>=b:
       q,r=divmod(q,b)
       res=[r]+res
     res=[q]+res
     return res
```

```
def b2d(B,b):
      k=len(B)
      res=0
      for i in [0..k-1]:
        res=res+(B[i])*b^(k-i-1)
      return res
```

Una observació de caràcter històric. En la nostra forma d'escriure els nombres, quan en comencem a escriure un i posem, per exemple, 4, el qui ho veu no pot saber si aquest 4 significarà 4, 40, 400, etc.; no pot saber el significat del 4 fins que el nombre no estigui completat. Seria més raonable escriure, per exemple, el quatre-cents vint-i-set en la forma 724, que llegiríem «set, vint, quatre-cents» Així, la primera xifra que s'escriuria és la de les unitats, la segona la de les desenes, etc, i no caldria haver d'esperar a completar el nombre per saber el significat de cada xifra.

Aquest disfunció prové de les traduccions dels àrabs. Les xifres tal com les emprem es van introduir a occident a través dels àrabs, els quals escriuen de dreta a esquerra. Així en la seva escriptura, ells escriuen primer les unitats, després de desenes, etc. El llatí, però, s'escriu d'esquerra a dreta i així ho feien els traductors de l'àrab al llatí. Però les xifres eren símbols nous que no van traduir: ho van deixar com a l'original àrab. I així es van quedar les unitats com a última xifra de la dreta, cosa natural en l'escriptura de dreta a esquerra, però absurda en la nostra escriptura d'esquerra a dreta.

En el cas de la base $b = 2$, les xifres només poden ser 0 i 1. Per tant,

Corol·lari 2.3 *Tot nombre enter* ≥ 1 *és suma única de potències de* 2.

Aquest últim corol·lari és la base del joc dels cartrons. Els cartrons estan encapçalats pels nombres, 1, 2, 4, 8, 16 i 32; etiquetarem els cartrons amb aquests nombres. En cap nombre entre 1 i 63, posat com a suma de potències de 2 apareix una potència superior

a $2^5 = 32$ perquè $63 = 32 + 16 + 8 + 4 + 2 + 1$. Notem, per exemple, el que passa amb el nombre $37 = 32 + 4 + 1$: apareix exactament en els cartrons 32, 4 i 1; el nombre $53 = 32+16+4+1$ apareix exactament en els cartrons 32, 16, 4 i 1; el nombre 63 apareix a tots els cartrons. Així, si poseu un nombre com a suma de potències de 2, el nombre apareix exactament en els cartrons la suma dels quals dona el nombre. Aleshores, quan Pere li va donant a Maria els cartrons en què surt el nombre, Maria només ha d'anar sumant el primers nombres dels cartrons rebuts per endevinar el número pensat.

L'expressió d'un nombre com a combinació lineal entera de potències de 10 és el que hi ha darrera del joc següent.

Joc 2. Endevinar el valor d'una suma

Pere fa les operacions següents.

- Escriu un nombre N_1 de cinc xifres amb la primera major que la darrera.
- Escriu el nombre N_2 resultant de N_1 permutant les xifres primera i última.
- Calcula la diferència $N_3 = N_1 - N_2$.
- Escriu el nombre N_4 resultant de N_3 permutant les xifres primera i última.
- Calcula $S = N_3 + N_4$.

Maria endevina S.

L'explicació de com Maria endevina el valor de la suma és la següent.

Sigui $N_1 = xyztu$ amb $x > u$. Llavors,

$$\begin{aligned} N_1 &= x \cdot 10^4 + y \cdot 10^3 + z \cdot 10^2 + t \cdot 10 + u \\ N_2 &= u \cdot 10^4 + y \cdot 10^3 + z \cdot 10^2 + t \cdot 10 + x \\ N_3 = N_1 - N_2 &= (x - u) \cdot 10^4 + (u - x) \end{aligned}$$

Notem que $u - x < 0$, així que $x - u$ no és una xifra de N_3. Però podem obtenir les xifres de N_3:

$$N_3 = (x - u - 1) \cdot 10^4 + 9 \cdot 10^3 + 9 \cdot 10^2 + 9 \cdot 10 + (10 - (x - u)).$$

Les xifres de N_3 són $x - u - 1$ (eventualment pot ser 0), 9, 9, 9 i $10 - (x - u)$. Llavors, N_4 és

$$N_4 = (10 - (x - u)) \cdot 10^4 + 9 \cdot 10^3 + 9 \cdot 10^2 + 9 \cdot 10 + (x - u - 1)$$

i

$$N_3 + N_4 = 9 \cdot 10^4 + 18 \cdot 10^3 + 18 \cdot 10^2 + 18 \cdot 10 + 9 = \mathbf{1099989}.$$

El resultat, 1099989, és independent del nombre inicial. Així, Maria sempre pot endevinar el resultat.

El mateix truc i argument es pot fer amb un nombre diferent de xifres. Amb 3 xifres resulta 10989, amb 6 resulta 10999989 i, en general, amb n xifres resulta un nombre començat amb 10 seguit de $n - 2$ nous i acabat en 89.

3 Aritmètica modular i regles de divisibilitat

L'expressió d'un nombre com a suma de potències de 10 multiplicades per les xifres és la base dels criteris de divisibilitat, que donen unes quantes possibilitats de jocs, com els tres següents en els que s'endevina una xifra, excepte en un cas en que la xifra pot tenir dos valors.

Tres jocs d'endevinar (quasi sempre) una xifra.

Joc 3. Endevinar una xifra (I)

Pere construeix, amb les 10 xifres $0, \ldots, 9$, el nombres que vol i els suma. Després diu totes les xifres de la suma en ordre arbitrari excepte una. Llavors Maria endevina la que falta.

Per exemple, Pere fa $75+134+20+689 = 918$ (noteu que, a la suma, cada xifra apareix només una vegada). A continuació Pere escull una xifra de la suma, per exemple 1, i diu les altres en l'ordre que vol, per exemple 8 i 9. Llavors Maria endevina que la que falta és 1.

Joc 4. Endevinar una xifra (II)

Pere escull el nombre enter enter positiu A que vol. Calcula la suma S de les seves xifres i calcula $A - S$. Després diu totes les xifres de $A - S$ en ordre arbitrari, menys una. Maria endevina la que falta.

Per exemple, Pere escull $A = 540232$, calcula $S = 5+4+0+2+3+2 = 16$, i fa la resta $A - S = 540216$. Escull una xifra, per exemple 2, i diu les altres en un ordre qualsevol, per exemple 0, 1, 4, 5 i 6. Llavors Maria endevina que manca un 2.

Joc 5. Endevinar una xifra (III)

Pere escull el nombre enter positiu A que vol. Després canvia l'ordre de les seves xifres com vol i obté un nombre B. A continuació resta el més petit de A i B del més gran i diu totes les xifres de la resta en ordre arbitrari menys una. Maria endevina la que falta.

Per exemple, Pere escull $A = 761902$, i tria com a $B = 290617$. Fa la resta $A - B = 471285$. Escull una xifra, diguem 7. Llavors diu les altres en qualsevol ordre, per exemple 2, 4, 5, 8, 1. Llavors Maria endevina que la que falta és 7.

L'explicació dels tres jocs anteriors es basa en el criteri de divisibilitat per 9. Recordeu l'equivalència entre $N \equiv 0 \pmod{m}$ i que m divideix m.

Proposició 3.1 *Mòdul 9, un nombre és congru amb la suma de les seves xifres. En particular, un nombre és divisible per* 9 *si, i només si, ho és la suma de les seves xifres.*

Demostració. Si el nombre és

$$N = a_k a_{k-1} \ldots a_0 = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0,$$

atès que $10 \equiv 1 \pmod{9}$, resulta

$$N \equiv a_k + a_{k-1} + \cdots + a_1 + a_0 \pmod{9}.$$

En particular,

$$\begin{aligned} N \text{ és divisible per } 9 &\Leftrightarrow N \equiv 0 \pmod 9 \\ &\Leftrightarrow a_k + \cdots + a_0 \equiv 0 \pmod 9 \\ &\Leftrightarrow a_k + \cdots + a_0 \text{ és divisible per } 9. \qquad \square \end{aligned}$$

En les explicacions dels jocs 3, 4 i 5 que segueixen totes les congruències cal entendre-les mòdul 9.

En el joc 3, cadascun dels nombres que posa l'estudiant és congru amb la suma de les seves xifres. Aleshores, la suma S és un nombre congru amb

$$0 + 1 + 2 + \cdots + 9 = \frac{10 \cdot 9}{2} = 45 \equiv 0.$$

Ara, si la suma de les xifres de S menys una (la que no diu Pere) és congru amb la xifra $a \neq 0$, la xifra que falta és $9 - a$ per tal que S sigui congru amb 0. Però si la suma S és congru amb 0, la xifra que falta tant pot ser 0 com 9.

Considerem el joc 4. Segons hem vist, el nombre A és congru amb la suma S de les seves xifres. Per tant, $A - S \equiv 0$. Com en el cas anterior, si la suma de les xifres de $A - S$ menys una és congru amb la xifra $a \neq 0$, la xifra que falta és $9 - a$. Si la suma de les xifres menys una és congru amb 0, llavors la que falta pot ser 0 o 9.

En el joc 5, els nombres A i B són congrus perquè tenen les mateixes xifres. Per tant, $A - B \equiv 0$. Com en els casos anteriors, si la suma de les xifres de $A - B$ menys una és congru amb la xifra $a \neq 0$, la xifra que falta és $9 - a$. Si la suma de les xifres menys una és congru amb 0, llavors la que falta pot ser 0 o 9.

Les regles de divisibilitat per 3, 5 i 11 són ben conegudes:

Proposició 3.2 *Sigui $N = a_k a_{k-1} \ldots a_1 a_0$. Llavors*

(i) $N \equiv a_k + a_{k-1} + \cdots + a_0 \pmod 3$. *En particular, N és divisible per 3 si, i només si, ho és la suma de les seves xifres.*

(ii) $N \equiv a_0 \pmod 5$. *En particular, N és divisible per 5 si, i només si, $a_0 \in \{0, 5\}$.*

(iii) *Si k és parell, $N \equiv a_k + a_{k-2} + \cdots + a_0 - (a_{k-1} + a_{k-3} + \cdots + a_1) \pmod{11}$. Si k és senar, $N \equiv a_k + a_{k-2} + \cdots + a_1 - (a_{k-1} + a_{k-3} + \cdots + a_0) \pmod{11}$. En particular, N és divisible per 11 si, i només si, ho és la diferència entre la suma de les xifres que ocupen un lloc parell i la suma de les xifres que ocupen un lloc senar.*

Demostració. Tenim

$$N = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0. \tag{1}$$

(i) Com que $10 \equiv 1 \pmod 3$, resulta $10^i \equiv 1 \pmod 3$ per a tot enter $i \geq 0$. Prenent congruències mòdul 3 a (1), obtenim

$$N \equiv a_k + a_{k-1} + \cdots + a_0, + \cdots + a_0$$

i, naturalment, $N \equiv 0 \pmod 3$ si, i només si, $a_k + \cdots + a_0 \equiv 0 \pmod 3$.

(ii) Com que $10 \equiv 0 \pmod 5$, resulta $10^i \equiv 0 \pmod 5$ per a tot enter $i \geq 1$. Aleshores, prenent congruències a (1) obtenim $N \equiv a_0 \pmod 5$. En particular $N \equiv 0 \pmod 5$ si, i només si $a_0 \equiv 0 \pmod 5$, és a dir, si, i només si a_0 és 0 o 5.

(iii) Notem que $10 \equiv -1 \pmod{11}$, així que $10^i \equiv -1$ si i és senar i $10^i \equiv 1 \pmod{11}$ si i és parell. Si k és parell, tenim

$$N \equiv a_k - a_{k-1} + a_{k-2} - \cdots - a_1 + a_0 = a_k + a_{k-2} + \cdots + a_0 - (a_{k-1} + a_{k-3} + \cdots + a_1) \pmod{11}.$$

En particular, $N \equiv 0 \pmod{11}$ si, i només si,

$$a_k + a_{k-2} + \cdots + a_0 - (a_{k-1} + a_{k-3} + \cdots + a_1) \equiv 0 \pmod{11}.$$

L'argument és similar en el cas que k és senar. □

L'argument fet en el cas de 11 es pot generalitzar. Per un mòdul m qualssevol, cal trobar els residus dels $10^i \equiv c_i \pmod m$ i aleshores $N \equiv c_k a_k + c_{k-1} a_{k-1} + \cdots + c_1 a_1 + a_0$. En el cas de $m = 11$, els coeficients c_i són 1 i -1 alterns, però per a altres valors de m poden ser nombres que facin la regla no gaire útil.

Exemples. Prenem $m = 15$. Com que $100 \equiv 10 \pmod{15}$, $10^3 \equiv 10^2 \cdot 10 \equiv 10 \cdot 10 \equiv 10$ i, en general, per a $i \geq 1$, tenim $10^i \equiv 10 \pmod{15}$. Aleshores

$$N = a_k 10^k + \cdots + a_1 10 + a_0 \equiv 10(a_k + a_1 + \cdots + a_1) + a_0 \pmod{15}.$$

Així, mòdul 15, un nombre és congru amb la suma de la xifra de les unitats i deu vegades la suma de les altres xifres.

Per a $m = 16$, tenim $10^2 \equiv 4 \pmod{16}$, $10^3 \equiv 8 \pmod{16}$ i $10^4 \equiv 0 \pmod{16}$. Aleshores,

$$N = N = a_k 10^k + \cdots + a_1 10 + a_0 \equiv 8a_3 + 4a_2 + 10a_1 + a_0 \pmod{16}. \qquad \|$$

Recordem certes propietats de les congruències mòdul un nombre primer.

Proposició 3.3 *Sigui $p \geq 2$ un nombre primer i $a \in \{1, \ldots, p-1\}$. Llavors,*

(i) *existeix $b \in \{1, \ldots, p-1\}$ tal que $ab \equiv 1 \pmod p$. (Altrament dit, $\mathbb{Z}_p$ és un cos.)*

(ii) *Si $ax \equiv 0 \pmod p$, llavors $x \equiv 0 \pmod p$.*

DEMOSTRACIÓ. (Totes les congruències ho són mòdul p.)

(i) Com que p és primer, tenim $\text{mcd}(a,p)=1$ i, per a certs y,z es compleix $ay+pz=1$. Llavors $ay\equiv 1$. Si $y\equiv b\in\{1,\dots,p-1\}$, tenim $ab\equiv 1 \pmod p$.

(ii) Sigui b tal que $ab\equiv 1$. Multiplicant per b la congruència $ax\equiv 0$, obtenim $x\equiv 0$. □

Corol·lari 3.4 *Si $p\geq 2$ és un nombre primer i x i y són enters tals que $xy\equiv 0 \pmod p$, aleshores $x\equiv 0 \pmod p$ o $y\equiv 0 \pmod p$.*

DEMOSTRACIÓ. (Sobreentenem que totes les congruències ho són mòdul p.)

Suposem que $x\not\equiv 0$ i veurem que necessàriament $y\equiv 0$. Com que $x\not\equiv 0$, x és congru amb un nombre $a\in\{1,\dots,p-1\}$. Per la proposició anterior, existeix b tal que $ab\equiv 1$. Llavors, $0\equiv xy\equiv ay$. Multiplicant per b, resulta $0\equiv bay\equiv y$. □

Si a i b són enters i $ab\equiv 1 \pmod m$, es diu que a i b són *inversos* mòdul m.

Veurem ara una caracterització de la divisibilitat per 7.

Proposició 3.5 *Un nombre és divisible per 7 si, i només si, ho és el nombre que resulta al suprimir l'última xifra i restar el doble de l'última xifra.*

DEMOSTRACIÓ. Sigui $N=a_ka_{k-1}\dots a_1a_0$. Notem que $10\equiv 3 \pmod 7$. A més 5 és invers de 3 mòdul 7 perquè $5\cdot 3=15\equiv 1 \pmod 7$. Tenim:

$$\begin{aligned} N &= a_k10^k+a_{k-1}10^{k-1}+\cdots+a_110+a_0\\ &= 10(a_k10^{k-1}+\cdots a_1)+a_0\\ &\equiv 3(a_k10^{k-1}+\cdots a_1)+a_0 \pmod 7. \end{aligned}$$

Aleshores

$$\begin{aligned} N\equiv 0 \pmod 7 &\Leftrightarrow 3(a_k10^{k-1}+\cdots+a_1)+a_0\equiv 0 \pmod 7\\ &\Leftrightarrow 5\cdot 3(a_k10^{k-1}+\cdots+a_1)+5a_0\equiv 0 \pmod 7\\ &\Leftrightarrow (a_k10^{k-1}+\cdots+a_1)-2a_0\equiv 0 \pmod 7 \end{aligned}$$ □

EXEMPLES. Considerem, per exemple, 7527. Suprimim l'última xifra 7 i queda 752, del qual restem $2\cdot 7=14$. Tenim, $752-14=738$. Repetim el procediment: $738\to 73-16=57$, que no és múltiple de 7. Per posar un altre exemple,

$$2289\to 228-18=210\to 21-0=21,$$

que sí és divisible per 7 i, per tant, 2289 també. ‖

L'argument fet amb el 7 es pot generalitzar per a altres mòduls m sempre que 10 tingui invers mòdul m. Per exemple:

Proposició 3.6 *Un nombre és divisible per* 13 *si, i només si, ho és el nombre que resulta al suprimir l'última xifra* a_0 *i restar al nombre resultant* $9a_0$.

Demostració. Sigui $N = a_k a_{k-1} \dots a_1 a_0$. Notem que $4 \cdot 10 = 40 = 13 \cdot 3 + 1 \equiv 1 \pmod{13}$ i que $4 \equiv -9 \pmod{13}$. Llavors,

$$N = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0 = 10(a_k 10^{k-1} + \cdots + a_1) + a_0.$$

Per tant,

$$\begin{aligned} N \equiv 0 \pmod{13} &\Leftrightarrow 10(a_k 10^{k-1} + \cdots + a_1) + a_0 \equiv 0 \pmod{13} \\ &\Leftrightarrow 4 \cdot 10(a_k 10^{k-1} + \cdots + a_1) + 4a_0 \equiv 0 \pmod{13} \\ &\Leftrightarrow (a_k 10^{k-1} + \cdots + a_1) - 9a_0 \equiv 0 \pmod{13}. \qquad \square \end{aligned}$$

Exemple. Considerem, per exemple, 4914. Tenim

$$4914 \to 491 - 36 = 455 \to 45 - 45 = 0.$$

Per tant, 4914 és múltiple de 13. En efecte, $4914 = 13 \cdot 378$. $\|$

4 Un joc basat en congruències

La realització del joc següent requereix una certa pràctica, però és vistós.

Joc 6. Trobar la carta que falta.

D'una baralla s'excloen les cartes de nombres superiors a 10. Pere la barreja a consciència i després en tria una. Maria pot endevinar fàcilment quina ha estat la carta triada: mira les altres 39, i la que manca és la que Pere ha triat. Maria va mirant les cartes (que, recordem, estan ben barrejades) una a una a un ritme una mica lent, però constant, i quan ha acabat diu la carta triada.

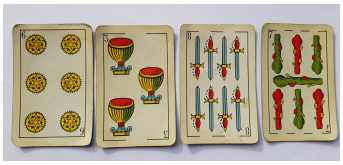
Com ho fa Maria? Avancem que a Maria li caldrà fer moviments amb mans i peus, per la qual cosa caldrà que segui, a ser possible amb una taula que faci no visibles els seus peus. Cal endevinar dues coses: el nombre i el pal. Vejam primer com trobar el nombre. La suma de tots els nombres de les cartes mòdul 10 és

$$4(1+2+3+4+5+6+7+8+9+10) = 4(11 \cdot 10)/2 = 2 \cdot 11 \cdot 10 \equiv 0 \pmod{10}.$$

Per tant, només cal anar fent la suma mòdul 10 de les cartes que van sortint fins arribar a l'última. Si $s \in \{0, 1, \dots, 9\}$ és la suma mòdul 10 de les 39 cartes, la que falta té número $10 - s$. Amb això podem determinar fàcilment el nombre perquè les sumes mòdul 10 són fàcils de fer: només cal quedar-se amb l'última xifra de la suma ordinària.

Ara vejam com deduir el pal. Identifiquem cada pal amb una parella binària:

Oros	$(0,0)$
Copes	$(0,1)$
Espases	$(1,0)$
Bastos	$(1,1)$



Com a regla nmotècnica, observem que les cartes d'oros tenen la ratlla superior sense forats, les de copes amb un forat, les d'espases amb 2 i les de bastos amb 3. Així, les parelles corresponents formen el nombre de forats de la ratlla de dalt en base 2.

La suma de les 40 parelles (x, y) mòdul 2 és $(0, 0)$ perquè n'hi ha 10 de cada. Si es fa la suma de les 39 parelles i surt una parella (x, y), aquest és el pal.

Una manera de dur el control de la suma d'aquestes parelles mòdul 2 és amb els peus (recordem que les mans són ocupades calculant el número). Comencem amb els peus plans damunt el trespol. Si la carta que surt és oros, no fem res; si surt copes canviem la posició del peu dret (si és pla, en pugem la punta; si és amunt el baixem); si surt espases, canviem de posició el peu esquerra; si surt bastos, canviem els dos. La posició dels peus després de l'última carta diu el pal de la carta que falta.

No negaré que cal una certa concentració i pràctica per fer, alhora, la suma mòdul 10 dels nombres i el moviment de peus que fa la suma mòdul 2 de les parells binàries. Però sembla més difícil del que realment és i amb unes quantes proves els càlculs i moviments surten automàtics.

5 El joc del Nim

Un *joc progressiu finit* és un joc que compleix les condicions següents:

1) Hi ha dos jugadors que mouen per torn. Abans de començar, els dos jugador han acordat qui fa el primer moviment.

2) Hi ha una posició inicial.

3) Les regles que marquen els moviments vàlids són les mateixes per als dos jugadors i el moviment el decideix el jugador sense dependència de cap procés aleatori, com llançar un dau, o una moneda.

4) No hi ha informació oculta. Tota la informació sobre l'estat del joc és a la vista dels dos jugadors en tot moment.

5) Per a cada posició del joc, cada jugador té un nombre finit de moviments possibles.

6) El joc acaba, en un nombre finit de moviments, quan un dels dos jugadors no pot fer cap moviment vàlid; aquest jugador és el que perd i l'altre és el vencedor.

Com a exemple, considerem el joc progressiu finit següent.

Joc 7. El joc de les 18 granisses.

En una taula posem 18 objectes en fila. El tipus d'objecte és irrellevant, però per fixar idees suposarem que són granisses. Hi ha dos jugadors A i B. Per torn, començant A, cada jugador pot enretirar una, dues o tres granisses. Guanya qui neteja la taula, és a dir, qui pren l'última granissa.

En aquest joc hi ha una estratègia que permet guanyar al primer jugador A, que és la següent: a cada moviment, prendre un nombre de granisses de forma que a la taula en quedi un nombre múltiple de 4. Més precisament,

1) prendre dues granisses al primer moviment;

2) als altres moviments, completar a quatre la tirada del jugador B, és a dir: si B en pren una, A en pren tres; si B en pren 2, A també i, si B en pren tres, aleshores A en pren una.

En efecte, fent-ho així, després de cada jugada de A, la quantitat de granisses que romanen a la taula és, successivament 16, 12, 8, 4 i 0, i, per tant, A guanya.

En aquest joc, el conjunt de posicions $\{16, 12, 8, 4, 0\}$ formen el que s'anomena el *nucli* del joc. Noteu que, des d'una posició del nucli un moviment sempre mena a una posició que no és del nucli i des d'una posició que no és del nucli sempre es pot fer un moviment que mena a una posició del nucli.

El *Nim* és un altre joc progressiu finit, però d'estratègia guanyadora més complicada. No és gens clar l'origen del nom *nim*. La popularització del joc en el món de les matemàtiques es deu a Charles L. Bouton[2], que el 1901 en va fer una anàlisi completa. En el seu article, Bouton reconeix que no ha estat capaç de descobrir massa res de la història del joc, i en proposa el nom de *nim* però no explica per quin motiu l'escull. Potser el nom prové del verb alemany *nimm* que vol dir *prendre*. Sigui com sigui, ha quedat fixat el nom de *nim*.[3]

Joc 8. El Nim

Inicialment hi ha sobre la taula de joc un cert nombre $n \geq 2$ de files i cada fila i té un cert nombre $p_i \geq 1$ de granisses. Una jugada vàlida consisteix en escollir una fila que no sigui buida i prendre d'aquesta fila el nombre de granisses que es vulgui. El primer jugador que no pot moure, perd; altrament dit, el jugador que neteja la taula guanya.

Per explicar l'estratègia guanyadora, identifiquem primer la posició inicial del joc amb la n-pla $(p_1, \ldots, p_n)$ on p_i és el nombre de granisses de la fila i. Les posicions possibles del joc són les n-ples $(q_1, \ldots, q_k)$ amb $0 \leq q_i \leq p_i$. Si el joc és a una posició $(q_1, \ldots, q_n)$, una tirada vàlida és prendre un cert nombre g de granisses d'una fila i. Naturalment, ha de ser $1 \leq g \leq q_i$. Així, un moviment és anar d'una posició $(q_1, \ldots, q_n)$ a una posició $(q_1, \ldots, q_i - g, \ldots q_n)$. Qui, amb un moviment, arriba a la posició $(0, \ldots, 0)$, guanya.

[2]Chales L. Bouton. St. Louis, Missouri, Estats Units d'Amèrica, 1869; Cambridge, Massachusetts, Estats Units d'Amèrica, 1922.

[3]No recordo qui em va fer notar que si escriviu la paraula NIM i gireu el full 180 graus, llegireu WIN, que vol dir *guanyar* en anglès.

El segon pas és pensar les coordenades q_i de les posicions en base 2. Si el p_i més gran té k xifres en base 2, identificarem cada posició amb una n-pla de k-eples posant els q_i en base 2 amb zeros a l'esquerra, si cal, per completar k coordenades. Per exemple, si hi ha tres files amb 5, 10 i 17 granisses respectivament, atès que

$$5 = 101_{2)}, \quad 10 = 1010_{2)}, \quad 17 = 10001_{2)},$$

la posició $(5, 10, 17)$ s'escriu $((0, 0, 1, 0, 1), (0, 1, 0, 1, 0), (1, 0, 0, 0, 1))$. Definim la *suma* de la posició com la suma mòdul 2 d'aquestes k-eples binàries, en el nostre cas

$$(0, 0, 1, 0, 1) + (0, 1, 0, 1, 0) + (1, 0, 0, 0, 1) = (1, 1, 1, 1, 0).$$

El *nucli* del joc és el conjunt de posicions de suma $\mathbf{0} = (0, \ldots, 0)$. Per exemple, la posició $(5, 10, 17)$ no és del nucli perquè té suma $(1, 1, 1, 1, 0)$. Però si prenem 2 granisses de la pila 3, ens quedarà la posició $(5, 10, 15)$ i, com que $15 = 1111_{2)}$, la posició $(5, 10, 15)$ té suma

$$(0, 0, 1, 0, 1) + (0, 1, 0, 1, 0) + (0, 1, 1, 1, 1) = (0, 0, 0, 0, 0),$$

i, per tant, $(5, 10, 15)$ és del nucli.

Notem que, si som a una posició del nucli, un moviment modificarà alguna coordenada d'un sumand i, per tant, la posició resultant ja no serà del nucli.

El punt crucial és el següent.

Proposició 5.1 *En el joc del nim, des d'una posició del nucli, qualsevol moviment duu a una posició que no és del nucli, i des d'una posició que no és del nucli, sempre es pot fer un moviment que mena a una posició del nucli.*

Demostració. Suposem que som a una posició del nucli. Un moviment consisteix en triar una pila i que té, diguem, q_i granisses, i prendre un cert nombre de granisses g. Si posem q_i i $q_i - g < q_i$ en binari, alguna coordenada de q_i haurà passat de 1 a 0. Per tant, a la suma, la coordenada corresponent haurà passat de 0 a 1 i obtindrem una posició que no és del nucli.

Recíprocament, suposem que una posició $(q_1, \ldots, q_n)$ no és del nucli. La suma té alguna coordenada que és 1. Sigui h la posició de la primera coordenada que és 1 a la suma. Triem una pila, diguem i, que a la coordenada h tingui un 1, i canviem el valor de totes les posicions de la pila i on la suma tingui un 1. Obtenim una k-epla que representa en binari un nombre $q_i' < q_i$. La posicó $(q_1, \ldots, q_i', \ldots, q_n)$ és del nucli perquè hem canviat les posicions on la suma tenia 1 i ara tindrà 0. Prenent $q_i - q_i'$ granisses de la pila i anem a la posició del nucli $(q_1, \ldots, q_i', \ldots, q_n)$. □

Exemple. A l'exemple d'abans, la suma corresponent a $(5, 10, 17)$ és

$$(0, 0, 1, 0, 1) + (0, 1, 0, 1, 0) + (1, 0, 0, 0, 1) = (1, 1, 1, 1, 0).$$

A la suma, la primera posició diferent de 0 és la primera. Escollim una pila que tingui un 1 a la primera posició: en aquest cas només pot ser la tercera. Com que la suma té uns a

les posicions 1, 2, 3 i 4, canviem aquestes coordenades a la pila 3 i obtenim $(0, 1, 1, 1, 1)$, que correspon al nombre 15. Farem, doncs, un moviment que deixi 15 granisses a la pila 3, és a dir, prendrem dues granisses de la pila 3.

Si la posició és $(5, 10, 15)$, com que

$$(0, 0, 1, 0, 1) + (0, 1, 0, 1, 0) + (0, 1, 1, 1, 1) = (0, 0, 0, 0, 0),$$

és del nucli, qualsevol moviment canviarà d'un únic sumand alguna coordenada i, per tant, canviarà la suma que ja no serà amb totes les coordenades 0 i, per tant, no serà del nucli. ‖

6 La constant de Kaprekar

Siguin A el conjunt de nombres enters positius de quatre xifres o menys no totes iguals. Siguin $n \in A$ i $a_0 \leq a_1 \leq a_2 \leq a_3$ les xifres de n ordenades de menor a major; afegim el nombre de zeros que calgui si el nombre té menys de quatre xifres per completar quatre xifres. Definim

$$T(n) = a_3a_2a_1a_0 - a_0a_1a_2a_3.$$

Exemples.

$$T(36) = T(0036) = 6300 - 0036 = 6264;$$
$$T(6264) = 6642 - 2466 = 4176.$$

Aquesta aplicació es diu *aplicació de Kaprekar*[4]

Joc 8. La constant de Kaprekar

Pere escull un nombre de A i itera la funció de Kaprekar fins que arriba a un nombre K tal que $T(K) = K$. Maria endevina K.

Kaprekar va observar un fet sorprenent. Si s'itera la seva aplicació, amb 7 o menys iteracions s'obté sempre el nombre 6174, que és el que diu Maria. No hi ha realment (o jo no la sé) una raó per la qual això passa. Simplement, es comprova que, sigui quin sigui el nombre inicial, s'acaba amb el 6174 que, és fix

$$T(6174) = 7641 - 1467 = 6174.$$

[4]Dattatreya Ramachandra Kaprekar. Danahu, la India, 1905; Devlali, la Índia, 1986.

En els programes que segueixen `kaprekar(n)` retorna el valor de la funció de Kaprekar per al nombre n, i `itkaprekar(n)` retorna la llista de tots els iterats fins al 6174.

```
def kaprekar(n):
    A=sorted(d2b(n,10))
    while len(A)<4:
      A=[0]+A
    B=[A[3-i] for i in [0..3]]
    A=b2d(A,10)
    B=b2d(B,10)
    return B-A
```

```
def itkaprekar(n):
    nou=n
    res=[nou]
    while nou !=6174:
      nou=kaprekar(nou)
      res=res+[nou]
    return res
```

Per exemple, com que

$$T(5107) = 7510 - 0157 = 7353;$$
$$T(7353) = 7533 - 3357 = 4176;$$
$$T(4176) = 7641 - 1467 = 6174.$$

`itkaprekar(5107)` retorna `[5107,7353,4176,6174]`.

Per veure que l'observació de Kaprekar és certa, prenem el conjunt A de tots els nombres enters x amb $1000 \leq x \leq 9998$, exclosos els que tenen quatre xifres iguals, que són els múltiples de 1111. Notem que als efectes de calcular les imatges per la funció de Kaprekar això és suficient perquè els nombres amb menys de quatre xifres tenen la mateixa imatge que els acabats en zeros, per exemple $T(97) = T(9700)$. Aleshores calculem $T(A) = \{T(x) : x \in A\}$ i $T^2(A) = T(T(A))$, etc. i comprovem que $T^7(A) = \{6174\}$.

`Iteracions(L)` calcula el conjunt imatge de `kaprekar` per a tots els nombres de la llista L i els posa en una llista, amb la qual torna a fer el mateix, i així successivament fins que la imatge es redueix al 6174. A cada iteració escriu els nombres de la imatge i quants n'hi ha.

```
def iteracions(L):
     nL=set(L)
     repetides={i*1111 for i in [0..8]}
     nL=nL.difference(repetides)
     while len(nL)>1:
          nL=set([kaprekar(x) for x in nL])
          print(len(nL))
          print(sorted(nL))
     return nL
```

Heus ací les iteracions:

```
iteracions([1000..9998])
54
[ 999, 1089, 1998, 2088, 2178, 2997, 3087, 3177, 3267, 3996, 4086, 4176,
 4266, 4356, 4995, 5085, 5175, 5265, 5355, 5445, 5994, 6084, 6174, 6264,
 6354, 6444, 6534, 6993, 7083, 7173, 7263, 7353, 7443, 7533, 7623, 7992,
 8082, 8172, 8262, 8352, 8442, 8532, 8622, 8712, 8991, 9081, 9171, 9261,
 9351, 9441, 9531, 9621, 9711, 9801]
20
[1089, 1998, 3087, 3996, 4176, 5265, 5355, 5994, 6174, 6264, 6354, 7173,
 7443, 7992, 8082, 8172, 8352, 8532, 8991, 9621]
14
[1998, 3087, 3996, 4176, 5355, 6174, 6264, 6354, 7173, 7443, 8082, 8352,
 8532, 9621]
10
[1998, 3087, 3996, 4176, 6174, 6264, 6354, 8082, 8352, 8532]
7
[3087, 4176, 6174, 6264, 8082, 8352, 8532]
4
[4176, 6174, 8352, 8532]
1
[6174]
{6174}
```

---

7 Successions tipus Fibonacci

Joc 8. Endevinar el terme següent d'un terme donat d'una successió tipus Fibonacci

Pere escull dos nombres enters $a_0 < a_1$ de dues xifres i per a $n \geq 2$, calcula

$$a_n = a_{n-1} + a_{n-2}$$

fins a un terme $n \geq 11$ de la seva elecció. Calcula també a_{n+1}. Pere diu quin nombre és a_n i, sense saber ni a_0, ni a_1 ni n, Maria endevina a_{n+1}.

Les successions que es defineixen a partir de dos valors inicials a_0 i a_1 i, després, cada terme és la suma dels dos anteriors ($a_n = a_{n-1} + a_{n-2}$) es diuen successions tipus Fibonacci[5]. La successió de Fibonacci per antonomàsia és la que comença amb $a_0 = 0$ i $a_1 = 1$.

[5]Leonardo Pisano Fibonacci. Pisa (avui Itàlia) 1170–1250.

L'objectiu immediat és obtenir una forma explícita per a la successió tipus Fibonacci de valors inicials a_0 i a_1. Per això ens calen unes propietats de les solucions d'una certa equació quadràtica.

Proposició 7.1 *Les solucions de l'equació quadràtica* $x^2 - x - 1 = 0$ *són*

$$\alpha = (1 + \sqrt{5})/2, \quad \beta = (1 - \sqrt{5})/2,$$

i compleixen

$$\begin{array}{llll} \alpha^0 = 1, & \alpha^1 = \alpha, & \alpha^n = \alpha^{n-1} + \alpha^{n-2} & \text{per a } n \geq 2, \\ \beta^0 = 1, & \beta^1 = \alpha, & \beta^n = \beta^{n-1} + \beta^{n-2} & \text{per a } n \geq 2. \end{array}$$

Demostració. Per veure que les solucions de l'equació quadràtica són α i β només cal aplicar la fórmula per resoldre equacions de segon grau.

Evidentment, $\alpha^0 = 1$ i $\alpha^1 = \alpha$. Ara, com que α és solució de $x^2 - x - 1 = 0$, tenim $\alpha^2 = \alpha + 1 = \alpha^1 + \alpha^0$. Si $n \geq 3$ i el resultat val per a un $n-1$, és a dir, $\alpha^{n-1} = \alpha^{n-2} + \alpha^{n-3}$, aleshores,

$$\alpha^n = \alpha \cdot \alpha^{n-1} = \alpha(\alpha^{n-2} + \alpha^{n-3}) = \alpha^{n-1} + \alpha^{n-2}.$$

L'argument és idèntic per a les β. □

Proposició 7.2 *Definim una successió* $(a_n : n \geq 0)$ *amb dos valors inicials* a_0, a_1 *i, per a* $n \geq 2$, $a_n = a_{n-1} + a_{n-2}$. *Siguin*

$$P = \frac{1}{\sqrt{5}}(a_1 - \beta a_0), \quad Q = \frac{1}{\sqrt{5}}(a_0\alpha - a_1).$$

Aleshores per a tot $n \geq 0$ *es compleix*

$$a_n = P\alpha^n + Q\beta^n.$$

Demostració. Per inducció sobre n. Per a $n = 0$ i $n = 1$, tenim

$$\begin{aligned} P + Q &= \frac{1}{\sqrt{5}}(a_1 - \beta a_0 + a_0\alpha - a_1) = \frac{1}{\sqrt{5}}a_0(\alpha - \beta) = \frac{1}{\sqrt{5}}a_0\sqrt{5} = a_0. \\ P\alpha + Q\beta &= \frac{1}{\sqrt{5}}(a_1\alpha - \alpha\beta a_0 + \beta\alpha a_0 - \beta a_1) = \frac{1}{\sqrt{5}}a_1(\alpha - \beta) = a_1. \end{aligned}$$

Per tant, la igualtat es compleix per a $n = 0$ i $n = 1$. Si $n \geq 2$ i es compleix per als valors anteriors, tenim

$$\begin{aligned} a_n &= a_{n-1} + a_{n-2} \\ &= P\alpha^{n-1} + Q\beta^{n-1} + P\alpha^{n-2} + Q\beta^{n-2} \\ &= P(\alpha^{n-1} + \alpha^{n-2}) + Q(\beta^{n-1} + \beta^{n-2}) \\ &= P\alpha^n + Q\beta^n. \qquad \square \end{aligned}$$

Ara, $\beta \simeq -0.618$. Com que $|\beta| < 1$, tenim $\lim_n \beta^n = 0$. Per tant, per a n prou gran, $a_n \simeq P\alpha^n$. Llavors,

$$\frac{a_{n+1}}{a_n} \simeq \frac{P\alpha^{n+1}}{P\alpha^n} = \alpha,$$

i resulta $a_{n+1} \simeq a_n\alpha$. Per tant, si Maria té emmagatzemat α a la calculadora i, quan li diuen a_n, el multiplica per α, si n és prou gran, l'enter més proper a αa_n és a_{n+1}. Calen, però, algunes precisions.

El significat de «l'enter més proper al nombre real x» resulta equívoc quan $x = z + 1/2$ per a un enter z. Quin és l'enter més proper a 3.5? El 3 o el 4? Depenent del context, s'adopta el conveni d'arrodonir per dalt (prendre el 4) o per baix (prendre el 3). En el nostre cas, com que α és irracional i a_n és un enter, el nombre αa_n no pot ser racional, o sigui que no és de la forma $z + 1/2$ amb z enter. Així doncs, en aquest context el cas dubtós no es presenta. Que a_{n+1} sigui l'enter més proper a αa_n és equivalent a dir que a_{n+1} és a una distància de αa_n menor que $1/2$: $|a_{n+1} - \alpha a_n| < 1/2$.

Assegurem:

• *Si $a_0 < a_1$ són nombres de dues xifres i $n \geq 11$, aleshores l'enter més proper a αa_n és el nombre a_{n+1}.*

Demostració. Volem demostrar que, en les condicions de l'enunciat,

$$|a_{n+1} - \alpha a_n| < 1/2.$$

Ara,

$$\begin{aligned} a_{n+1} - \alpha a_n &= P\alpha^{n+1} + Q\beta^{n+1} - \alpha P\alpha^n - \alpha Q\beta^n \\ &= Q\beta^n(\beta - \alpha) \\ &= -\sqrt{5}Q\beta^n = (a_0\alpha - a_1)\beta^n. \end{aligned}$$

Per tant, cal veure que en les condicions de l'enunciat, és a dir, amb a_0 i a_1 enters de dues xifres i $n \geq 12$, es compleix

$$|(a_0\alpha - a_1)\beta^n| < 1/2,$$

Ara,

$$-82.82 \simeq 10\alpha - 99 \leq a_0\alpha - a_1 \leq a_1\alpha - a_1 = a_1(\alpha - 1) \leq 99(\alpha - 1) < 61.2$$

Per tant,

$$|a_0\alpha - a_1| < 83.$$

Com que $|b^{11}| \cdot 83 < 0.41$, resulta que, per a $n \geq 11$ l'aproximació és, de fet, exacta i que l'enter més proper a αa_n és el nombre enter a_{n+1}. □

Remarca. La fita anterior és ajustada. Per exemple, si prenem $a_0 = 15$ i $a_1 = 99$, el desè terme és $a_{10} = 5955$ i l'enter més proper a αa_{10} resulta ser 9635, però $a_{11} = 9636$,

així que a_{11} no és l'enter més proper a αa_{10}. En canvi, l'enter més proper a αa_{11} sí que és $a_{12} = 15591$. ‖

`fibgen(a0,a1,n)` retorna la llista dels termes de la successió de Fibonacci de valors inicials a_0 i a_1 fins el terme a_n. La funció `proper(s)` arrodoneix $s\alpha$ a l'enter més proper.

```
def fibgen(a0,a1,n):
    if n==0:
       return [a0]
    if n==1:
       return [a0,a1]
    res=[a0,a1]
    it=1
    b0=a0
    b1=a1
    while it<n:
       nou=b0+b1
       res=res+[nou]
       b0=b1
       b1=nou
       it=it+1
    return res

def proper(s):
    return floor(s*(1+sqrt(5))/2+1/2)
```
