Butlletí de la Societat Catalana de Matemàtiques
Vol. 38, núm. 1, 2023. Pàg. 33–66. DOI: 10.2436/20.2002.01.108

Les matemàtiques dels setins

Carles Lladó i Josep M. Brunat

> Per això els textos i els teixits comparteixen tantes paraules: la trama del relat, el nus de l'argument, el fil de la història, el desenllaç de la narració; entortolligar-se el cervell, brodar un discurs, filar prim, ordir una intriga.
>
> **Irene Vallejo**
> ***L'infinit en un jonc,* segona part, 44**

Resum: Els setins són una classe especialment rellevant dels lligats dels teixits. Aquest article forneix un marc general que identifica un setí amb un reticle de $\mathbb{Z}^2$ i relaciona l'anàlisi dels setins amb resultats clàssics de teoria de nombres i de geometria. S'hi tracten els setins quadrats, els simètrics (en particular, simètrics rectangulars i simètrics rombals), i els setins concordants. També s'introdueixen els setins de Fibonacci, dels quals es caracteritzen els que són simètrics i els que són quadrats.

Paraules clau: lligat, curs, setí, setí quadrat, setí simètric, reticle, algorisme d'Euclides estès, base òptima, nombres de Fibonacci, setí de Fibonacci.

Classificació MSC2020: 11Z05, 52C05, 11A05, 11B39, 11B50.

1 Introducció

Els teixits a què ens referim en aquest article són els fabricats amb els telers. Deixarem de banda, per exemple, peces fetes amb un únic fil que s'entrellaça amb ell mateix, com passa amb el ganxet i el punt de mitja. En aquest text, doncs, un teixit consta d'un conjunt de fils paral·lels i equidistants, anomenats *fils de l'ordit*, i d'un conjunt de fils perpendiculars als anteriors, també equidistants, dits *fils de la trama* o *passades*. De fet, els que anomenem *fils de la trama* són un únic fil que va passant, mitjançant la llançadora del teler, successivament i alternativa de dreta a esquerra i d'esquerra a dreta; d'aquí el nom de *passada*. Un *punt* és un encreuament d'un fil de l'ordit i un de la trama.

Un punt es diu un *pren* o una *deixa* segons que, en aquest punt, el fil de l'ordit passi per sobre o per sota, respectivament, del de la trama.

El *tissatge* és el conjunt d'operacions en la confecció d'un teixit que tenen per objectiu entrellaçar els fils per fer-ne teles. Una part del tissatge està estretament relacionada amb els telers, l'evolució dels quals ha estat una llarga, complicada i interessant història. Però abans d'engegar el teler, o de fer-ne anar un de manual, cal decidir com s'entrellaçaran els fils. La forma en què els fils queden entrellaçats es diu *lligat* (o *lligament*). La forma tradicional de representar un lligat és mitjançant una quadrícula en la qual cada quadradet representa un punt. Les columnes il·lustren els fils de l'ordit, i les files, els fils de la trama. Un quadradet fosc representa un pren, i un de blanc, una deixa. A la figura 1 es mostren dos lligats i les seves respectives representacions per una quadrícula. En cada cas, a l'esquerra hi ha el lligat, on els fils s'han dibuixat prou amples per tal que es vegi bé si el fil de l'ordit passa per sobre o per sota del de la trama, és a dir, per remarcar si un punt és un pren o una deixa. A la dreta hi ha la representació del lligat per una quadrícula. El lligat i la representació se suposen estesos a tot el pla, tot deixant de banda el problema de les vores del teixit.

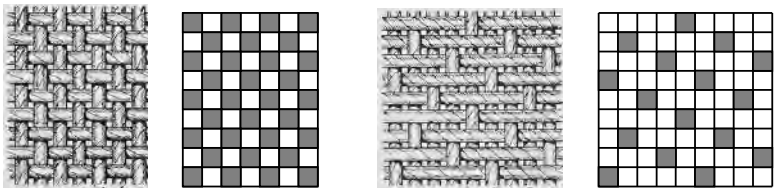


FIGURA 1

Tant per raons estètiques com per facilitat de fabricació, un lligat consisteix en còpies d'una peça quadrada o rectangular que es van juxtaposant en sentit de l'ordit i en el de la trama. Una peça mínima amb què, juxtaposant-la, s'obté el lligat es diu un *curs* del lligat. Atesa la generació del lligat a partir del curs, qualsevol punt es pot prendre com el punt inferior esquerre del curs, però és normal prendre el curs de manera que el seu punt inferior esquerre sigui un pren. Així, en el lligat de l'esquerra de la figura 1 podem identificar el seu curs com un quadrat de 2×2, mentre que en el lligat de la dreta el seu curs és un quadrat de 5×5. Tots dos es veuen a la figura 2. A la figura 3

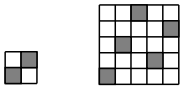


FIGURA 2

hem representat dos lligats més, que cal suposar estesos a tot el pla. En ambdós hem marcat còpies del curs, nou còpies d'un curs quadrat 4×4 en el primer

cas i quatre còpies d'un curs rectangular 8×4 en el segon. En tot el que segueix, però, centrarem l'atenció només en lligats de curs quadrat.

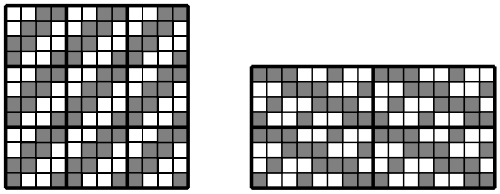


FIGURA 3

Naturalment, el curs cal dissenyar-lo de manera que, en juxtaposar les seves còpies, generi un lligat tal que el teixit que en resulti efectivament es «mantingui unit»; és a dir, que el conjunt de tots els fils quedin entrelligats de manera que sigui impossible de separar-los en dos subconjunts en què cada fil del primer subconjunt quedi per sobre de cada un dels fils del segon conjunt. Si es donés aquest cas, el teixit se separaria en dos. Per exemple, a l'esquerra de la figura 4 es veu un pretès curs, però a la dreta s'assenyalen els fils de l'ordit i de la trama que, entrelligats entre ells, queden per sobre i separats de la resta de fils, de manera que el pretès curs no genera un lligat.

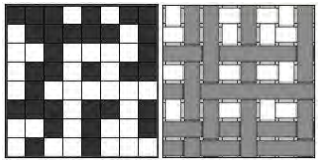


FIGURA 4

Sovint, només l'experiència indicava quins cursos donaven teixits que realment «es mantinguessin units». Però, a partir dels anys vuitanta del segle passat, es publiquen resultats generals i rigorosos en aquest sentit, com els de C. Delaney [8], R. E. Griswold [15], T. C. Enns [9] i C. R. J. Clapham [5]. Comentem aquest últim tot seguit. Clapham explicita una condició necessària i suficient sobre la quantitat de prens a cada fil de l'ordit i a cada fil de la trama del curs per tal de garantir que un curs generi un lligat. Com que ens restringirem a cursos quadrats, enunciem la condició de Clapham per a aquesta mena de cursos. El *mòdul* d'un curs quadrat és el nombre de fils de l'ordit i de la trama del curs.

PROPOSICIÓ 1. *Donat un curs quadrat de mòdul m, considerem el nombre de prens a cada fil de l'ordit del curs, i siguin $o_1 \geq o_2 \geq \cdots \geq o_m$ aquests nombres ordenats de major a menor. Anàlogament per als fils de la trama, siguin $t_1 \leq t_2 \leq \cdots \leq t_m$ els nombres corresponents ordenats de menor a major. Aleshores el curs genera un lligat si i només si per a cada $r, s \in \{1, \ldots, m\}$, es compleix*

$$\sum_{i=1}^{r} t_i + \sum_{j=1}^{s} (m - o_j) \geq rs, \tag{1}$$

i es compleix la igualtat per a $r = s = m$.

En un segon article [6], Clapham associa a cada curs un cert graf dirigit bipartit i mostra que la seva condició equival al fet que el graf dirigit sigui fortament connex, la qual cosa li permet obtenir condicions suficients sobre el nombre de prens en el curs en cada fil de l'ordit i de la trama per garantir un lligat.

Un *curs fonamental* és un curs quadrat tal que en cada fil de l'ordit del curs hi ha exactament un pren, la qual cosa comporta que en cada fil de la trama del curs hi hagi també un únic pren. Si el curs té mòdul m, aleshores el curs conté exactament m prens. La figura 5 mostra un curs fonamental de mòdul 8.

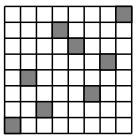


FIGURA 5

Els cursos fonamentals compleixen la condició de Clapham: tenim $t_i = o_i = 1$ per a $i \in \{1, \ldots, m\}$, i la desigualtat (1) de la proposició 1 esdevé $r + s(m-1) \geq rs$, que es compleix amb la desigualtat estricta si $m - 1 \geq r$ i val la igualtat per a $r = s = m$. Ara, en general, la irregularitat de la distribució dels prens en el curs no proporciona resultats estètics gaire valorats. Els setins, que definim tot seguit, tenen els prens disposats amb regularitat.

Lligat de setí

Un *setí* és un curs fonamental en el qual, a més del mòdul m, es fixa un nombre a anomenat *escalonat* que compleixi les condicions que $1 \leq a \leq m - 1$ i $\mathrm{mcd}(m, a) = 1$. El curs d'un setí de mòdul m i escalonat a consta de m fils de l'ordit, que numerarem $0, 1, \ldots, m-1$, i m fils de la trama, també numerats $0, \ldots, m-1$. La graella del curs la podem identificar amb $\mathbb{Z}_m \times \mathbb{Z}_m$. Els prens (x, y) del curs són els que compleixen $y \equiv ax \pmod{m}$, és a dir, els punts de l'aplicació $\mathbb{Z}_m \to \mathbb{Z}_m$ definida per $x \mapsto ax$. Aquesta aplicació és bijectiva perquè la condició $\mathrm{mcd}(m, a) = 1$ implica que a és invertible a $\mathbb{Z}_m$. A la figura 6 hi ha el curs del setí de mòdul 8 i escalonat 3.

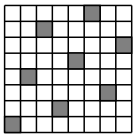


FIGURA 6

El setí de mòdul m i escalonat 1 es diu *sarja directa*, i el de mòdul m i escalonat $m - 1$ es diu *sarja indirecta*. En el cas $m = 2$, les dues sarges coincideixen i el setí es diu *plana* o *tafetà* (és el cas del curs de l'esquerra de

la figura 7). Tot i que, en textos clàssics, sarges i planes es consideren sovint diferents dels setins, en el model que seguirem és natural incloure-les entre els setins, encara que són, realment, casos extrems que de vegades cal tractar a part en determinades discussions. A la figura 7 hi ha representats també el curs de la sarja directa i el de la sarja indirecta de mòdul 5.

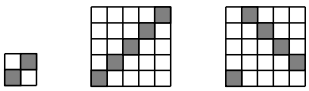


FIGURA 7

Si $k > 1$ és un enter, quan un fil d'ordit té prens en k passades consecutives, es diu que es forma una *basta d'ordit* de k, i es diu que es forma una *basta de trama* de k quan hi ha k deixes consecutives sobre una mateixa passada. En els lligats de setí no hi ha bastes d'ordit però cada passada té una basta de trama de $m - 1$. Així, en la figura 6 es poden veure les bastes de 7 que es formen en cada una de les passades del setí de mòdul 8 i escalonat 3. Des del punt de vista de les característiques materials del teixit a què donen lloc els lligats de setí, les bastes massa llargues són poc adequades. A la pràctica, sovint, hom parteix del curs d'un setí, i s'afegeixen de manera creativa nous prens amb la finalitat de reduir la longitud de les bastes. Aquests nous cursos s'anomenen *derivats*. A la figura 8 podem veure un curs derivat del curs del setí de mòdul 8 i escalonat 3 de la figura 6 obtingut afegint un pren a la dreta i al damunt de cada pren del setí original. A la figura, els punts de gris més clar són els prens del setí original, i els punts de gris fosc, els prens afegits. Es pot veure com les bastes d'ordit són com a màxim de 2 i les de trama són com a màxim de 3.

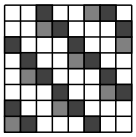


FIGURA 8

Des del camp del tissatge és interessant conèixer quants setins hi ha de mòdul m fixat. Com que un setí de mòdul m queda unívocament determinat pel seu escalonat a, que és un invertible de $\mathbb{Z}_m$, la funció ϕ d'Euler definida per als enters $m \geq 1$ per

$$\phi(m) = |\{a \in \{1, \ldots, m\} : \mathrm{mcd}(a, m) = 1\}|$$

dona el nombre de setins de mòdul m (incloses les dues sarges). Si es coneix la factorització de m en producte de primers, aleshores es pot calcular $\phi(m)$ com segueix (vegeu, per exemple D. M. Burton [3]).

PROPOSICIÓ 2. *Siguin* $2 \leq p_1 < p_2 \cdots < p_r$ *nombres primers i* $\alpha_1, \ldots, \alpha_r$ *enters positius. Si* $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, *el nombre de setins de mòdul* m *és*

$$\phi(m) = p_1^{\alpha_1 - 1} \cdots p_r^{\alpha_r - 1}(p_1 - 1) \cdots (p_r - 1) = m \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right).$$

Així, per exemple, el nombre de setins de mòdul $m = 15 = 3 \cdot 5$ és de $\phi(15) = 2 \cdot 4 = 8$, mentre que, si m és un nombre primer, aleshores $\phi(m) = m - 1$.

Segurament, el primer de considerar els setins des d'un punt de vista matemàtic fou Édouard Lucas [24] el 1867, motivat per dos articles del mateix any de l'industrial Édouard Gand [12, 13]. Lucas insistí en el tema amb un article i un apèndix en una revista italiana d'enginyeria [25, 26]. Cal reconèixer, però, que la bibliografia relacionada amb les matemàtiques dels setins i del disseny de teixits en general no és gaire abundant. Podem esmentar l'article de S. A. Shorter de 1920 [36]. Els articles de H. J. Woods [38, 39, 40, 41] dels anys 1935 i 1936 donen molta informació, però, tal com el mateix Woods diu en el primer article de la sèrie, «illustrations rather than proofs will be given of most of the statements made». Des del punt de vista matemàtic, els treballs dels anys vuitanta del segle passat de B. Grünbaum i G. C. Shephard [16, 17, 18] són més significatius. També D. W. Crowe ([7]) té un breu article sobre el treball de Woods, en el qual comenta de passada les etapes de matematització que representen alguns textos clàssics sobre ornamentació. En tot cas, l'interès principal en aquests treballs és la simetria dels teixits obtinguts. Més recentment, V. R. Krishnamurthy *et al.* ([22]) han desenvolupat un marc general per al disseny i construcció de formes entrellaçades que omplen l'espai i que tenen simetria induïda pels setins.

Ens ha semblat interessant fer palès un marc matemàtic general per estudiar els setins, que mena de forma natural a temes clàssics de teoria de nombres i de geometria. Els detalls de la major part del que reflectim aquí es poden trobar al llibre [23]; també hi resumim alguns resultats de [1]. L'apartat dels setins de Fibonacci és material nou. Hi ha també, de vegades en esquema, de vegades en detall, algun altre resultat suggerit per textos i articles antics de teoria de teixits. En tot cas, els setins conformen un exemple més de la ubiqüitat de les matemàtiques, exemple que ens sembla poc conegut i que amb aquestes pàgines pretenem divulgar.

2 Reticles. Bases òptimes

Des del punt de vista del model matemàtic, més útil que la tradicional representació per una quadrícula és emprar coordenades; això no és gaire usual en el context dels teixits, però un precedent ben antic, de 1870, és el de F. Cerruti [4]. Identificarem un setí amb un cert subgrup de $\mathbb{Z}^2$.

Si $\mathbf{u}$ i $\mathbf{v}$ són dos vectors independents de $\mathbb{Z}^2$, el *reticle* generat per $\mathbf{u}$ i $\mathbf{v}$ és el subgrup additiu de $\mathbb{Z}^2$

$$\langle \mathbf{u}, \mathbf{v} \rangle = \{\alpha\mathbf{u} + \beta\mathbf{v} : \alpha, \beta \in \mathbb{Z}\}.$$

La parella de vectors $(\mathbf{u}, \mathbf{v})$ es diu una *base* del reticle $\langle \mathbf{u}, \mathbf{v} \rangle$.

Denotem amb $L(m, a)$ un setí de mòdul m i escalonat a. Els prens (v, r) del curs són els que compleixen $av \equiv r \pmod{m}$. En juxtaposar còpies del curs per cobrir tot el pla, els prens $(v, r) \in \mathbb{Z}^2$ són, també, els que compleixen $av \equiv r \pmod{m}$. Aleshores

$$\begin{aligned}(v, r) \in L(m, a) &\Leftrightarrow av \equiv r \pmod{m} \\ &\Leftrightarrow r = av + \beta m \text{ per a algun } \beta \in \mathbb{Z} \\ &\Leftrightarrow (v, r) = v(1, a) + \beta(0, m) \text{ per a algun } \beta \in \mathbb{Z} \\ &\Leftrightarrow (v, r) \in \langle (1, a), (0, m) \rangle.\end{aligned}$$

D'acord amb això, el setí de mòdul m i escalonat a és el reticle $L(m, a) = \langle (1, a), (0, m) \rangle$. Així, la plana és el setí $L(2, 1) = \langle (1, 1), (0, 2) \rangle$, la sarja directa de mòdul m és el setí $L(m, 1) = \langle (1, 1), (0, m) \rangle$ i la sarja indirecta de mòdul m és el setí $L(m, m-1) = \langle (1, m-1), (0, m) \rangle$.

Per representar $L(m, a)$ com a reticle, prenem un pren com a origen de coordenades i, llavors, un punt de coordenades enteres (v, r) és un pren si i només si $av \equiv r \pmod{m}$.

Com que $|\det((1, a), (0, m))| = m$, el paral·lelogram de costats els dos vectors $(1, a)$ i $(0, m)$ amb origen a un pren té àrea m i no té prens al seu interior. A més, tots aquests paral·lelograms tessel·len el pla. La figura 9 mostra, a l'esquerra, el curs del lligat $L(7, 3)$ i, a la dreta, part del reticle corresponent, amb els paral·lelograms d'àrea 7 amb els costats determinats pels vectors $(1, 3)$ i $(0, 7)$ tessel·lant el pla. Els punts foscos corresponen als prens del curs.

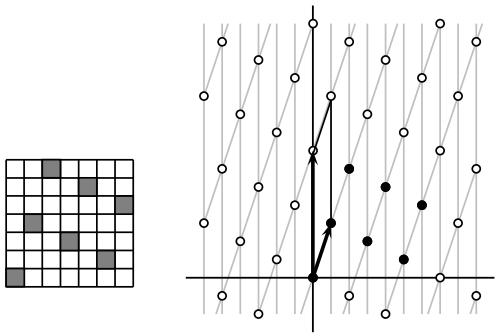


FIGURA 9

Naturalment, si $\mathbf{u} \in L(m, a)$, la translació de vector $\mathbf{u}$ deixa invariant $L(m, a)$. Les juxtaposicions del curs per crear el lligat corresponen a les imatges del curs per a les translacions de vectors $\mathbf{u} = \alpha(0, m) + \beta(m, 0)$ amb α i β enters.

Un setí $L(m,a)$ admet moltes bases: si dos vectors $\mathbf{x},\mathbf{y}\in L(m,a)$ compleixen

$$|\det(\mathbf{x},\mathbf{y})| = |\det((1,a),(0,m))| = m,$$

aleshores $(\mathbf{x},\mathbf{y})$ és també una base de $L(m,a)$. Una qüestió natural associada a un reticle, en particular a un setí, és trobar una base amb els dos vectors tan curts com sigui possible. Es defineix, doncs, una *base òptima* d'un reticle L com una base $(\mathbf{b}_1,\mathbf{b}_2)$ tal que

(1) $\|\mathbf{b}_1\| \le \|\mathbf{b}_2\|$;
(2) per a tot $\mathbf{x}\in L\setminus\{\mathbf{0}\}$, si $\|\mathbf{x}\| \le \|\mathbf{b}_2\|$, aleshores $\|\mathbf{x}\| = \|\mathbf{b}_1\|$ o $\|\mathbf{x}\| = \|\mathbf{b}_2\|$.

El vector $\mathbf{b}_1$ d'una base òptima $(\mathbf{b}_1,\mathbf{b}_2)$ és el *vector més curt*. Notem que l'article determinat és un abús de llenguatge perquè n'hi pot haver més d'un, per exemple, els vectors $\mathbf{b}_1$ i $-\mathbf{b}_1$ tenen la mateixa norma i tots dos es poden prendre com el vector més curt. Sovint prendrem un vector més curt amb la segona component positiva.

OBSERVACIÓ. En textos clàssics de teoria de teixits es troben nombrosos intents de classificar els setins basant-se en la geometria de la distribució dels prens, en particular mitjançant paral·lelograms que tenen per vèrtexs aquests punts. Aquest és el cas, per exemple, de V. Galcerán [11] i T. Giménez [14], entre d'altres. És possible que aquests intents responguessin en el fons a la voluntat de determinar bases òptimes.

Una base òptima d'un reticle $L=\langle\mathbf{u},\mathbf{v}\rangle$ es pot obtenir mitjançant l'algorisme de Lagrange-Gauss, que descrivim tot seguit (els detalls es poden trobar al llibre de J. Hoffstein, J. Pipher i J. H. Silverman [19] o al text de S. D. Galbraith [10]).

Per a un nombre real μ, sigui $\lfloor\mu\rceil$ l'enter més proper a μ i, si $\mu = z+1/2$ amb z enter, prenem $\lfloor\mu\rceil = z$. Denotem el producte escalar de dos vectors $\mathbf{u}$ i $\mathbf{v}$ amb $\mathbf{u}\cdot\mathbf{v}$. L'algorisme, que té una semblança amb el mètode de Gram-Schmidt per trobar una base ortonormal en un espai vectorial euclidià, és com segueix:

ENTRADA Una base $(\mathbf{u},\mathbf{v})$ d'un reticle L amb $\|\mathbf{u}\|\le\|\mathbf{v}\|$.
SORTIDA Una base òptima $(\mathbf{b}_1,\mathbf{b}_2)$ de L.
1) Fer $\mathbf{b}_1=\mathbf{u}$, $\mathbf{b}_2=\mathbf{v}$, $h=\lfloor(\mathbf{b}_1\cdot\mathbf{b}_2)/\|\mathbf{b}_1\|^2\rceil$.
2) Mentre $h\neq 0$ fer
   2.1) $\mathbf{b}_2=\mathbf{b}_2-h\mathbf{b}_1$;
   2.2) si $\|\mathbf{b}_2\|<\|\mathbf{b}_1\|$ intercanviar $\mathbf{b}_1$ i $\mathbf{b}_2$.
3) Retornar $(\mathbf{b}_1,\mathbf{b}_2)$.

EXEMPLE. Considerem el setí $L(16,7)$. Les iteracions de l'algorisme de Lagrange-Gauss donen els valors següents:

$$\begin{array}{llll}
\mathbf{b}_1=(1,7), & \mathbf{b}_2=(0,16), & h=\lfloor 112/50\rceil=2, & \mathbf{b}_2-2\mathbf{b}_1=(-2,2);\\
\mathbf{b}_1=(-2,2), & \mathbf{b}_2=(1,7), & h=\lfloor 12/8\rceil=1, & \mathbf{b}_2-\mathbf{b}_1=(3,5);\\
\mathbf{b}_1=(-2,2), & \mathbf{b}_2=(3,5), & h=\lfloor 4/8\rceil=0. &
\end{array}$$

Una base òptima del setí $L(16,7)$ és, doncs, $((-2,2),(3,5))$.

EXEMPLE. En el cas del setí $L(7,3)$ de la figura 9, l'algorisme de Lagrange-Gauss dona

$$\begin{array}{llll} \mathbf{b}_1 = (1,3), & \mathbf{b}_2 = (0,7), & h = \lfloor 21/10 \rceil = 2, & \mathbf{b}_2 = \mathbf{b}_2 - 2\mathbf{b}_1 = (-2,1); \\ \mathbf{b}_1 = (-2,1), & \mathbf{b}_2 = (1,3), & h = \lfloor 1/5 \rceil = 0. & \end{array}$$

Per tant, $((-2,1),(1,3))$ és una base òptima. La figura 10 mostra la mateixa part del setí que a la figura 9, però ara amb els paral·lelograms corresponents a la base òptima $((-2,1),(1,3))$.

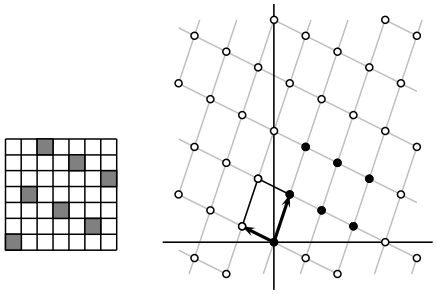


FIGURA 10

OBSERVACIÓ. Si $(\mathbf{u},\mathbf{v})$ és una base d'un reticle L amb $\|\mathbf{u}\| \le \|\mathbf{v}\|$ i $\mathbf{u}$ i $\mathbf{v}$ són ortogonals, aleshores la base $(\mathbf{u},\mathbf{v})$ és òptima perquè a la primera iteració de l'algorisme ja resulta $h = 0$.

OBSERVACIÓ. Suposem que $(\mathbf{u},\mathbf{v})$ és una base d'un reticle L i que $\mathbf{u}$ és el vector més curt de L. En aplicar l'algorisme a aquesta base, cal calcular $\mu = (\mathbf{u}\cdot\mathbf{v})/\|\mathbf{u}\|^2$ i $h = \lfloor \mu \rceil$. Si $h = 0$, la base $(\mathbf{u},\mathbf{v})$ és òptima; si no, el nou valor de h és $h' = \lfloor \mu' \rceil$, on

$$\mu' = \frac{1}{\|\mathbf{u}\|^2}(\mathbf{u}\cdot(\mathbf{v} - h\mathbf{u})) = \mu - h.$$

Com que $-1/2 < \mu - h \le 1/2$, tenim $h' = \lfloor \mu' \rceil = \lfloor \mu - h \rceil = 0$. Llavors, $(\mathbf{u}, \mathbf{v} - h'\mathbf{u})$ és una base òptima de L. Per tant, si una base de L conté el vector més curt, aleshores o bé la base ja és òptima o bé amb una etapa de l'algorisme de Lagrange-Gauss s'obté una base òptima.

Sigui per aplicació de l'algorisme de Lagrange-Gauss o sigui comprovant que els vectors que es donen són ortogonals i del reticle, s'obtenen les bases òptimes de la plana i de les sarges que s'indiquen a la taula 1.

lligat	reticle	base òptima
plana	$L(2,1)$	$((1,1),\ (-1,1))$
sarja directa m senar	$L(m,1)$	$((1,1),((-m+1)/2,(m+1)/2))$
sarja directa m parell	$L(m,1)$	$((1,1),(-m/2,m/2))$
sarja indirecta m senar	$L(m,m-1)$	$((-1,1),((m-1)/2,(m+1)/2))$
sarja indirecta m parell	$L(m,m-1)$	$((-1,1),(m/2,m/2))$

TAULA 1

Els dos setins $L(m,a)$ i $L(m,m-a)$ es diuen *complementaris*. Les següents equivalències, on cal entendre que les congruències ho són mòdul m, proven que setins complementaris són simètrics respecte als dos eixos de coordenades:

$$(v,r) \in L(m,a) \Leftrightarrow av \equiv r \Leftrightarrow (m-a)v \equiv -r \Leftrightarrow (v,-r) \in L(m,m-a)$$
$$\Leftrightarrow (-v,r) \in L(m,m-a).$$

Atès que l'origen de coordenades es pot prendre en qualsevol pren, els setins $L(m,a)$ i $L(m,m-a)$ són simètrics respecte a totes les rectes de la graella de coordenades enteres.

La simetria entre $L(m,a)$ i $L(m,m-a)$ implica que, a l'efecte de trobar bases òptimes, podem restringir el valor a de l'escalonat a $a < m/2$ perquè, si $((v_1,r_1),(v_2,r_2))$ és una base i òptima de $L(m,a)$, aleshores $((-v_1,r_1),(-v_2,r_2))$ és una base òptima de $L(m,m-a)$.

3 Obtenció de bases per l'algorisme d'Euclides

En aquest apartat veurem que l'algorisme d'Euclides aplicat al mòdul m i a l'escalonat a d'un setí proporciona una seqüència de vectors del setí tals que cada dos de consecutius formen una base, una de les quals conté el vector més curt.

Recordem que, donats dos enters m i a amb $1 \le a < m$, l'algorisme estès d'Euclides amb entrada (m,a) comença amb els valors inicials

$$(u_0,v_0,r_0) = (1,0,m), \quad (u_1,v_1,r_1) = (0,1,a),$$

i, per a cada enter $i \ge 1$, si q_i és el quocient de la divisió entera de r_{i-1} per r_i,

$$(u_{i+1},v_{i+1},r_{i+1}) = (u_{i-1},v_{i-1},r_{i-1}) - q_i(u_i,v_i,r_i).$$

La successió dels r_i és estrictament decreixent i existeix un n tal que $r_{n+1} = 0$. Aleshores $r_n = \mathrm{mcd}(m,a)$ i, per a tot $i \in \{0,\dots,n+1\}$, es compleix $u_i m + v_i a = r_i$. Per a $i = n$, es té la identitat de Bézout $u_n m + v_n a = \mathrm{mcd}(m,a)$.

La proposició que segueix explicita determinades propietats de la seqüència (u_i,v_i,r_i) generada per l'algorisme d'Euclides estès (els detalls es poden veure a V. A. Shoup [37, teorema 4.3]).

PROPOSICIÓ 3. *Siguin $m > a > 1$ enters i sigui (u_i,v_i,r_i), $i \in \{0,\dots,n+1\}$, la seqüència generada per l'algorisme d'Euclides estès aplicat a m i a.*

(i) *Per a tot $i \in \{2,\dots,n+1\}$, si i és parell, $u_i > 0$; si i és senar, $u_i < 0$.*

(ii) *Per a tot $i \in \{1,\dots,n+1\}$, si i és parell, $v_i < 0$; si i és senar, $v_i > 0$.*

(iii) $|u_{i+1}| \ge |u_i|$ *per a tot $i \in \{1,\dots,n\}$.*

(iv) $|v_{i+1}| \ge |v_i|$ *per a tot $i \in \{0,\dots,n\}$ i, si $a < m/2$, aleshores les desigualtats són estrictes.*

(v) *Si $r_n = \mathrm{mcd}(m,a) = 1$, aleshores $|u_n| \le a/2$ i $|u_{n+1}| = a$.*

(vi) *Si $r_n = \mathrm{mcd}(m,a) = 1$, aleshores $|v_n| \le m/2$ i $|v_{n+1}| = m$.*

Interpretem ara m i a com el mòdul i l'escalonat d'un setí $L(m,a)$, amb la qual cosa $u_n m + v_n a = 1$. Les igualtats $u_i m + v_i a = r_i$ impliquen $a v_i \equiv r_i \pmod{m}$, és a dir que $\mathbf{e}_i = (v_i, r_i) \in L(m,a)$ per a tot $i \in \{0,\dots,n+1\}$. Anomenarem

$$\mathbf{e}_0 = (v_0, r_0), \quad \mathbf{e}_1 = (v_1, r_1), \dots, \mathbf{e}_{n+1} = (v_{n+1}, r_{n+1})$$

els *vectors d'Euclides* del setí $L(m,a)$. D'acord amb l'algorisme,

$$\mathbf{e}_0 = (0,m), \quad \mathbf{e}_1 = (1,a), \quad \mathbf{e}_{i+1} = \mathbf{e}_{i-1} - q_i \mathbf{e}_i \quad (i \in \{1,\dots,n\}).$$

Notem que la primera parella de vectors d'Euclides $(\mathbf{e}_0, \mathbf{e}_1)$ coincideix amb la base inicial del setí i es compleix que el valor absolut del seu determinant és

$$|\det(\mathbf{e}_0, \mathbf{e}_1)| = |\det((0,m),(1,a))| = m.$$

Per a tot $i \geq 1$ tenim,

$$\begin{aligned} |\det(\mathbf{e}_i, \mathbf{e}_{i+1})| &= |\det(\mathbf{e}_i, \mathbf{e}_{i-1} - q_i \mathbf{e}_i)| = \\ &= |\det(\mathbf{e}_{i-1}, \mathbf{e}_i)| = \cdots = |\det(\mathbf{e}_0, \mathbf{e}_1)| = m. \end{aligned}$$

Per tant, totes les parelles $(\mathbf{e}_i, \mathbf{e}_{i+1})$ amb $i \in \{0,\dots,n\}$ són bases del setí.

El teorema següent assegura que entre els vectors d'Euclides de $L(m,a)$ es troba el vector més curt i, en alguns casos, dos vectors d'Euclides no necessàriament consecutius formen una base òptima (vegeu les proves a [1]).

TEOREMA 4. *Sigui $L(m,a)$ un setí amb $m > 2$ i $\mathbf{e}_i = (v_i, r_i)$, $i \in \{0,\dots,n+1\}$, els vectors d'Euclides de $L(m,a)$. Sigui $k = \min\{i : |v_i| > r_i\}$. Aleshores un dels quatre vectors $\mathbf{e}_{k-2}$, $\mathbf{e}_{k-1}$, $\mathbf{e}_k$ o $\mathbf{e}_{k+1}$ és el vector més curt de $L(m,a)$. A més,*

(i) *Si $\mathbf{e}_{k-2}$ és el vector més curt, aleshores $(\mathbf{e}_{k-2}, \mathbf{e}_{k-1})$ o $(\mathbf{e}_{k-2}, \mathbf{e}_k)$ és una base òptima.*

(ii) *Si $\mathbf{e}_{k+1}$ és el vector més curt, aleshores $(\mathbf{e}_{k+1}, \mathbf{e}_k)$ o $(\mathbf{e}_{k+1}, \mathbf{e}_{k-1})$ és una base òptima.*

La demostració de la primera part del teorema 4 es pot veure com segueix (vegeu la figura 11). Per a cada vector d'Euclides $\mathbf{e}_i = (v_i, r_i)$ de $L(m,a)$, considerem el punt del primer quadrant $\tilde{\mathbf{e}}_i = (|v_i|, r_i)$. Connectant punts d'índexs consecutius, obtenim una poligonal amb inici a $\tilde{\mathbf{e}}_0 = (0,m)$ i cada vèrtex més avall (perquè els r_i decreixen) i més a la dreta (perquè, d'acord amb la proposició 3, els $|v_i|$ creixen). El primer vèrtex després que la poligonal talli la bisectriu del quadrant correspon a l'índex k. El vector més curt correspon a un dels quatre punts més propers a la bisectriu.

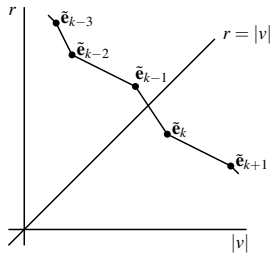


FIGURA 11

Sigui $L(m,a)$ un setí. Denotem amb a' l'enter tal que $1 \leq a' \leq m-1$ i $aa' \equiv 1 \pmod{m}$. Els setins $L(m,a)$ i $L(m,a')$ es diuen *associats*. Notem que, amb totes les congruències mòdul m,

$$(v,r) \in L(m,a) \Leftrightarrow av \equiv r \Leftrightarrow v \equiv a'r \Leftrightarrow (r,v) \in L(m,a') \Leftrightarrow (-r,-v) \in L(m,a'),$$

així que setins associats són simètrics respecte a la bisectriu dels quadrants primer i tercer i respecte a la bisectriu dels quadrants segon i quart.

Amb la notació de la proposició 3, si m i a són el mòdul i l'escalonat d'un setí $L(m,a)$, de la identitat de Bézout $u_n m + v_n a = \mathrm{mcd}(m,a) = 1$ s'obté $a' \equiv v_n \pmod{m}$. Si n és senar, tenim $v_n > 0$ i $a' = v_n < m/2$. Si n és parell, $v_n < 0$ i $m - a' = |v_n| < m/2$.

D'aquestes propietats de a' se'n dedueixen d'altres que tenen relació amb determinades bases d'un setí $L(m,a)$ que involucren a'. Suposem que n és senar. Els dos vectors $(1,a)$, $(a',1)$ són de $L(m,a)$ i el seu determinant és, en valor absolut, $|\det((1,a),(a',1))| = aa' - 1$. Per tant, $((1,a),(a',1))$ és una base de $L(m,a)$ si i només si $aa' - 1 = m$. Com que n és senar, $a' = v_n$ i $aa' - 1 = av_n - 1 = |u_n|m$, i la condició $aa' - 1 = m$ equival a $|u_n| = 1$. Anàlogament, si n és parell, $((1,a),(m-a',-1)) = ((1,a),(-v_n,-1))$ és una base si i només si $a(-v_n) + 1 = m$, és a dir, si $|u_n|m = m$, i retrobem la condició $|u_n| = 1$.

Els apartats següents es dediquen als setins quadrats, que són els que compleixen $a' = m - a$ (o, equivalentment, $a^2 \equiv -1 \pmod{m}$), i als simètrics, que són els que compleixen $a' = a$ (o, equivalentment, $a^2 \equiv 1 \pmod{m}$).

4 Setins quadrats

Definició

Ja des dels articles esmentats de Gand i Lucas el 1867 i de Woods el 1906, els setins quadrats han merescut atenció especial. El motiu és, generalment, estètic: tenen una simetria que els fa visualment atractius.

Formalment, un setí $L(m,a)$ és setí *quadrat* si compleix alguna de les condicions equivalents següents:

(a) El setí $L(m,a)$ admet una base òptima $(\mathbf{u},\mathbf{v})$ tal que $\mathbf{u}\cdot\mathbf{v}=0$ i $\|\mathbf{u}\|=\|\mathbf{v}\|$.
(b) El setí $L(m,a)$ és invariant per a girs d'angle recte centrat en un pren.
(c) Per a tot $(v,r)\in L(m,a)$, es compleix $(-r,v)\in L(m,a)$.

Les condicions anteriors són de tipus geomètric, però es poden traduir fàcilment a la condició aritmètica següent:

PROPOSICIÓ 5. *Un setí $L(m,a)$ és setí quadrat si i només si $a^2+1\equiv 0 \pmod m$.*

PROVA. (Totes les congruències de la prova ho són mòdul m.) Suposem que $L(m,a)$ és quadrat. Com que $(1,a)\in L(m,a)$, tenim $(-a,1)\in L(m,a)$, és a dir, $a(-a)\equiv 1$, o sigui $a^2\equiv -1$. Recíprocament, si $a^2\equiv -1$, aleshores $\mathrm{mcd}(m,a)=1$ i

$$(v,r)\in L(m,a)\Leftrightarrow av\equiv r\Leftrightarrow a^2v\equiv ar\Leftrightarrow v\equiv -ar\Leftrightarrow(-r,v)\in L(m,a),$$

i el setí $L(m,a)$ és quadrat. □

Notem que, per a un setí $L(m,a)$ quadrat, si $(\mathbf{u},\mathbf{v})$ és una base òptima, l'àrea del paral·lelogram determinat per $\mathbf{u}$ i $\mathbf{v}$ és alhora $\|\mathbf{u}\|^2$ i $|\det(\mathbf{u},\mathbf{v})|=m$, així que $\|\mathbf{u}\|^2=\|\mathbf{v}\|^2=m$.

A la figura 12 es veu el curs del setí quadrat de mòdul $m=13$ i escalonat $a=5$, amb uns quadrats remarcats no determinats per cap base del setí. En un setí quadrat $L(m,a)$, l'existència d'aquests quadrats s'ha pres de vegades com a justificació de l'adjectiu «quadrat» aplicat a aquest setí; vegeu, per exemple, E. Gand [12], E. Lucas [24] i P. Rodón y Amigó [29].

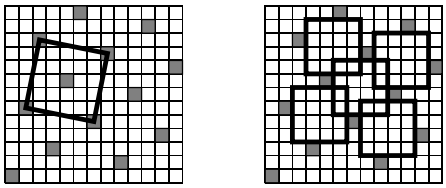


FIGURA 12

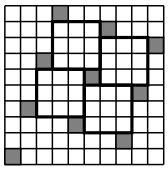


FIGURA 13

Si un setí quadrat $L(m,a)$ admet el vector $(1,a)$ com a vector més curt, aleshores els quadrats com els de la dreta de la figura 12 tessel·len el pla, excepte els prens, és a dir, tessel·len totes les deixes. Per exemple, el setí quadrat $L(10,3)$ admet la base òptima $((1,3),(-3,1))$, i la quadrícula del setí

es pot veure a la figura 13 amb els quadrats marcats tessel·lant totes les deixes del lligat. En general, si $a > 2$ és un enter i definim $m = a^2 + 1$, aleshores, $\mathrm{mcd}(m, a) = 1$ i $L(m, a)$ és un setí quadrat que admet la base òptima $((1, a), (-a, 1))$. Recíprocament, si $L(m, a)$ és un setí quadrat que admet una base òptima $((1, x), (-x, 1))$, aleshores $m = |\det((1, x), (-x, 1))| = 1 + x^2$ i tenim $|x| < m/2$ i $a \equiv x \pmod{m}$. Si $x > 0$, llavors $a = x$. Si $x < 0$, llavors $a = m - |x|$. Per tant, els setins quadrats que produeixen aquestes tessel·lacions corresponen als setins $L(m, a)$ amb $m = a^2 + 1$ i als seus complementaris.

Curiosament, aquest tipus de tessel·lacions són el patró que es pot veure en determinats enrajolats modernistes, com el del bany de la casa Navàs de Reus, on es pot trobar l'enrajolat de la figura 14, que correspon al setí $L(5, 3)$, del qual hem remarcat un curs. Les rajoles petites amb flors corresponen als prens. El complementari de $L(5, 3)$ és $L(5, 2)$ (que compleix $5 = 2^2 + 1$), el qual té base òptima $((1, 2), (-2, 1))$.

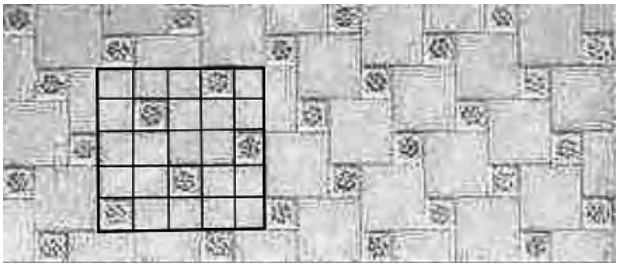


FIGURA 14

L'algorisme d'Euclides en setins quadrats

L'algorisme d'Euclides, aplicat als setins quadrats, té algunes propietats addicionals curioses que permeten obtenir una base òptima. Resumim els resultats en el teorema següent, la prova del qual es pot veure a [1, 23]. Deixarem de banda la plana, de base òptima $((-1, 1), (1, 1))$, i les sarges, que no són setins quadrats. També hem comentat que, a l'efecte de trobar bases òptimes de setins $L(m, a)$, la condició $a < m/2$ no és restrictiva.

TEOREMA 6. *Sigui $L(m, a)$ un setí amb $1 < a < m/2$ i $m \geq 5$, i siguin $\mathbf{e}_i = (v_i, r_i)$, $i \in \{0, \ldots, n + 1\}$, els vectors d'Euclides. Aleshores $L(m, a)$ és quadrat si i només si $v_n = -a$. En aquest cas, es compleixen les propietats següents:*

(i) *n és parell;*

(ii) *$|v_{n+1-i}| = r_i$ per a $i \in \{0, \ldots, n + 1\}$;*

(iii) *$\|\mathbf{e}_{n+1-i}\| = \|\mathbf{e}_i\|$ per a $i \in \{0, \ldots, n + 1\}$;*

(iv) *si $k = \min\{i : |v_i| > r\}$, aleshores $k = (n + 2)/2$;*

(v) *si $k = (n + 2)/2$, aleshores $(\mathbf{e}_{k-1}, \mathbf{e}_k)$ és una base òptima.*

Així, per trobar una base òptima d'un setí quadrat, només cal aplicar l'algorisme d'Euclides fins a trobar un índex k tal que $|v_k| > r_k$. Llavors, $(\mathbf{e}_{k-1}, \mathbf{e}_k)$ és una base òptima.

EXEMPLE. Considerem el setí $L(65,18)$. Com que $18^2 + 1 = 325 = 65 \cdot 5$, el setí $L(65,18)$ és quadrat. L'algorisme d'Euclides dona

i	0	1	2	3	4	5	6	7
v_i	0	1	-3	4	-7	11	-18	65
q_i		3	1	1	1	1	3	
r_i	65	18	11	7	4	3	1	0
r_{i+2}	11	7	4	3	1	0		

Veiem que (i) $n = 6$ és parell; (ii) els valors dels $|v_i|$ llegits de dreta a esquerra coincideixen amb els dels r_i llegits d'esquerra a dreta; (iii) les parelles de vectors

$$\mathbf{e}_0 = (0,65) \quad \text{i} \quad \mathbf{e}_7 = (65,0), \qquad \mathbf{e}_1 = (1,18) \quad \text{i} \quad \mathbf{e}_6 = (-18,1),$$
$$\mathbf{e}_2 = (-3,11) \quad \text{i} \quad \mathbf{e}_5 = (11,3), \qquad \mathbf{e}_3 = (4,7) \quad \text{i} \quad \mathbf{e}_4 = (-7,4),$$

tenen la mateixa norma; (iv) $k = \min\{i : |v_i| > r\} = 4 = (n+2)/2$. Finalment, el teorema assegura que $(\mathbf{e}_3, \mathbf{e}_4)$ és una base òptima.

Mòduls i escalonats de setins quadrats

En els textos clàssics de teoria de teixits hi ha hagut força interès a trobar els mòduls m que admeten escalonats a tals que $L(m,a)$ sigui quadrat.

Donat un enter $m \geq 2$, un enter z és un *residu quadràtic* mòdul m si existeix un enter a tal que $a^2 \equiv z \pmod{m}$. Determinar si un enter z és o no un residu quadràtic mòdul m és un tema clàssic de la teoria de nombres. Veiem que un setí de mòdul m admet un escalonat a tal que $L(m,a)$ és quadrat si i només si -1 és un residu quadràtic mòdul m, i els escalonats són les solucions a de la congruència $a^2 \equiv -1 \pmod{m}$ compreses entre 1 i $m-1$.

Per al mòdul $m = 2$, només hi ha un escalonat possible, $a = 1$, i s'obté la plana, que és un setí quadrat. Deixarem de banda aquest cas en el que queda d'apartat, i considerarem només mòduls $m > 2$. Per a mòduls primers, tenim el resultat següent (la prova es pot veure, per exemple, a D. M. Burton [3, teorema 5.5]).

TEOREMA 7. *Sigui $p > 2$ un nombre primer. Aleshores la congruència $x^2 \equiv -1 \pmod{p}$ té solució si i només si $p \equiv 1 \pmod{4}$. En aquest cas, les dues solucions són $x \equiv \pm((p-1)/2)! \pmod{p}$.*

En termes de setins:

TEOREMA 8. *Sigui $p > 2$ un nombre primer.*

(i) *Si $p \equiv 3 \pmod{4}$, aleshores no hi ha setins quadrats de mòdul p.*

(ii) *Si $p \equiv 1 \pmod{4}$, sigui $a \equiv ((p-1)/2)! \pmod{p}$ amb $1 < a < p-1$. Aleshores hi ha exactament dos setins quadrats de mòdul p, que són els setins complementaris $L(p,a)$ i $L(p,p-a)$.*

Considerem ara els mòduls m que són potències de primer. Si $k > 1$ és un enter i $m = 2^k$, la congruència $x^2 + 1 \equiv 0 \pmod{2^k}$ no té solució: en efecte, una solució x també és solució respecte al mòdul $2^2 = 4$. Però $x^2 + 1 \equiv 0 \pmod 4$ no té solució. Per tant, no hi ha setins quadrats de mòdul $m = 2^k$ amb $k > 1$.

Sigui ara un enter $k > 1$, un enter primer $p > 2$ i $m = p^k$. Si $x^2 + 1 \equiv 0 \pmod{p^k}$, aleshores $x^2 + 1 \equiv 0 \pmod p$. Per tant, si $x^2 + 1 \equiv 0 \pmod{p^k}$ té solució, també en té $x^2 + 1 \equiv 0 \pmod p$ i ha de ser $p \equiv 1 \pmod 4$.

Queda per estudiar el cas que el mòdul és $m = p^k$ amb $k \geq 1$ enter i p un primer $p \equiv 1 \pmod 4$. El teorema 7 assegura que, en el cas $k = 1$, hi ha dues solucions. El lema següent, que és una versió particular de l'anomenat *lema de Hensel* (vegeu, per exemple, I. Niven, H. S. Zuckerman, H. L. Montgomery [27, teorema 2.23]), mostra com, disposant d'una solució mòdul p^s, se'n pot trobar una altra mòdul p^{s+t} amb $t \leq s$, la qual es diu l'*aixecada* a p^{s+t} de la primera.

LEMA 9. *Siguin $p > 2$ un nombre primer, $s \geq t \geq 1$ enters, i a i h enters tals que $a^2 + 1 = hp^s$.*

(i) *Existeix l'invers v de $2a$ mòdul p^t.*

(ii) *Sigui $y \equiv -hv \pmod{p^t}$. Aleshores $a + yp^s$ és solució de $x^2 + 1 \equiv 0 \pmod{p^{s+t}}$.*

Així, si $p > 2$ és un nombre primer amb $p \equiv 1 \pmod 4$, i $k > 1$, podem calcular els dos escalonats que donen setins quadrats de mòdul p i, per aplicació del lema de Hensel, trobar dos escalonats d'un setí de mòdul p^k que donin setins quadrats. I només n'hi ha dos: la congruència $x_1^2 + 1 \equiv x_2^2 + 1 \equiv 0 \pmod{p^k}$ implica $x_1^2 - x_2^2 = (x_1 + x_2)(x_1 - x_2) \equiv 0 \pmod{p^k}$. Si p divideix els dos factors, aleshores p divideix la seva diferència $2x_2$ i, com que $p > 2$, divideix x_2. Aleshores $1 \equiv x_2^2 + 1 \equiv 0 \pmod p$, la qual cosa és contradictòria. Per tant, p només divideix un dels factors i passa el mateix amb p^k. Si p^k divideix $x_1 + x_2$, tenim $x_1 \equiv -x_2 \pmod{p^k}$. Si divideix $x_1 - x_2$, tenim $x_1 \equiv x_2 \pmod{p^k}$. Per tant, tenim:

TEOREMA 10. *Sigui $k > 1$ un enter i $p \geq 2$ un nombre primer.*

(i) *Si $p = 2$ o $p \equiv 3 \pmod 4$, no existeixen setins quadrats de mòdul $m = p^k$.*

(ii) *Si $p \equiv 1 \pmod 4$, existeixen exactament dos setins quadrats de mòdul $m = p^k$, els escalonats dels quals s'obtenen aixecant els dos escalonats dels setins quadrats de mòdul p.*

Si es coneix la factorització d'un enter $m > 2$ en producte de primers, els escalonats a tals que $L(m, a)$ és quadrat es troben emprant els resultats per a quan el mòdul m és una potència de primer i el teorema xinès dels residus. El resultat és el següent.

TEOREMA 11. *Sigui $m = 2^{\alpha_0} p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ amb $2 < p_1 < \cdots < p_s$ primers diferents, $\alpha_0 \geq 0$ i $\alpha_1, \ldots, \alpha_s \geq 1$ enters. Existeixen setins quadrats de mòdul m si i només si $\alpha_0 \in \{0, 1\}$ i $p_i \equiv 1 \pmod 4$ per a $i \in \{1, \ldots, s\}$. En aquest cas, el nombre d'escalonats de setins quadrats és 2^s.*

Una altra caracterització dels mòduls dels setins quadrats s'obté de la caracterització de Fermat dels enters positius m que són suma de dos quadrats, és a dir, que són de la forma $m = x^2 + y^2$ per a certs enters x i y (vegeu, per exemple, D. M. Burton [3, teorema 13.3]).

TEOREMA 12 (FERMAT). *Un enter positiu m és suma de dos quadrats si i només si cada factor primer p de m tal que $p \equiv 3 \pmod 4$ apareix amb exponent parell a la factorització de m en producte de primers.*

Aleshores es té:

TEOREMA 13. *Un enter positiu $m > 2$ és el mòdul d'un setí quadrat si i només si existeixen enters x i y tals que $m = x^2 + y^2$ i $\operatorname{mcd}(x, y) = 1$. En aquest cas, si z és l'invers de x mòdul m i $a \equiv zy \pmod m$, $1 < a < m - 1$, el setí $L(m, a)$ és quadrat.*

PROVA. Si $L(m, a)$ és un setí quadrat, sigui $((x, y), (-y, x))$ una base òptima de $L(m, a)$. Llavors, $m = |\det((x, y), (-y, x))| = x^2 + y^2$ és suma de dos quadrats. Per a certs enters z i t tenim que $a^2 + 1 = zm$ i $y = ax + tm$. Aleshores

$$\begin{aligned} m = x^2 + y^2 &= x^2 + (ax + tm)^2 = \\ &= (1 + a^2)x^2 + tm(tm + 2ax) = \\ &= zmx^2 + tm(tm + ax + ax) = \\ &= m(zx + ta)x + tmy. \end{aligned}$$

Simplificant m, obtenim $1 = (zx + ta)x + ty$, la qual cosa implica $\operatorname{mcd}(x, y) = 1$.

Recíprocament, suposem que existeixen els enters x i y tals que $m = x^2 + y^2$ i $\operatorname{mcd}(x, y) = 1$. Aleshores $\operatorname{mcd}(m, x) = \operatorname{mcd}(m, y) = 1$ i $\operatorname{mcd}(m, a) = 1$. A més,

$$a^2 + 1 \equiv z^2y^2 + 1 \equiv z^2(m - x^2) + 1 \equiv z^2m - z^2x^2 + 1 \equiv 0 \pmod m,$$

i $L(m, a)$ és un setí quadrat. □

5 Setins simètrics

Definició

Per motius similars als dels setins quadrats, els setins simètrics també han merescut força interès. Un setí $L(m, a)$ és setí *simètric* si compleix les condicions equivalents següents:

(a) Si $(x, y) \in L(m, a)$, aleshores $(y, x) \in L(m, a)$, és a dir, si el reticle $L(m,a)$ és simètric respecte a la bisectriu del primer i tercer quadrants.

(b) Si $(x, y) \in L(m, a)$, aleshores $(-y, -x) \in L(m, a)$, és a dir, si el reticle $L(m, a)$ és simètric respecte a la bisectriu del segon i quart quadrants.

La traducció a una condició aritmètica és immediata:

PROPOSICIÓ 14. *Un setí $L(m,a)$ és setí simètric si i només si $a^2 \equiv 1 \pmod m$.*

PROVA. Si $L(m,a)$ és simètric, com que $(1,a) \in L(m,a)$, resulta que $(a,1) \in L(m,a)$, això és, $a^2 \equiv 1 \pmod m$. Recíprocament, si $L(m,a)$ és un setí tal que $a^2 \equiv 1 \pmod m$, aleshores és simètric: si $(x,y) \in L(m,a)$, tenim $ax \equiv y \pmod m$ i $x \equiv a^2x \equiv ay \pmod m$, és a dir, $(y,x) \in L(m,a)$. □

La condició $a^2 \equiv 1 \pmod m$ és equivalent a la condició $a' = a$, així que un setí simètric es pot definir també com un setí igual al seu associat. Les sarges, per exemple, són setins simètrics.

Una base $(\mathbf{u},\mathbf{v})$ d'un setí és *rectangular* si $\mathbf{u} \cdot \mathbf{v} = 0$. Evidentment, una base rectangular és òptima. Un *setí rectangular* és un setí que admet una base rectangular. Segons la taula 1, la sarja directa de mòdul m parell, per exemple, admet la base rectangular $((1,1),(-m/2,m/2))$, i la sarja indirecta de mòdul m parell admet la base rectangular $((-1,1),(m/2,m/2))$.

Una base $(\mathbf{u},\mathbf{v})$ d'un setí és *rombal* si $\|\mathbf{u}\| = \|\mathbf{v}\|$. Un *setí rombal* és un setí que admet una base rombal. Per exemple, l'aplicació de l'algorisme de Lagrange-Gauss a $L(24,5)$ dona la base rombal òptima $((1,5),(5,1))$. Ara, mentre que una base rectangular és automàticament òptima, no passa el mateix amb una base rombal. Per exemple, una sarja indirecta de mòdul m senar admet la base òptima $((-1,1),(m-1)/2,(m+1)/2))$, que no és ni rombal ni rectangular. Però, per simetria, el vector$((m+1)/2,(m-1)/2)$ també és del setí i, com que

$$\left|\det\left(\left(\frac{m-1}{2},\frac{m+1}{2}\right),\left(\frac{m+1}{2},\frac{m-1}{2}\right)\right)\right| = m,$$

la parella $((m-1)/2,(m+1)/2)),((m+1)/2,(m-1)/2))$ és una base, evidentment rombal.

L'algorisme d'Euclides en setins simètrics

També per a setins simètrics l'algorisme d'Euclides té propietats addicionals. Les resumim tot seguit (vegeu [1, 23]).

PROPOSICIÓ 15. *Sigui $L(m,a)$ un setí amb $a < m/2$ i siguin $\mathbf{e}_i = (v_i,r_i)$, $i \in \{0,\dots,n+1\}$, els vectors d'Euclides. Llavors, el setí $L(m,a)$ és simètric si i només si $v_n = a$. En aquest cas, es compleixen les propietats següents:*

(i) *n és senar;*
(ii) *$|v_{n+1-i}| = r_i$ per a $i \in \{0,\dots,n+1\}$;*
(iii) *$|v_j| = r_j$ per a $j = (n+1)/2$;*
(iv) *$\|\mathbf{e}_{n+1-i}\| = \|\mathbf{e}_i\|$;*
(v) *si $k = \min\{i : |v_i| > r_i\}$, aleshores $k = (n+3)/2$;*
(vi) *si $k = (n+3)/2$ i $\mathbf{e}_{k-2}$ és el vector més curt, aleshores $(\mathbf{e}_{k-2},\mathbf{e}_k)$ és una base rombal òptima.*

EXEMPLE. El setí $L(30,11)$ és simètric perquè $11^2 = 121 = 30 \cdot 4 + 1 \equiv 1 \pmod{30}$. L'algorisme d'Euclides dona

i	0	1	2	3	4	5	6
v_i	0	1	-2	3	-8	11	-30
q_i		2	1	2	1	2	
r_i	30	11	8	3	2	1	0
r_{i+2}	8	3	2	1	0		

Obtenim, doncs, els vectors d'Euclides

$$\mathbf{e}_0 = (0,30), \quad \mathbf{e}_1 = (1,11), \quad \mathbf{e}_2 = (-2,8), \quad \mathbf{e}_3 = (3,3),$$
$$\mathbf{e}_4 = (-8,2), \quad \mathbf{e}_5 = (11,1), \quad \mathbf{e}_6 = (-30,0).$$

Veiem que (i) $n = 5$ és senar; (ii) la seqüència dels $|v_i|$ llegida de dreta a esquerra coincideix amb la dels r_i llegida d'esquerra a dreta; (iii) per a $j = (n+1)/2 = 3$ tenim $|v_3| = r_3 = 3$; (iv) les parelles de vectors

$$\mathbf{e}_0 \text{ i } \mathbf{e}_6, \quad \mathbf{e}_1 \text{ i } \mathbf{e}_5, \quad \mathbf{e}_2 \text{ i } \mathbf{e}_4,$$

tenen la mateixa norma; (v) el primer índex k tal que $|v_k| > r_k$ és $k = 4 = (n+3)/2$; (vi) en aquest cas el vector més curt és $\mathbf{e}_3 = (3,3)$ i l'algorisme no dona una base òptima. Aplicant una etapa de l'algorisme de Lagrange-Gauss a la base $(\mathbf{e}_2, \mathbf{e}_3)$ s'obté la base òptima $((3,3),(-5,5))$, que és rectangular.

Setins simètrics rombals i rectangulars

B. Grünbaum i G. C. Shephard ([16]) afirmen que tot setí simètric és rectangular o rombal i donen un esquema de la demostració. El resultat que descrivim en aquest subapartat dona condicions aritmètiques per decidir una cosa o l'altra, i per trobar bases òptimes i rombals (vegeu [1]).

Associat a un setí simètric $L(m,a)$, definim els paràmetres i vectors següents:

(a) $d_1 = \operatorname{mcd}(a+1, m)$, $\quad \mathbf{d}_1 = (d_1, d_1)$.

(b) $m_1 = m/d_1$, $\quad \mathbf{m}_1 = (-m_1, m_1)$.

(c) Si m_1 és parell i $a^2 - 1 \equiv 0 \pmod{2m}$, $\quad \mathbf{w}_1 = (d_1/2, d_1/2)$.

(d) Si m_1 és parell i $a^2 - 1 \not\equiv 0 \pmod{2m}$, $\quad$ o si m_1 és senar,

$$x_1 = (d_1 + m_1)/2, \quad \mathbf{u}_1 = (d_1 - x_1, x_1), \quad \mathbf{v}_1 = (x_1, d - x_1).$$

Es pot demostrar que $\mathbf{d}_1, \mathbf{m}_1 \in L(m,a)$ i que, en les condicions de (c), es compleix $\mathbf{w}_1 \in L(m,a)$ i, en les de (d), es compleix $\mathbf{u}_1, \mathbf{v}_1 \in L(m,a)$. A més, es pot veure fàcilment que l'únic setí simètric amb $m_1 = d_1$ és la sarja directa de mòdul $m = 4$. Deixem de banda, doncs, la plana i les sarges. El teorema següent classifica els setins simètrics en rectangulars i rombals i dona en cada cas una base òptima i, en el cas dels rombals, també una base rombal.

TEOREMA 16. *Sigui $L(m,a)$ un setí simètric amb $m \geq 5$ i $1 < a < m-1$.*

(i) *Si m és parell i $a^2 - 1 \equiv 0 \pmod{2m}$, llavors el setí és rectangular. En aquest cas, d_1 és parell i $d_1/2 \neq m_1$. A més, una base rectangular òptima és $(\mathbf{w}_1, \mathbf{m_1})$ si $d_1/2 < m_1$ o $(\mathbf{m_1}, \mathbf{w}_1)$ si $m_1 < d_1/2$.*

(ii) *Si m és parell i $a^2 - 1 \not\equiv 0 \pmod{2m}$, o si m és senar, llavors $(\mathbf{u}_1, \mathbf{v}_1)$ és una base rombal de $L(m,a)$. En aquest cas, $(\mathbf{d}_1, \mathbf{u}_1)$ i $(\mathbf{m}_1, \mathbf{u}_1)$ també són bases, els tres vectors $\mathbf{d}_1$, $\mathbf{m_1}$ i $\mathbf{u}_1$ tenen normes diferents i, si $\mathbf{e}$ és el de menor norma dels tres, es dona exactament una de les tres situacions següents:*

(ii.1) $\mathbf{e} = \mathbf{d}_1$, $3d_1^2 < m_1^2$, *i* $(\mathbf{d}_1, \mathbf{u}_1)$ *és una base òptima.*

(ii.2) $\mathbf{e} = \mathbf{m_1}$, $3m_1^2 < d_1^2$, *i* $(\mathbf{m_1}, \mathbf{u}_1)$ *és una base òptima.*

(ii.3) $\mathbf{e} = \mathbf{u}_1$, $m_1^2 < 3d_1^2$, $d_1^2 < 3m_1^2$, *i* $(\mathbf{u}_1, \mathbf{v}_1)$ *és una base rombal òptima.*

OBSERVACIÓ. La condició $a^2 - 1 \equiv 0 \pmod{m}$ de setí simètric es pot escriure $(a+1)(a-1) \equiv 0 \pmod{m}$. A partir de $d_1 = \mathrm{mcd}(m, a+1)$ hem definit $\mathbf{d}_1$, $\mathbf{m}_1$, $\mathbf{w}_1$, $\mathbf{u}_1$ i $\mathbf{v}_1$. Però, prenent $d_2 = \mathrm{mcd}(m, a-1)$, es pot refer tota la discussió per obtenir resultats similars amb $m_2 = m/d_2$, $\mathbf{m}_2 = (m_2, m_2)$, $\mathbf{w}_2 = (-d_2/2, d_2/2)$, $x_2 = (d_2 + m_2)/2$, $\mathbf{u}_2 = (x_2, m_2 - x_2)$ i $\mathbf{v}_2 = (m_2 - x_2, x_2)$.

Mòduls i escalonats de setins simètrics

Com en el cas dels setins quadrats, trobar les parelles (m,a) tals que $L(m,a)$ sigui simètric ha estat un focus d'interès. En termes de teoria de nombres, es tracta de trobar les parelles (m,a) tals que el residu quadràtic de a mòdul m sigui 1. Naturalment, $(m,1)$ i $(m,-1)$, que corresponen a les sarges, són solució. L'interès és saber si n'hi ha d'altres.

La discussió segueix el mateix patró que en el cas dels setins quadrats: estudiant primer el cas de mòdul potència de primer i després via el teorema xinès dels residus, s'obté el cas general. Enunciem els resultats directament en termes de setins.

Per a mòduls 2, 3 i 4, només les sarges són setins simètrics. Considerarem, doncs, $m \geq 5$. Per a potències de primer, tenim:

PROPOSICIÓ 17. *Siguin p un nombre primer, $k \geq 1$ un enter i $m = p^k$.*

(i) *Si $p > 2$, els únics setins simètrics de mòdul m són les sarges.*

(ii) *Si $p = 2$ i $k \geq 3$, aleshores hi ha quatre setins simètrics de mòdul m, que són les dues sarges i els d'escalonat $2^{k-1} - 1$ i $2^{k-1} + 1$.*

Si es disposa de la factorització de m en producte de primers, les solucions per a cada potència de primer es combinen via el teorema xinès dels residus per obtenir la solució per a m. El nombre de solucions depèn només del nombre de factors primers diferents de 2 i de l'exponent del 2 a la factorització.

TEOREMA 18. *Siguin* $2 < p_1 < \cdots < p_r$ *nombres primers,* $\alpha_0 \geq 0$ *i* $\alpha_1, \ldots, \alpha_r$ *enters positius. Si* $m = 2^{\alpha_0} p_1^{\alpha_1} \cdots p_r^{\alpha_r}$*, el nombre de setins simètrics de mòdul* m *és*

(i) 2^{α_0} *si* $\alpha_0 \in \{0, 1\}$*;*

(ii) 2^{r+1} *si* $\alpha_0 = 2$*;*

(iii) 2^{r+2} *si* $\alpha_0 \geq 3$*.*

6 Setins concordants

Entre 1906 i 1907, el badaloní Pau Rodón, que aleshores era el director de *Cataluña Textil*, una revista de gran difusió en el món tèxtil espanyol i sud-americà, publicà una sèrie de set articles [29, 30, 31, 32, 33, 34, 35] amb el títol genèric «Estudio científico de los rasos regulares». Els «rasos regulares» són els setins. Des del punt de vista matemàtic, els articles no resisteixen l'anàlisi més benevolent. Definicions de vegades massa particulars i restrictives, regles que inicialment s'anuncien com a necessàries i suficients, però que al final s'expliciten com una condició suficient i, fins i tot, alguna regla errònia, com la dels setins quadrats. A més, totes les regles estan basades simplement en uns quants exemples particulars, amb nombres concrets, que després generalitza sense més contemplacions. Però, tot i això, des del punt de vista històric, els articles són interessants perquè presenten els tipus de setins que es consideraven més rellevants. S'hi tracten els setins quadrats, els simètrics i els simètrics rombals i rectangulars, que són els que hem comentat fins aquí. Com que també s'hi tracten els setins concordants, en donarem ara una notícia breu.

La idea intuïtiva d'un setí concordant directe (resp. indirecte) és que té tots els prens situats en rectes de pendent 1 (resp. de pendent -1). Formalment, un setí $L(m, a)$ és *concordant directe* (resp. *concordant indirecte*) si existeix un enter p amb $0 < p < m$ tal que, per a tot pren (x, y), el punt $(x + p, y + p)$ (resp. $(x - p, y + p)$) també és un pren. Notem que aquesta condició és equivalent al fet que $(p, p) \in L(m, a)$ (resp. $(-p, p) \in L(m, a)$). En tots dos casos, el menor p amb la propietat corresponent es diu el *pas*. La figura 15 mostra quatre cursos de setins. El primer, $L(9, 4)$, és concordant directe de pas 3, però no concordant indirecte; el segon, $L(9, 2)$, no és concordant directe, però és concordant indirecte de pas 3; el tercer, $L(8, 3)$, és alhora concordant directe de pas 4 i concordant indirecte de pas 2; finalment, $L(7, 3)$ no és concordant ni directe ni indirecte.

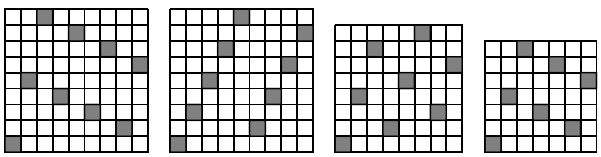


FIGURA 15

La caracterització dels setins concordants en termes del mòdul i l'escalonat és senzilla i és la següent.

PROPOSICIÓ 19. *Siguin $L(m,a)$ un setí, $d_1 = \mathrm{mcd}(m, a+1)$ i $d_2 = \mathrm{mcd}(m, a-1)$. Llavors:*

(i) *El setí $L(m,a)$ és concordant directe si i només si $d_2 > 1$; en aquest cas, el seu pas és m/d_2.*

(ii) *El setí $L(m,a)$ és concordant indirecte si i només si $d_1 > 1$; en aquest cas, el seu pas és m/d_1.*

PROVA. (i) Suposem que $L(m,a)$ és concordant directe de pas p. Llavors $ap \equiv p \pmod m$, d'on $p(a-1) \equiv 0 \pmod m$. Si $d_2 = \mathrm{mcd}(m, a-1) = 1$, tindríem $p \equiv 0 \pmod m$, la qual cosa és contradictòria perquè $1 \le p \le m-1$. Per tant, $d_2 > 1$. Llavors, $p(a-1)/d_2 \equiv 0 \pmod{m/d_2}$ i, com que $\mathrm{mcd}((a-1)/d_2, m/d_2) = 1$, resulta $p \equiv 0 \pmod{m/d_2}$, és a dir, $p = m/d_2$.

Recíprocament, suposem $d_2 = \mathrm{mcd}(m, a-1) > 1$. Si $a - 1 = d_2 k$, tenim $(a-1)(m/d_2) = d_2 k(m/d_2) = km \equiv 0 \pmod m$, la qual cosa implica que $(m/d_2, m/d_2) \in L(m,a)$ i que $L(m,a)$ és concordant.

Anàlogament es demostra (ii). □

A conseqüència de la proposició anterior, veiem que, si m és un nombre primer, no hi ha setins concordants ni directes ni indirectes de mòdul m.

Veurem ara que, en un setí $L(m,a)$ concordant directe de pas p, el vector $\mathbf{p} = (p,p)$ sempre forma part d'una base.

PROPOSICIÓ 20. *Sigui $L(m,a)$ un setí concordant directe de pas p, i siguin $d_2 = \mathrm{mcd}(m, a-1)$ i x i y enters tals que $xm + y(a-1) = d_2$. Aleshores els vectors $\mathbf{p} = (p,p)$ i $\mathbf{u} = x(0,m) + y(1,a)$ formen una base de $L(m,a)$.*

PROVA. És clar que $\mathbf{u} \in L(m,a)$. Com que $L(m,a)$ és concordant directe, el pas és $p = m/d_2$ i $\mathbf{p} = (p,p) \in L(m,a)$. Només cal veure que $|\det(\mathbf{p},\mathbf{u})| = m$. Tenim

$$\begin{aligned} |\det(\mathbf{p},\mathbf{u})| &= |\det(\mathbf{p}, x(0,m) + y(1,a))| = \\ &= |x\det(\mathbf{p},(0,m)) + y\det(\mathbf{p},(1,a))| = \\ &= |xpm + y(pa-p)| = |p(xm + y(a-1))| = pd_2 = m. \end{aligned}$$ □

Així, amb la notació de la proposició anterior, cada parella (x,y) de coeficients de la identitat de Bézout $xm + y(a-1) = d_2$ proporciona un vector que forma base amb $\mathbf{p} = (p,p)$. Per exemple, per a $L(9,4)$, tenim $d_2 = \mathrm{mcd}(9,3) = 3$. Si prenem $x = 1$, $y = -2$, resulta $\mathbf{u} = (0,9) - 2(1,4) = (-2,1)$, amb la qual cosa tenim la base $(\mathbf{p},\mathbf{u}) = ((3,3),(-2,1))$. Si prenem $x = 0$ i $y = 1$, llavors $\mathbf{u} = (1,4)$ i obtenim la base $(\mathbf{p},\mathbf{u}) = ((3,3),(1,4))$. Notem que una base òptima de $L(9,4)$ és $((-2,1),(1,4))$. Per posar un tercer cas, per a $x = 3$ i $y = -8$, resulta $\mathbf{u} = (-8,-5)$ i la base $(\mathbf{p},\mathbf{u}) = ((3,3),(-8,-5))$.

La discussió és anàloga per als setins concordants indirectes. Només enunciem la proposició corresponent.

PROPOSICIÓ 21. *Sigui $L(m,a)$ un setí concordant indirecte de pas p, i siguin $d_1 = \mathrm{mcd}(m,a+1)$ i x i y enters tals que $xm + y(a+1) = d_1$. Aleshores els vectors $\mathbf{p} = (p,-p)$ i $\mathbf{u} = x(0,m) + y(1,a)$ formen una base de $L(m,a)$.*

Un setí és *concordant* si és concordant directe i indirecte alhora. Per als setins simètrics tenim la proposició següent.

PROPOSICIÓ 22. *Tot setí simètric de mòdul $m > 2$ és concordant.*

PROVA. Sigui $L(m,a)$ un setí simètric, $d_1 = \mathrm{mcd}(m,a+1)$ i $m_1 = m/d_1$. D'acord amb el que hem comentat a la pàgina 51, els vectors $\mathbf{d}_1 = (d_1,d_1)$ i $\mathbf{m}_1 = (-m_1,m_1)$ són tots dos de $L(m,a)$. Suposant que no es tracti de la plana, aleshores $d_1 > 2$ i $m_1 > 2$, amb la qual cosa $L(m,a)$ és concordant directe i concordant indirecte alhora. □

Considerem ara setins quadrats. Atès que un setí quadrat és invariant per girs d'angle $\pi/2$ centrats a l'origen, un setí quadrat o bé és alhora concordant directe i indirecte, com $L(10,3)$, o no és cap de les dues coses, com $L(13,5)$.

PROPOSICIÓ 23. *Un setí quadrat $L(m,a)$ és concordant si i només si m és parell.*

PROVA. La condició $a^2 \equiv -1 \pmod{m}$ de setí quadrat implica que m i a tenen diferent paritat i que m i $a-1$ tenen la mateixa paritat.

Si m és parell, llavors m i $a-1$ són tots dos parells i $d_2 = \mathrm{mcd}(m,a-1) > 1$. Així, $L(m,a)$ és concordant.

Suposem que m és senar i que el setí $L(m,a)$ és concordant, és a dir, que $d_2 = \mathrm{mcd}(m,a-1) > 1$. Com que m i $a-1$ són senars, $d_2 \geq 3$. Llavors, $\mathbf{p} = (m/d_2, m/d_2) \in L(m,a)$. Tenim (amb totes les congruències mòdul m) $a(m/d_2) \equiv m/d_2$ i, multiplicant per a, obtenim $-m/d_2 \equiv a(m/d_2) \equiv m/d_2$. Per tant, $2m/d_2 \equiv 0$. Com que $d_2 \geq 3$, resulta una contradicció. Per tant, si m és senar, $L(m,a)$ no és concordant. □

7 Setins equivalents

En els textos clàssics, la definició de setí no sempre es correspon amb la que hem donat aquí. Per exemple, P. Rodón [29] el defineix mitjançant dos enters a i b amb $\mathrm{mcd}(a,b) = 1$. Si $a < b$, anomena *a escalonat directe* i *b escalonat indirecte o complementari*. El que aquí hem anomenat *mòdul*, per a ell és $m = a + b$. Com que $\mathrm{mcd}(a,m) = \mathrm{mcd}(a,a+b) = \mathrm{mcd}(a,b)$, les condicions $\mathrm{mcd}(a,b) = 1$ i $\mathrm{mcd}(m,a) = 1$ són equivalents. Veiem, doncs, que, per a Rodón, els setins complementaris $L(m,a)$ i $L(m,m-a)$ són el mateix setí. En la terminologia que introduirem a continuació, es tractarà de setins equivalents, que definirem en termes geomètrics i en veurem l'equivalent aritmètic.

Una *equivalència* d'un setí $L(m_1, a)$ en un setí $L(m_2, b)$ és un moviment f del pla tal que

$$\mathbf{x} \in L(m_1, a) \Leftrightarrow f(\mathbf{x}) \in L(m_2, b),$$

és a dir, és un moviment del pla que conserva els prens. Si existeix una tal equivalència, posarem $L(m_1, a) \simeq L(m_2, b)$ i direm que els dos setins són *equivalents*. És clar que la relació $\simeq$ és d'equivalència.

Si f és una equivalència d'un setí $L(m_1, a)$ en un setí $L(m_2, b)$ i $\mathbf{z} \in \mathbb{Z}^2$, aleshores $\mathbf{z}$ és la intersecció de dues rectes paral·leles als eixos que contenen prens de $L(m_1, a)$; per tant, $f(\mathbf{z})$ també és la intersecció de dues rectes perpendiculars que contenen prens de $L(m_2, b)$ i tenim que $f(\mathbf{z}) \in \mathbb{Z}^2$. Una equivalència, doncs, conserva la graella de coordenades enteres.

Els moviments del pla són les translacions, els girs, les simetries axials i les simetries lliscants (una simetria lliscant és una simetria axial seguida d'una translació definida per un vector director de la recta eix de la simetria axial). No és gaire difícil caracteritzar els moviments f del pla tals que $f(\mathbb{Z}^2) = \mathbb{Z}^2$. Enunciem el resultat a continuació. Per flexibilitzar el llenguatge, anomenarem *recta vertical* una recta de vector director $(0, 1)$, *recta horitzontal* una recta de vector director $(1, 0)$, i *recta diagonal* una recta de vector director $(1, 1)$ o $(1, -1)$. També anomenarem *punt enter* un punt amb les dues coordenades enteres i, anàlogament, *vector enter* un vector amb les dues components enteres.

PROPOSICIÓ 24. *Sigui f un moviment del pla tal que $f(\mathbb{Z}^2) = \mathbb{Z}^2$. Aleshores f és un moviment d'un dels tipus següents:*

(i) *Una translació segons un vector enter.*

(ii) *Un gir d'angle múltiple enter de $\pi/2$ i de centre $\mathbf{z}$ o $\mathbf{z} + (1/2, 1/2)$ per a un punt enter $\mathbf{z}$.*

(iii) *Una simetria axial respecte a una recta horitzontal o vertical tal que, per a un punt enter $\mathbf{z}$, la recta passa pel punt $\mathbf{z}$ o pel punt $\mathbf{z} + (1/2, 1/2)$.*

(iv) *Una simetria axial respecte a una recta diagonal que passa per un punt $\mathbf{z}$ enter.*

(v) *Una simetria lliscant composició d'una simetria axial com les de (iii) o (iv) i d'una translació segons un vector enter en la direcció de la recta de la simetria.*

Amb l'ajuda d'aquesta proposició es poden caracteritzar els setins equivalents en termes del mòdul i l'escalonat. Veurem que els setins equivalents a $L(m, a)$ són el seu complementari, el seu associat i el complementari del seu associat.

TEOREMA 25. *Dos setins $L(m_1, a)$ i $L(m_2, b)$ són equivalents si i només si $m_1 = m_2$ i $b \in \{a, m - a, a', m - a'\}$.*

ESQUEMA DE LA PROVA. Si f és una equivalència de $L(m_1, a)$ en $L(m_2, b)$ i $(\mathbf{u}, \mathbf{v})$ és una base de $L(m_1, a)$, i F és l'aplicació ortogonal associada al moviment f, aleshores $(F(\mathbf{u}), F(\mathbf{v}))$ és una base de $L(m_2, b)$, així que

$$m_2 = |\det(F(\mathbf{u}), F(\mathbf{v}))| = |\det(\mathbf{u}, \mathbf{v})| = m_1,$$

i veiem que setins equivalents tenen el mateix mòdul. En el que segueix, $m = m_1 = m_2$ i totes les congruències ho són mòdul m. Només ens cal demostrar, doncs, que $L(m, a) \simeq L(m, b)$ si i només si $b \in \{a, m-a, a', m-a'\}$.

Suposem que $b \in \{a, m-a, a', m-a'\}$. En els quatre casos, es pot demostrar fàcilment que l'aplicació f que donem és una equivalència de $L(m, a)$ a $L(m, b)$. Si $b = a$, la identitat és l'equivalència cercada. Si $b = m - a$, definim f per $f((x, y)) = (-x, y)$, que és la simetria respecte de l'eix d'ordenades. Llavors

$$(x, y) \in L(m, a) \Leftrightarrow ax \equiv y \Leftrightarrow (m-a)(-x) \equiv y \Leftrightarrow (-x, y) \in L(m, m-a),$$

i veiem que f és una equivalència. Anàlogament, si $b = a'$, definim f per $f((x, y)) = (y, x)$, que és la simetria respecte a la recta diagonal de pendent 1, i si $b = m - a'$, definim f per $f((x, y)) = (-y, x)$, que és el gir de centre l'origen i angle $\pi/2$. Es comprova fàcilment que es tracta d'equivalències.

Recíprocament, sigui f una equivalència de $L(m, a)$ en $L(m, b)$. Indicarem (sense donar detalls) quin és el valor de b en funció de a dependent del tipus de moviment.

Si f és una translació de vector $\mathbf{u} = (u_1, u_2)$, aleshores $\mathbf{u}$ és un vector enter, $au_1 \equiv u_2 \pmod{m}$ i $b = a$.

Si f és un gir de centre $\mathbf{c}$ i angle α que és diferent de la identitat, d'acord amb la proposició 24 podem suposar que l'angle α compleix $\alpha \in \{\pi/2, \pi, 3\pi/2\}$. Llavors, si $\alpha = \pi/2$, aleshores $b = m - a'$; si $\alpha = \pi$, aleshores $b = a$; si $\alpha = 3\pi/2$, aleshores $b = m - a'$.

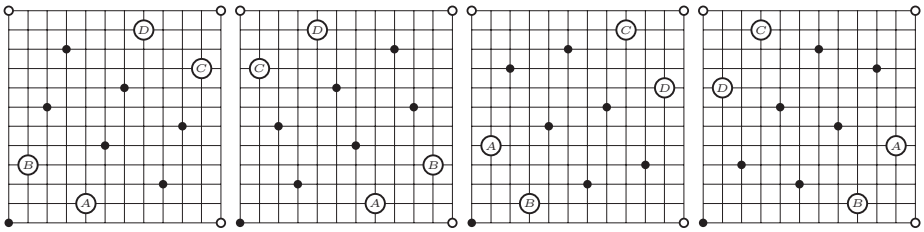
Si f és una simetria axial respecte a una recta ℓ, llavors, si ℓ és vertical o horitzontal, aleshores $b = m - a$; si ℓ és diagonal, aleshores $b = a'$.

Finalment, considerem el cas que f és una simetria lliscant $f = t \circ s$, on s és una simetria axial i t una translació en la direcció de l'eix de la simetria s. Es pot demostrar que necessàriament també s i t són equivalències. Llavors, com en el cas de la simetria axial, $b \in \{m - a, a'\}$. □

En definitiva, la classe dels setins equivalents a un setí donat està formada per ell mateix, el seu complementari, el seu associat i el complementari d'aquest associat. La classe d'equivalència de la plana té cardinal 1. Si el mòdul és $m > 2$, la classe d'equivalència d'un setí simètric té cardinal 2 perquè $a = a'$; la d'un setí quadrat també té cardinal 2 perquè $a = m - a'$; en tots els altres casos, la classe d'equivalència té cardinal 4.

EXEMPLE. El tercer quadrat de la figura 16 és la part del reticle $L(m, a) = L(11, 4)$ que correspon als punts de coordenades compreses entre 0 i 11 i hi hem marcat amb les lletres A, B, C i D els quatre prens que tenen alguna coordenada 1 o 10. Els altres tres quadrats són les mateixes parts dels reticles $L(m, m-a) = L(11, 7)$, $L(m, m-a') = L(11, 8)$ i $L(m, a') = L(11, 3)$,

i en els tres hem marcat els prens que es corresponen amb els marcats del tercer per fer més evident les simetries. És clar que $L(m, m-a') = L(11,8)$ s'obté per un gir d'angle recte de $L(m,a) = L(11,4)$, que $L(m,a') = L(11,3)$ i $L(m, m-a') = L(11,8)$ són simètrics respecte a un costat vertical del quadrat, i el mateix passa amb $L(m,a) = L(11,4)$ i $L(m, m-a) = L(11,7)$.



$L(m,a') = L(11,3)$ $L(m, m-a') = L(11,8)$ $L(m,a) = L(11,4)$ $L(m, m-a) = L(11,7)$

FIGURA 16

8 Setins isonemals

Les equivalències d'un setí $L = L(m,a)$ en ell mateix es diuen *simetries* del setí, i formen un grup $S(L)$.

Un fil de l'ordit d'un lligat s'identifica amb un conjunt $\mathcal{O}_x = \{x\} \times \mathbb{R}$ amb x enter, i un fil de la trama, amb un conjunt $\mathcal{T}_y = \mathbb{R} \times \{y\}$ amb y enter. Un fil del lligat és un dels fils $\mathcal{O}_x$ o $\mathcal{T}_y$; denotarem amb $\mathcal{F}$ el conjunt de fils.

Un setí $L = L(m,a)$ es diu *isonemal* si el grup $S(L)$ de les seves simetries és transitiu sobre els fils, és a dir, si, donats dos fils $F_1, F_2 \in \mathcal{F}$, existeix una simetria $f \in S(L)$ tal que $f(F_1) = F_2$. El concepte de lligat isonemal s'estén a lligats generals, inclosos els que no són generats necessàriament per un curs de lligat quadrat, però la definició és lleugerament diferent perquè en el cas general s'admet una simetria consistent a intercanviar prens i deixes. Els teixits isonemals han estat estudiats per B. Grünbaum i G. C. Shephard; vegeu [16, 17, 18].

Probablement, a part del seu interès estètic, l'interès pràctic dels teixits isonemals prové del fet que, si en un nombre fixat i gran de passades un fil de l'ordit té molts més prens aïllats que un altre fil de l'ordit, el primer acabarà essent sotmès a una tensió més gran que el segon, amb perill de trencament. Per tant, un teixit isonemal té l'avantatge de ser un teixit en què tots els fils de l'ordit són sotmesos a la mateixa tensió durant tot el procés de tissatge.

Bona part de l'interès en els setins simètrics i quadrats és que són els únics setins isonemals. En aquest apartat proporcionem un esquema de la prova, que comença amb el lema següent de prova fàcil que ometem.

LEMA 26. *Sigui L un setí i F_1, F_2 dos fils de L, tots dos de l'ordit o tots dos de la trama. Si $\mathbf{p}_1$ és un pren de F_1 i $\mathbf{p}_2$ és un pren de F_2, aleshores la translació t de vector $\mathbf{u} = \mathbf{p}_2 - \mathbf{p}_1$ és una simetria de L tal que $t(F_1) = F_2$.*

TEOREMA 27. *Un setí $L(m,a)$ és isonemal si i només si és simètric o quadrat.*

PROVA. Suposem que el setí $L(m,a)$ és simètric o quadrat, i siguin F_1 i F_2 dos fils. Si tots dos fils són de l'ordit o tots dos de la trama, el lema 26 garanteix que existeix una simetria que transforma l'un en l'altre. Suposem, doncs, que $F_1 = \mathcal{T}_{y_1}$ i $F_2 = \mathcal{O}_{x_2}$. Siguin $\mathbf{p}_1 = (x_1, y_1) \in L(m,a)$ i $\mathbf{p}_2 = (x_2, y_2) \in L(m,a)$ prens dels fils $\mathcal{T}_{y_1}$ i $\mathcal{O}_{x_2}$, respectivament. La translació t de vector $\mathbf{u} = \mathbf{p}_2 - \mathbf{p}_1$ aplica $\mathcal{T}_{y_1}$ en $\mathcal{T}_{y_2}$ conservant els prens.

Suposem que $L(m,a)$ és simètric. Si s és la simetria axial respecte a la recta diagonal de pendent 1 que passa per $\mathbf{p}_2$, aleshores s deixa invariant el pren $\mathbf{p}_2$ i aplica $\mathcal{T}_{y_2}$ en $\mathcal{O}_{x_2}$ conservant els prens. Aleshores $f = s \circ t$ és una simetria de $L(m,a)$ tal que $f(\mathcal{T}_{y_1}) = \mathcal{O}_{x_2}$.

Si $L(m,a)$ és quadrat, considerem el gir g d'angle recte de centre $\mathbf{p}_2$. Aquest gir també deixa invariant el pren $\mathbf{p}_2$ i aplica $\mathcal{T}_{y_2}$ en $\mathcal{O}_{x_2}$ conservant els prens. Per tant, $f = g \circ t$ és una simetria de $L(m,a)$ tal que $f(\mathcal{T}_{y_1}) = \mathcal{O}_{x_2}$.

En tots dos casos, doncs, existeix una simetria f de L tal que $f(\mathcal{T}_{y_1}) = \mathcal{O}_{x_2}$ i, evidentment, la simetria f^{-1} transforma $\mathcal{O}_{x_2}$ en $\mathcal{T}_{y_1}$. Donats dos fils, doncs, hi ha una simetria que transforma l'un en l'altre.

Recíprocament, suposem que un setí $L(m,a)$ és isonemal. Considerem els dos fils concrets $\mathcal{O}_0$ i $\mathcal{T}_0$, és a dir, els dos eixos de coordenades. Com que el setí és isonemal, existeix una simetria f del setí tal que transforma l'un en l'altre. La simetria f és, en aquest cas, un moviment del pla que transforma un eix de coordenades en l'altre i deixa fix l'origen. Per tant, f és una simetria axial respecte a una recta que passa per l'origen i de pendent 1 o -1, o bé f és un gir de centre l'origen i d'angle $\pi/2$ o $3\pi/2$. D'acord amb les definicions de les pàgines 44 i 49, en el primer cas es tracta d'un setí simètric i en el segon d'un setí quadrat. □

9 Setins de Fibonacci

La successió de Fibonacci $\mathcal{F} = (f_i : i \geq 0)$ es defineix pels valors inicials $f_0 = 0$, $f_1 = 1$ i per la recurrència $f_i = f_{i-1} + f_{i-2}$ per a $i \geq 2$. Els nombres de la successió $\mathcal{F}$ s'anomenen *nombres de Fibonacci* i és ben sabut que admeten l'expressió explícita següent: si $\phi = (1+\sqrt{5})/2$ i $\psi = (1-\sqrt{5})/2$, aleshores $f_i = (\phi^i - \psi^i)/\sqrt{5}$ per a tot $i \geq 0$.

Llevat el cas $f_1 = f_2 = 1$, cada nombre de Fibonacci és estrictament major que l'anterior. La fórmula recurrent $f_{i+1} = f_i + f_{i-1}$ indica que, per a $i \geq 2$, la divisió de f_{i+1} per f_i té quocient 1 i residu f_{i-1} i que $f_{i-1} < f_{i+1}/2$. També, per a $i \geq 4$,

$$f_{i+1} = f_i + f_{i-1} = (f_{i-1} + f_{i-2}) + f_{i-1} = 2f_{i-1} + f_{i-2}$$

indica que la divisió de f_{i+1} per f_{i-1} té quocient 2 i residu f_{i-2}.

Entre la inacabable llista de propietats dels nombres de Fibonacci, n'esmentem dues que ens faran servei. Les demostracions es poden trobar a molts llocs, per exemple a l'enciclopèdica obra de T. Koshy [21, volum 1, teorema 5.3 i teorema 10.3], dedicat als nombres de Fibonacci i de Lucas.

PROPOSICIÓ 28. *Els nombres de Fibonacci compleixen les propietats següents.*

(i) (Identitat de Cassini) *Per a tot enter* $i \geq 1$ *es compleix* $f_{i-1}f_{i+1} - f_i^2 = (-1)^i$.

(ii) *Per a qualssevol enters* $j \geq i \geq 1$, *si* $d = \mathrm{mcd}(j, i)$, *llavors* $\mathrm{mcd}(f_j, f_i) = f_d$.

Com que $\mathrm{mcd}(i+1, i) = 1$, l'apartat (ii) implica $\mathrm{mcd}(f_{i+1}, f_i) = f_1 = 1$. Com que $\mathrm{mcd}(i+1, i-1) = \mathrm{mcd}(i+1, 2) \in \{1, 2\}$ i $f_1 = f_2 = 1$, resulta $\mathrm{mcd}(f_{i+1}, f_{i-1}) = 1$. Així, si $i \geq 2$, aleshores $L(f_{i+1}, f_i)$ i $L(f_{i+1}, f_{i-1})$ són setins i, atès que la suma dels dos escalonats $f_i + f_{i-1}$ és el mòdul f_{i+1}, es tracta de setins complementaris; però només $L(f_{i+1}, f_{i-1})$ compleix que l'escalonat sigui menor que la meitat del mòdul.

D'entre totes les parelles d'enters $m > a > 0$ tals que l'algorisme d'Euclides per trobar $\mathrm{mcd}(m, a)$ requereix n divisions, els valors més petits de m i a són $m = f_{n+2}$ i $a = f_{n+1}$ (vegeu D. E. Knuth [20, apartat 4.5.3, teorema F]). Aquest fet va portar a pensar que els nombres de Fibonacci donarien exemples interessants d'aplicació de l'algorisme d'Euclides estès a trobar bases de setins. Per a $i \geq 5$, definim, doncs, l'i-èsim *setí de Fibonacci* $F(i)$ com el setí $F(i) = L(f_{i+1}, f_{i-1})$. Veurem que els setins de Fibonacci són simètrics o quadrats i que l'algorisme d'Euclides sempre en proporciona una base òptima les coordenades de la qual són, llevat del signe, també nombres de Fibonacci. En farem les demostracions perquè no són llargues i perquè no han estat publicades.

Coneguts els quocients de les divisions f_{i+1} per f_i i per f_{i-1} que hem esmentat més amunt, l'aplicació de l'algorisme d'Euclides per trobar els vectors d'Euclides de $F(i) = L(f_{i+1}, f_{i-1})$ dona el resultat següent, fàcilment demostrable per inducció.

PROPOSICIÓ 29. *Siguin* $i \geq 4$ *i* $\mathbf{e}_\alpha$, *amb* $\alpha \in \{0, \ldots, n+1\}$, *els vectors d'Euclides de* $F(i)$. *Aleshores* $n + 1 = i - 1$ *i els vectors* $\mathbf{e}_\alpha$ *són:*

$$\begin{aligned}
&\mathbf{e}_0 = (f_0, f_{i+1}),\\
&\mathbf{e}_\alpha = ((-1)^{\alpha+1} f_{\alpha+1}, f_{i-\alpha}) \text{ per a tot } \alpha \in \{1, \ldots, i-2\},\\
&\mathbf{e}_{i-1} = ((-1)^i f_{i+1}, f_0).
\end{aligned}$$

Amb això, podem veure que $F(i)$ és quadrat o simètric segons que i sigui parell o senar, i podem explicitar-ne una base òptima. Per a i parell, tenim:

TEOREMA 30. *Si* i *és parell, el setí de Fibonacci* $F(i)$ *és quadrat i, si definim* $k = i/2$, *aleshores una base òptima de* $F(i)$ *és* $(((-1)^k f_k, f_{k+1}), ((-1)^{k+1} f_{k+1},\ f_k))$.

PROVA. Per la identitat de Cassini $f_i^2 \equiv -1 \pmod{f_{i+1}}$. De $f_{i-1} + f_i = f_{i+1}$, obtenim $f_{i-1} \equiv -f_i \pmod{f_{i+1}}$ i $f_{i-1}^2 \equiv f_i^2 \equiv -1 \pmod{f_{i+1}}$. Per tant, $F(i)$ és un setí quadrat.

Com que $L(f_{i+1}, f_{i-1})$ té $n + 1 = i - 1$ vectors d'Euclides, tenim $n = i - 2$ i, pel teorema 6, si $k = (n+2)/2 = i/2$, una base òptima de $F(i)$ és $(\mathbf{e}_{k-1}, \mathbf{e}_k)$. Per aplicació de la proposició 29,

$$\mathbf{e}_{k-1} = ((-1)^{k-1} f_k, f_{k+1}), \quad \mathbf{e}_k = ((-1)^k f_{k+1}, f_k),$$

com volíem demostrar. □

Per a i senar, tenim:

TEOREMA 31. *Si i és senar, el setí $F(i)$ és simètric i, si definim $j = (i-1)/2$, aleshores una base òptima de $F(i)$ és* $(((-1)^{j+1}f_{j+1}, f_{j+1}),\ ((-1)^j f_j, f_{j+2}))$.

PROVA. Per la identitat de Cassini, $f_i^2 \equiv 1 \pmod{f_{i+1}}$. De $f_{i-1} + f_i = f_{i+1}$, obtenim $f_{i-1} \equiv -f_i \pmod{f_{i+1}}$ i $f_{i-1}^2 \equiv f_i^2 \equiv 1 \pmod{f_{i+1}}$. Per tant, $F(i)$ és simètric.

En aquest cas, l'índex central de l'algorisme d'Euclides és $j = (i-1)/2$, i $|v_j| = r_j = f_{i-j} = f_{j+1}$. A més, $k = \min\{\alpha : |v_\alpha| > r_\alpha\} = j+1$. El vector més curt de $F(i)$ és un dels quatre $\mathbf{e}_{j-1}$, $\mathbf{e}_j$, $\mathbf{e}_{j+1}$ i $\mathbf{e}_{j+2}$. Ara, $\|\mathbf{e}_{j+2}\| = \|\mathbf{e}_{j-2}\|$, però $\mathbf{e}_{j-2}$ no és el vector més curt. Com que $\|\mathbf{e}_{j+1}\| = \|\mathbf{e}_{j-1}\|$, el vector més curt és $\mathbf{e}_{j-1}$ o $\mathbf{e}_j$. Tenim,

$$\begin{aligned}
\|\mathbf{e}_j\| < \|\mathbf{e}_{j-1}\| &\Leftrightarrow f_{j+1}^2 + f_{j+1}^2 < f_j^2 + f_{j+2}^2 \\
&\Leftrightarrow f_{j+1}^2 - f_j^2 < f_{j+2}^2 - f_{j+1}^2 \\
&\Leftrightarrow (f_{j+1} + f_j)(f_{j+1} - f_j) < (f_{j+2} + f_{j+1})(f_{j+2} - f_{j+1}) \\
&\Leftrightarrow (f_{j+1} + f_j) f_{j-1} < (f_{j+2} + f_{j+1}) f_j.
\end{aligned}$$

Aquesta última desigualtat és òbvia, així que $\mathbf{e}_j$ és el vector més curt.

Apliquem l'algorisme de Lagrange-Gauss a la base $(\mathbf{e}_j, \mathbf{e}_{j-1})$. Tenim,

$$\mathbf{e}_j \cdot \mathbf{e}_{j-1} = -f_{j+1}f_j + f_{j+1}^2 = f_{j+1}(f_{j+1} - f_j) = f_{j+1}f_{j-1} = f_j^2 + (-1)^j.$$

Llavors,

$$\mu = \frac{\mathbf{e}_j \cdot \mathbf{e}_{j-1}}{\|\mathbf{e}_j\|^2} = \frac{f_j^2 + (-1)^j}{2f_{j+1}^2}.$$

És clar que $0 < \mu < 1/2$ i, en conseqüència, $h = \lfloor \mu \rceil = 0$. Per tant, $(\mathbf{e}_j, \mathbf{e}_{j-1})$ és una base òptima. Per la proposició 29,

$$\mathbf{e}_j = ((-1)^{j+1}f_{j+1}, f_{j+1}), \quad \mathbf{e}_{j-1} = ((-1)^j f_j, f_{j+2}),$$

com volíem demostrar. □

Acabem aquest últim apartat amb una qüestió natural. Considerem un setí tal que el mòdul i l'escalat siguin nombres de Fibonacci: $L(f_j, f_i)$ amb $j \geq i+2$. Per tal que es tracti efectivament d'un setí, cal que $\mathrm{mcd}(f_j, f_i) = 1$. Atès que, si $d = \mathrm{mcd}(j, i)$, es compleix $\mathrm{mcd}(f_j, f_i) = f_d$ (proposició 28(ii)) i que $f_d = 1$ és equivalent a $d \in \{1, 2\}$, cal exigir $\mathrm{mcd}(j, i) \in \{1, 2\}$. Suposat això, és natural preguntar-se per a quins valors de i i j el setí $L(f_j, f_i)$ és simètric o quadrat, altrament dit, esbrinar els i i j tals que $f_i^2 \equiv 1 \pmod{f_j}$ o $f_i^2 \equiv -1 \pmod{f_j}$.

Donat un enter $m \geq 2$, la successió $\mathcal{F}(m) = (f_i \pmod m : i \geq 0)$ és periòdica perquè només hi ha m^2 parelles de residus i, per tant, en algun punt de la successió $\mathcal{F}(m)$ es repeteix una parella de termes consecutius, és a dir, per a cert enter p, es compleix $(f_i \pmod m, f_{i+1} \pmod m) =$

$(f_{i+p} \pmod m, f_{i+p+1} \pmod m)$. Com que dos termes consecutius de la successió determinen tota la successió, en resulta la periodicitat. El període de la successió $\mathcal{F}(m)$ ha estat objecte d'estudi (vegeu la pàgina web mantinguda per M. Renault [28] i totes les seves referències). Que la successió $\mathcal{F}(m)$ sigui periòdica implica que totes les successions $\mathcal{F}^e(m) = (f_i^e \pmod m : i \geq 0)$ amb $e \geq 0$ enter també ho són, en particular les successions $\mathcal{F}^e(f_j)$, de les quals es coneix el període i els valors dels termes que es repeteixen (vegeu [2]). Per detectar els setins simètrics i quadrats d'entre tots aquells que tenen mòdul i escalonat que són nombres de Fibonacci, interessa la successió dels quadrats, és a dir, el cas $e = 2$, de la qual detallem el resultat.

PROPOSICIÓ 32. *Sigui $j \geq 4$ un enter i, per a $i \geq 0$, sigui $\rho_i \equiv f_i^2 \pmod{f_j}$ amb $0 \leq \rho_i \leq f_j - 1$.*

(i) *Si $j = 2t$ és parell, aleshores $\mathcal{F}^2(f_j)$ té periodicitat j i els valors dels ρ_i per a $i \in \{0, \ldots, j-1\}$ són:*

(i.1) $\rho_i = f_i^2$ *si* $i \in \{0, \ldots, t\}$;

(i.2) $\rho_i = f_{j-i}^2$ *si* $i \in \{t+1, \ldots, j-1\}$.

(ii) *Si $j = 2t+1$ és senar, aleshores $\mathcal{F}^2(f_j)$ té periodicitat $2j$ i els valors dels ρ_i per a $i \in \{0, \ldots, 2j-1\}$ són:*

(ii.1) $\rho_i = f_i^2$ *si* $i \in \{0, \ldots, t+1\}$;

(ii.2) $\rho_i = f_j - f_{j-i}^2$ *si* $i \in \{t+2, \ldots, j-1\}$;

(ii.3) $\rho_i = 0$ *si* $i = j$;

(ii.4) $\rho_i = \rho_{2j-i}$ *si* $i \in \{j+1, \ldots, 2j-1\}$.

Per exemple, per a $j = 10$, tenim $f_{10} = 55$ i la seqüència $\mathcal{F}^2(55)$ consta de la repetició dels 10 valors

$$0, 1, 1, 4, 9, 25, 9, 4, 1, 1,$$

mentre que, per a $j = 11$, tenim $f_{11} = 89$ i $\mathcal{F}^2(89)$ consta de la repetició dels 22 valors,

$$0, 1, 1, 4, 9, 25, 64, 80, 85, 88, 88, 0, 88, 88, 85, 80, 64, 25, 9, 4, 1, 1.$$

La proposició 32 permet demostrar la unicitat dels setins de Fibonacci com els únics setins definits per nombres de Fibonacci que són simètrics o quadrats.

TEOREMA 33. *Siguin $j > i + 1 \geq 3$ enters amb $\operatorname{mcd}(i, j) = \{1, 2\}$ i considerem el setí $L = L(f_j, f_i)$.*

(i) *Si j és parell, aleshores L no és quadrat i L és simètric si i només si $i = j-2$.*

(ii) *Si j és senar, aleshores L no és simètric i L és quadrat si i només si $i = j-2$.*

PROVA. Com abans, definim els ρ_i per $\rho_i \equiv f_i^2$ i $0 \le \rho_i < f_j - 1$. La proposició 32 dona els seus valors.

(i) Si $j = 2t$ és parell, veiem que

$$1 < \rho_3 < \cdots < \rho_{t-1} < \rho_t,$$
$$\rho_t > \rho_{t+1} > \cdots > \rho_{j-3} > \rho_{j-2} = \rho_{j-1} = 1,$$

amb $\rho_t = f_t^2 < f_j - 1$. Si $3 \le i \le j-1$, tenim $\rho_i \ne f_j - 1$, és a dir que $f_i^2 \not\equiv -1 \pmod{f_j}$; i $\rho_i = 1$, o sigui, $f_i^2 \equiv 1 \pmod{f_j}$ si i només si $i = j-1$ o $i = j-2$. Llavors $L(f_j, f_i)$ no és quadrat i, com que $i < j-1$, és simètric si i només si $i = j-2$.

(ii) Si $j = 2t+1$ és senar, veiem que

$$1 < \rho_3 < \cdots < \rho_{t-1} < \rho_t < \rho_{t+1},$$
$$\rho_{t+1} > \rho_{t+2} > \cdots > \rho_{j-2} = \rho_{j-1} > \rho_j = 0.$$

Ara, $\rho_{t+1} = f_{t+1}^2 < f_j - 1$ i $\rho_{j-2} = \rho_{j-1} = f_j - 1$. Llavors, $\rho_i \ne 1$, o sigui $f_i^2 \not\equiv 1 \pmod{f_j}$ i $\rho_i = f_j - 1$, o sigui $f_i^2 \equiv -1 \pmod{f_j}$ si i només si $i = j-1$ o $i = j-2$. Així (f_j, f_i) no és simètric i, com que $i < j-1$, és quadrat si i només si $i = j-2$. □

En general, la base de qualsevol curs d'un lligat és el d'un setí. En els telers clàssics, les restriccions mecàniques no permeten teixir cursos de mòdul gaire elevat: cursos de mòdul 16 o 24 ja són considerables. Per al tissatge de cursos de mòduls més grans cal utilitzar telers amb tecnologia Jacquard. Els setins de Fibonacci, que creixen de mòdul ràpidament, poden proporcionar amb facilitat setins quadrats i simètrics de mòdul gran.

10 Cloenda

És cert que la tasca dels teòrics del tèxtil considera molts més aspectes que els tractats aquí. Per exemple, cal estudiar les fibres que permeten fer fils adequats, cal considerar la torsió, el gruix i el color dels fils, s'ha de veure com convé passar els fils pels lliços i moltes altres qüestions rellevants. Però sembla clar que el curs fonamental dels lligats de setí són a la base de la teoria de teixits. La modelització que hem exposat d'aquests lligats emprant eines aritmètiques i geomètriques ajuda a la seva millor comprensió i dona eines per trobar, estudiar i classificar els setins, per saber-ne els límits i les potencialitats, en particular dels setins quadrats i dels simètrics. Potser això permetrà obrir camins cap a noves maneres de trobar nous cursos de lligat, ja siguin fonamentals i/o derivats.

Agraïments

Volem agrair a Manuel Udina els seus comentaris, que han millorat el text; a Joan Carles Lario, els seus suggeriments sobre els setins de Fibonacci; finalment, a la Casa Navàs, de Reus, el fet d'haver-nos permès utilitzar la imatge d'un detall dels seus enrajolats.

Referències

[1] Brunat, J. M.; Lario, J.-C. «Satins, lattices, and extended Euclid's algorithm». *Jpn. J. Ind. Appl. Math.*, 39 (1) (2022), 75–96.

[2] Brunat, J. M.; Lario, J.-C. «Periodicity of power Fibonacci sequences modulus a Fibonacci number». Preprint (2022). [Disponible en línia a arXiv:2204.00234]

[3] Burton, D. M. *Elementary Number Theory*. 6a ed. Nova York: McGraw Hill, 2007.

[4] Cerruti, F. «Nuovo metodo per la classificazione dei tessuti». *L'Ingegneria Civile e le Arti Industrial*, any v, núm. 10 (octubre 1870), 157–159.

[5] Clapham, C. R. J. «When a fabric hangs together». *Bull. London Math. Soc.*, 12 (3) (1980), 161–164.

[6] Clapham, C. R. J. «The bipartite tournament associated with a fabric». *Discrete Math.*, 57 (1-2) (1985), 195–197.

[7] Crowe, D. W. «The mosaic patterns of H. J. Woods». Symmetry: unifying human understanding, I. *Comput. Math. Appl. Part B*, 12 (1-2) (1986), 407–411.

[8] Delaney, C. «When a fabric hangs together». Thirteenth Australasian Conference on combinatorial mathematics and computing (Sydney, 1985). *Ars Combin.*, 21A (1986), 71–79.

[9] Enns, T. C. «An efficient algorithm determining when a fabric hangs together». *Geom. Dedicata*, 15 (3) (1984), 259–260.

[10] Galbraith, S. D. *Mathematics of Public Key Cryptography. Version 2.0*. Octubre 2018. [Disponible en línia a https://www.math.auckland.ac.nz/~sgal018/crypto-book/main.pdf]

[11] Galcerán, V. *Lecciones de Teoría de Tejidos. Monturas a Lizos*. Terrassa: Escuela Especial de Ingenieros de Industrias Textiles de Tarrassa, 1953.

[12] Gand, E. «Nouvelles méthodes de construction des satins réguliers, pairs et impairs. 1-Théorie des nombres premiers appliquée aux pointés de ces armures». *Bull. Soc. Ind. Amiens* (gener 1867), 57–88.

[13] Gand, E. «Nouvelles méthodes de construction des satins réguliers, pairs et impairs. 2-Armures-tissu, armures-dessin, mosaïques». *Bull. Soc. Ind. Amiens* (juliol 1867), 257–300.

[14] Giménez, T. «Algunas observaciones sobre la teoría de los rasos». *Cataluña Textil*, tom xi, núm. 133 (octubre 1917), 131–134.

[15] Griswold, R. E. «When a fabric hangs together (or doesn't)» (juliol, 2004). [Disponible en línia a https://www2.cs.arizona.edu/patterns/weaving/webdocs/gre_hng1.pdf]

[16] Grünbaum, B.; Shephard, G. C. «Satins and twills: an introduction to the geometry of fabrics». *Math. Mag.*, 53 (3) (1980), 139–161.

[17] Grünbaum, B.; Shephard, G. C. «A catalogue of isonemal fabrics». A: *Discrete Geometry and Convexity* (New York, 1982). Nova York: New York Academy of Sciences, 1985, 279–298. (Ann. New York Acad. Sci.; 440)

[18] Grünbaum, B.; Shephard, G. C. «An extension to the catalogue of isonemal fabrics». *Discrete Math.*, 60 (1986), 155–192.

[19] Hoffstein, J.; Pipher, J.; Silverman, J. H. *An Introduction to Mathematical Cryptography*. 2a ed. Nova York: Springer, 2014. (Undergrad. Texts Math.)

[20] Knuth, D. E. *The Art of Computer Programming. Vol. 2. Seminumerical Algorithms*. 3a ed. Reading, MA: Addison-Wesley, 1998.

[21] Koshy, T. *Fibonacci and Lucas Numbers with Applications*. Hoboken, NJ: John Wiley & Sons, Inc., 2018 i 2019. 2 v. (Pure Appl. Math. (Hoboken))

[22] Krishnamurthy, V. R.; Akleman, E.; Subramanian, S. G.; Ebert, M.; Cui, J.; Fu, C.-A.; Starrett, C. «Geometrically interlocking space-filling tiling based on fabric weaves». *IEEE Trans. Visual Comput. Graphics*, 28 (10) (2022), 3391–3404.

[23] Lladó, C. *Teoria de teixits, un camp d'experiència per a la matemàtica*. Sabadell: Fundació Bosch i Cardellach, 2022.

[24] Lucas, E. *Aplication de l'arithmétique a la construction de l'armure des satins réguliers.* París: Gustave Retaux, Librairie-éditeur, 1867.

[25] Lucas, E. «Principii fondamentali della geometria dei tessuti.» *L'Ingegneria Civile e le arti industriali. Geometria Aplicata all'Industria*, any vi, núm. 7 (juliol 1880).

[26] Lucas, E. «Principii fondamentali della geometria dei tessuti. Appendice». *L'Ingegneria Civile e le arti industriali. Geometria Aplicata all'Industria*, any vi, núm. 8 (agost 1880).

[27] Niven, I.; Zuckerman, H. S.; Montgomery, H. L. *An Introduction to the Theory of Numbers*. 5a ed. Nova York: John Wiley & Sons, Inc., 1991.

[28] Renault, M. «The Fibonacci sequence modulo *m*». [Disponible en línia a http://webspace.ship.edu/msrenault/fibonacci/fib.htm]

[29] Rodón y Amigó, P. «Estudio científico de los rasos regulares». *Cataluña Textil*, tom i (2) (1906), 44–46.

[30] Rodón y Amigó, P. «Estudio científico de los rasos regulares (continuación)». *Cataluña Textil*, tom i (3) (1906), 69–70.

[31] Rodón y Amigó, P. «Estudio científico de los rasos regulares (continuación)». *Cataluña Textil*, tom i (5) (1907), 117–121.

[32] Rodón y Amigó, P. «Estudio científico de los rasos regulares (continuación)». *Cataluña Textil*, tom i (6) (1907), 136–138.

[33] Rodón y Amigó, P. «Estudio científico de los rasos regulares (continuación)». *Cataluña Textil*, tom I (10) (1907), 232–236.

[34] Rodón y Amigó, P. «Estudio científico de los rasos regulares (continuación)». *Cataluña Textil*, tom I (12) (1907), 293–299.

[35] Rodón y Amigó, P. «Estudio científico de los rasos regulares (continuación)». *Cataluña Textil*, tom I (14) (1907), 357–365.

[36] Shorter, S. A. «The mathematical theory of the sateen arrangement». *Math. Gaz.*, 10 (147) (1920), 92–97.

[37] Shoup, V. *A Computational Introduction to Number Theory and Algebra*. 2a ed. Cambridge: Cambridge University Press, 2009.

[38] Woods, H. J. «The geometrical basis of pattern design. Part I: Points and line symmetry in simple figures and borders». *J. Textile Inst. Transactions*, 26 (6) (1935), T197–T210.

[39] Woods, H. J. «The geometrical basis of pattern design. Part II: Nets and sateens». *J. Textile Inst. Transactions*, 26 (10) (1935), T293–T308.

[40] Woods, H. J. «The geometrical basis of pattern design. Part III: Geometrycal symmetry in plane patterns». *J. Textile Inst. Transactions*, 26 (12) (1935), T341–T357.

[41] Woods, H. J. «The geometrical basis of pattern design. Part IV: Countercharge symmetry in plane patterns.» *J. Textile Inst. Transactions*, 27 (12) (1936), T305–T320.

Carles Lladó
Jubilat de l'IES Sabadell
C/ Juvenal, 1
08206 Sabadell, Catalunya
cllado@xtec.cat

Josep M. Brunat
Jubilat del Departament de Matemàtiques
Universitat Politècnica de Catalunya
C/ Jordi Girona, 1–3
08034 Barcelona, Catalunya
josep.m.brunat@upc.edu