Japan Journal of Industrial and Applied Mathematics (2022) 39:75–96
https://doi.org/10.1007/s13160-021-00477-9

ORIGINAL PAPER

Satins, lattices, and extended Euclid's algorithm

Josep M. Brunat[1] · Joan-C. Lario[1]

Received: 4 March 2021 / Revised: 29 June 2021 / Accepted: 26 July 2021 /
Published online: 21 August 2021

Abstract

Motivated by the design of satins with draft of period m and step a, we draw our attention to the lattices $L(m,a)=\langle(1,a),(0,m)\rangle$ where $1\le a<m$ are integers with $\gcd(m,a)=1$. We show that the extended Euclid's algorithm applied to m and a produces a shortest no null vector of $L(m,\ a)$ and that the algorithm can be used to find an optimal basis of $L(m,\ a)$. We also analyze square and symmetric satins. For square satins, the extended Euclid's algorithm produces directly the two vectors of an optimal basis. It is known that symmetric satins have either a rectangular or a rombal basis; rectangular basis are optimal, but rombal basis are not always optimal. In both cases, we give the optimal basis directly in terms of m and a.

Keywords Satins · square satins · symmetric satins · extended Euclid's algorithm · Lagrange–Gauss lattice basis reduction · shortest vector · optimal basis.

Mathematics Subject Classification 11A05 · 11Z05 · 52C05

1 Introduction

A fabric consists in two sets of threads in perpendicular directions, called warp and weft (or woof). The traditional way to represent it is by the tiling of the plane by unit squares. Each vertical strip represents a thread of the warp and each horizontal strip a thread of the weft. Thus, each unit square represents the crossing of a warp-thread and a weft-thread. If the warp-thread pass over the weft thread, then the corresponding square is colored black; otherwise it is colored white. A way to design a fabric is to take a squared pattern of $m\times m$ unit squares, called the draft or the *design*, color each unit square black or white, and repeat it to tiling the plane. To obtain a fabric,

✉ Joan-C. Lario
joan-carles-lario@upc.edu

Josep M. Brunat
josep.m.brunat@upc.edu

[1] Departament de Matemàtiques, Universitat Politècnica de Catalunya, Barcelona, Spain

all the threads must hang together, so in each column and row of the draft there must be some black and some white squares.

There are a few attempts to study the mathematics of fabric designs. We can cite a six-pages paper by Shorter [13] in 1920, a series of four papers by Woods [14–17] in 1935 and 1936, the papers by Grünbaum and Shephard [6, 7] in 1980 and 1986, and an article by Crowe [2] in 1986 about the work of Woods. In almost all the cases the main interest is the symmetry group of the fabric.

A satin or sateen is the following special class of fabrics. Take a draft of size m (that means a square of $m \times m$ of unit squares) and label columns and rows from 0 to $m-1$. Then take an integer $a \in \{1, \dots, m-1\}$ with $\gcd(m, a) = 1$, and color black the square (v, r) in column v and row r if and only if $av \equiv r \pmod{m}$. Note that, in this way, each column of the draft has exactly one black square, and the same for each row. The integer m is called the period, and the integer a the step of the satin. When the draft is extended to cover the plane, we also have that a unit square with coordinates (v, r) is black if and only if $av \equiv r \pmod{m}$. The case $m = 2$ and $a = 1$ is called plain or calico and, for $m \geq 3$, the case $a = 1$ is called direct twill, and the case $a = m - 1$ indirect twill (often plain and twills are not considered as particular cases of satins, but different from satins). Figure 1 shows the drafts of the satin of period $m = 11$ and step $a = 4$, of the plain satin, and of the twills of period 4. The bottom rows from left to right represent the crossing of the weaf 0 with the warps $0, 1, \dots, m-1$, and the first column from bottom to top the crossing of warp 0 with the weafs $0, 1, \dots, m-1$.

Probably the first in considering the design of satins from a mathematical point of view was Édouard Lucas [9] in 1867, motivated by two articles of the same year by the industrial Édouard Gand [4, 5]. After that, Lucas insisted in the topic with an article and an appendix in an Italian specialized industrial journal [10, 11]. The main interest of Lucas was to characterize periods and steps that produce satins considered of great quality: square and symmetric satins, which are those such that $a^2 + 1 \equiv 0 \pmod{m}$, and $a^2 - 1 \equiv 0 \pmod{m}$, respectively; this is to say to find periods m and steps a such that a has quadratic residue -1 or $+1$ modulus m.

Instead of the traditional representation by squares, we shall use coordinates; this is not usual in the context of fabrics, but an early precedent is Cerruti [1]. We identify the satin of size m and step a with the set

$$L(m, a) = \{(v, r) \in \mathbb{Z}^2 : av \equiv r \pmod{m}\}.$$

In fact, this set is a lattice:

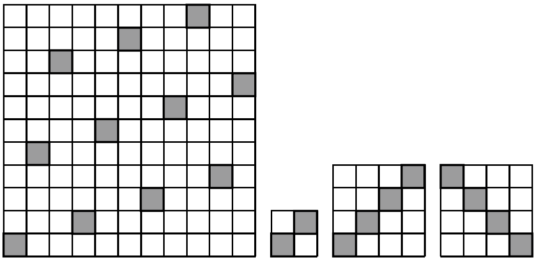

Fig. 1 The drafts of the satin of period $m = 11$ and step $a = 4$, of the plain satin, and of the direct and indirect twills of period 4

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

From now on, we identify a satin of period m and step a with the lattice

$$L(m,a)=\langle(1,a),(0,m)\rangle=\{\alpha(1,a)+\beta(0,m) : \alpha,\beta\in\mathbb{Z}\}.$$

A satin can be defined by its draft, but considered as a lattice, can be defined by a basis. It is natural to ask for the optimal basis; that is, a basis with the vectors as short as possible. An optimal basis can be obtained by the Lagrange–Gauss lattice basis-reduction algorithm.

Our goal is to relate the study of optimal basis in satin lattices $L(m, a)$ to the extended Euclid's algorithm applied to m and a. The paper is organized as follows.

In Sects. 2 and 3, we summarize basic properties of the extended Euclid's algorithm, and recall the Lagrange-Gauss algorithm for finding optimal basis; we apply it to obtain optimal basis of twills. In Sect. 4 we show how the extended Euclid's algorithm gives different basis of $L(m, a)$, and it always gives the shortest vector. Moreover, if the algorithm does not gives an optimal basis directly, then in just one step the Lagrange-Gauss algorithm finds the optimal basis. For square and symmetric satins, the extended Euclid's algorithm gives some additional information. In Sect. 5, we show that the algorithm always gives an optimal basis for square satins. Finally, in Sect. 6, we apply the algorithm to symmetric satins and provide their classification into rectangular and rombal, showing how to compute an optimal basis directly from the values of the period and step. While a rectangular basis is always optimal, a rombal basis can be optimal or not. In the case of rombal satins, we give both, the optimal and the rombal basis.

2 Extended Euclid's algorithm

Let us recall some of the basic properties of the extended Euclid's algorithm.

Let $1\le a<m$ be integers. Define by recursion the sequence $r_0=m$, $r_1=a$ and, for $i\ge 1$ and while $r_i\neq 0$, let q_i and r_{i+1} the quotient and the remainder of dividing r_{i-1} by r_i. If $r_{n+1}=0$, we have

$$r_{i+1}=r_{i-1}-q_ir_i \quad\text{for}\quad i\in\{1,\dots,n\},$$

and $r_n=\gcd(m,a)$. We also define, for $i\in\{1,\dots,n\}$,

$$\begin{aligned}u_0=1,\ \ u_1=0,\ \ u_{i+1}=u_{i-1}-q_iu_i,\\ v_0=0,\ \ v_1=1,\ \ v_{i+1}=v_{i-1}-q_iv_i.\end{aligned}$$

We shall denote the data of the extended Euclid's algorithm by

$$\mathrm{E}(m,a)=\{(u_i,v_i,r_i)\}_{i=0}^{n+1}\cup\{q_i\}_{i=1}^{n}.$$

The following properties are easily proved (most of them by induction) and almost all can be found in Shoup [12, Theorem 4.3].

Theorem 2.1 *Let* $1 \leq a < m$ *be integers and let* $d = \gcd(m, a)$. *Then*, $E(m,\ a)$ *satisfies*:

(i) $r_i = u_i m + v_i a$ *for all* $i \in \{0, 1 \dots, n+1\}$.
(ii) $\gcd(m, a) = r_n = u_n m + v_n a$.
(iii) $u_{i+1} v_i - u_i v_{i+1} = (-1)^{i+1}$ *for all* $i \in \{0, \dots, n\}$.
(iv) $\gcd(u_i, v_i) = 1$ *for all* $i \in \{0, \dots, n+1\}$.
(v) *For all* $i \in \{2, \dots, n+1\}$, *if* i *is even*, *then* $u_i > 0$; *if* i *is odd*, *then* $u_i < 0$.
(vi) *For all* $i \in \{1, \dots, n+1\}$, *if* i *is even*, *then* $v_i < 0$; *if* i *is odd*, *then* $v_i > 0$.
(vii) $|u_{i+1}| \geq |u_i|$ *for all* $i \in \{1, \dots, n\}$.
(viii) $|v_{i+1}| \geq |v_i|$ *for all* $i \in \{0, \dots, n\}$ *and*, *if* $a < m/2$, *then* $|v_{i+1}| > |v_i|$.
(ix) $u_{i+1} r_i - u_i r_{i+1} = (-1)^i a$ *and* $|u_{i+1}| r_i \leq a$, *for all* $i \in \{0, \dots, n\}$.
(x) $v_{i+1} r_i - v_i r_{i+1} = (-1)^i m$ *and* $|v_{i+1}| r_i \leq m$, *for all* $i \in \{0, \dots, n\}$.
(xi) $|u_{n+1}| = a/d, |v_{n+1}| = m/d$.
(xii) $|u_n| \leq \min\{a/2,\ a/d\}, |v_n| \leq \min\{m/2, m/d\}$.

Remark 2.1 If $\gcd(m, a) = 1$, then properties (xi) and (xii) above are

$$|u_{n+1}| = a, \quad |v_{n+1}| = m, \quad |u_n| \leq a/2, \quad |v_n| \leq m/2.$$

We set $\mathbf{e}_i = (v_i, r_i)$ for $i \in \{0, \dots, n+1\}$, and call them the vectors of $E(m,\ a)$.

The following property shall be useful to deal with square and symmetric satins.

Proposition 2.1 *Keep the above notations and assume that* $1 \leq a < m/2$. *For* $i \in \{1, \dots, n\}$, *the integers* $|v_{i-1}|$ *and* q_i *are the remainder and the quotient*, *respectively*, *of the division of* $|v_{i+1}|$ *by* $|v_i|$.

Proof Since $a < m/2$, we know that $0 = |v_0| < |v_1| < \dots < |v_n| < |v_{n+1}|$. By definition, $v_2 = v_0 - q_1 v_1 = -q_1 a$. The remainder of dividing $|v_2| = q_1 a$ by $|v_1| = a$ is $0 = v_0$. For $i \geq 3$, we have $v_{i+1} = v_{i-1} - q_i v_i$ and $v_{i-1} v_i < 0$. Then,

$$|v_{i+1}| = |v_{i-1}| + q_i |v_i|, \quad |v_{i-1}| < |v_i|,$$

that is, $|v_{i-1}|$ is the remainder of dividing $|v_{i+1}|$ by $|v_i|$ and q_i is the quotient. □

3 Lagrange–Gauss algorithm

Let $\mathbf{u} \in \mathbb{R}^2$ and denote $\langle \mathbf{u} \rangle = \{\alpha \mathbf{u} : \alpha \in \mathbb{Z}\}$. If $\mathbf{u}$ and $\mathbf{v}$ are two independent vectors of $\mathbb{R}^2$, the lattice generated by $\mathbf{u}$ and $\mathbf{v}$ is the additive subgroup of $\mathbb{R}^2$

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

An *optimal basis* of a lattice L is a basis $(\mathbf{b}_1, \mathbf{b}_2)$ such that for all $\mathbf{x} \in L \setminus \{\mathbf{0}\}$ one has:

1. $\|\mathbf{b}_1\| \leq \|\mathbf{x}\|$;
2. if $\|\mathbf{x}\| \leq \|\mathbf{b}_2\|$ then $\|\mathbf{x}\| = \|\mathbf{b}_1\|$ or $\|\mathbf{x}\| = \|\mathbf{b}_2\|$.

The vector $\mathbf{b}_1$ of an optimal basis $(\mathbf{b}_1, \mathbf{b}_2)$ is called a *shortest vector* of L, and $\mathbf{b}_2$ a *second shortest vector*. Note that if $\mathbf{b}_1$ is a shortest vector, $-\mathbf{b}_1$ is a shortest vector too. Hence, we can always take a shortest vector with a no negative second coordinate.

An optimal basis of a lattice $L = \langle \mathbf{u}, \mathbf{v} \rangle$ can be found by using the Lagrange–Gauss algorithm. We refer, for instance, to Hoffstein and Pipper [8] or Galbraith [3] for more details. We denote $\lfloor \mu \rceil = \lfloor \mu + 1/2 \rfloor$ the closest integer to the real number μ; note that in case that z is an integer and $\mu = z + 1/2$, then $\lfloor \mu \rceil = z$.

Input A basis $(\mathbf{u}, \mathbf{v})$ of a lattice L with $\|\mathbf{u}\| \leq \|\mathbf{v}\|$.

Output An optimal basis $(\mathbf{b}_1, \mathbf{b}_2)$ of L.

```
1  Let $\mathbf{b}_1 = \mathbf{u}$,   $\mathbf{b}_2 = \mathbf{v}$,  $h = \lfloor (\mathbf{b}_1 \cdot \mathbf{b}_2)/\|\mathbf{b}_1\|^2 \rceil$.
2  If $h = 0$, then output $(\mathbf{b}_1, \mathbf{b}_2)$. End.
3  If $h \neq 0$, then $\mathbf{b}_2 = \mathbf{b}_2 - h\mathbf{b}_1$.
4  If $\|\mathbf{b}_2\| < \|\mathbf{b}_1\|$ then swap $\mathbf{b}_1$ and $\mathbf{b}_2$.
5  Repeat with the new input $(\mathbf{b}_1, \mathbf{b}_2)$.
```

Remark 3.1 Note that if $(\mathbf{u}, \mathbf{v})$ is a basis of a lattice L with $\|\mathbf{u}\| \leq \|\mathbf{v}\|$, and the vectors $\mathbf{u}$ and $\mathbf{v}$ are ortogonal, then $(\mathbf{u}, \mathbf{v})$ is an optimal basis.

Remark 3.2 Suppose that $(\mathbf{u}, \mathbf{v})$ is a basis of a lattice L and that $\mathbf{u}$ is a shortest vector of L. Then, the Lagrange–Gauss algorithm takes at most one step to find an optimal basis. Indeed, we calculate $\mu = (\mathbf{u} \cdot \mathbf{v})/\|\mathbf{u}\|^2$ and $h = \lfloor \mu \rceil$. If $h = 0$, then $(\mathbf{u}, \mathbf{v})$ is optimal. If not, the new value of h is $h' = \lfloor \mu' \rceil$ where

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

As $-1/2 < \mu - h \leq 1/2$, we have $h' = \lfloor \mu' \rceil = \lfloor \mu - h \rceil = 0$. Hence, $(\mathbf{u}, \mathbf{v} - h'\mathbf{u})$ is an optimal basis of L.

As an immediate application of the algorithm, we consider the case of direct twills; that is, the satin lattices $L(m, 1)$ with period $m \geq 3$ and step $a = 1$. (Observe that the plain satin $L(2, 1)$ has optimal basis $((1, 1), (-1, 1))$.

Proposition 3.1 *An optimal basis of the direct twill $L(m, 1)$ is given by*:

(i) $((1,1),(-m/2,m/2))$, *if m is even*;
(ii) $((1,1),(-(m-1)/2,(m+1)/2))$, *if m is odd.*

Proof As $m \geq 3$, the vector $\mathbf{b}_1 = (1,1)$ has norm less or equal to the norm of $\mathbf{b}_2 = (0,m)$. Suppose that m is even. In the first iteration,

$$h = \left\lfloor \frac{m}{2} \right\rceil = \frac{m}{2}.$$

The new $\mathbf{b}_2$ is

$$\mathbf{b}_2 = (0,m) - \frac{m}{2}(1,1) = \left(-\frac{m}{2}, \frac{m}{2}\right),$$

which is orthogonal to (1, 1). Hence, $((1,1),(-m/2,m/2))$ is an optimal basis. If m is odd, then

$$h = \left\lfloor \frac{m}{2} \right\rceil = \frac{m-1}{2},$$

and the new $\mathbf{b}_2$ is

$$\mathbf{b}_2 = (0,m) - \frac{m-1}{2}(1,1) = \left(-\frac{m-1}{2}, \frac{m+1}{2}\right).$$

For the next iteration,

$$\mathbf{b}_1 \cdot \mathbf{b}_2 = (1,1) \cdot \left(-\frac{m-1}{2}, \frac{m+1}{2}\right) = 1, \qquad \|\mathbf{b}_1\|^2 = 2.$$

Therefore, $h = \lfloor 1/2 \rceil = 0$ and we have that $((1,1),(-(m-1)/2,(m+1)/2))$ is an optimal basis. □

Two satins $L(m, a)$ and $L(m, m-a)$ are called *complementaries*. The equivalences

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

show that the lattices $L(m, a)$ and $L(m, m-a)$ are symmetrical with respect to the two coordinate axis. Then, properties of $L(m, m-a)$ can be deduced from properties of $L(m, a)$ by symmetry. Thus, when necessary, we can restrict ourselves to the case $a < m/2$. For instance, if $a < m/2$ and $((u_1,u_2),(v_1,v_2))$ is an optimal basis of $L(m, a)$, then $((-u_1,u_2),(-v_1,v_2))$ is an optimal basis of $L(m, m-a)$. In particular, as a consequence of Proposition 3.1, we have

Proposition 3.2 *An optimal basis of the indirect twill* $L(m, m-1)$ *of period* m *is given by*:

(i) $((-1,1),(m/2,m/2))$, *if* m *is even*;
(ii) $((-1,1),((m-1)/2,(m+1)/2))$, *if* m *is odd.*

4 Euclid's algorithm and the shortest vector

Consider the basis $((1, a), (0, m))$ of the satin $L(m, a)$. Given vectors $\mathbf{u}, \mathbf{v}$ in $L(m, a)$, one has that $(\mathbf{u}, \mathbf{v})$ is another basis of $L(m, a)$ if and only if $m = |\det((1, a), (0, m))| = |\det(\mathbf{u}, \mathbf{v})|$. We can see that a pair of consecutive vectors of $E(m, a)$ form a basis of $L(m, a)$.

Proposition 4.1 *Let* $L(m, a)$ *be a satin and let* $\mathbf{e}_0, \dots, \mathbf{e}_{n+1}$ *be the vectors of* $E(m, a)$. *Then, for all* $i \in \{0, \dots, n\}$, *the couple* $(\mathbf{e}_i, \mathbf{e}_{i+1})$ *is a basis of* $L(m, a)$.

Proof The vectors $\mathbf{e}_0 = (0, m)$ and $\mathbf{e}_1 = (1, a)$ are in $L(m, a)$. By induction, if $\mathbf{e}_{i-2}$ and $\mathbf{e}_{i-1}$ are vectors of $L(m, a)$, then $\mathbf{e}_{i+1} = \mathbf{e}_{i-1} - q_i\mathbf{e}_i \in L(m, a)$. Then all the vectors of $E(m, a)$ are vectors of $L(m, a)$. By Theorem 2.1 (x), we have

$$|\det(\mathbf{e}_i, \mathbf{e}_{i+1})| = |v_i r_{i+1} - v_{i+1} r_i| = |(-1)^{i+1} m| = m.$$

Hence, $(\mathbf{e}_i, \mathbf{e}_{i+1})$ is a basis of $L(m, a)$. □

Our next goal is to show that we can found among the vectors of $E(m, a)$ one that is a shortest vector of $L(m, a)$. First, we get easy bounds on the coordinates of a shortest vector in $L(m, a)$.

Lemma 4.1 *Let* $\mathbf{e} = (v, r)$ *be a shortest vector of the satin* $L(m, a)$, *with* $r \geq 0$. *Then, one has*

$$\|\mathbf{e}\| < m, \quad 0 < r < m, \quad \text{and} \quad 0 < |v| < m.$$

Proof The conditions $1 \leq a < m$ and $(1, a) \in L(m, a)$ imply $\|\mathbf{e}\|^2 \leq \|(1, a)\|^2 = 1 + a^2 < (1 + a)^2 \leq m^2 .= 1 + a^2 < (1 + a)^2 \leq m^2$. It follows $\|\mathbf{e}\| < m$. The inequality $m^2 > \|\mathbf{e}\|^2 = v^2 + r^2$ implies $m > r$ and $m > |v|$.

If $0 = |v|$, then $\mathbf{e} = (0, r) = x(0, m) + y(1, a) = (y, xm + ya)$ for some intergers x and y, which implies $y = 0$ and $m > r = xm \geq m$, a contradiction. Hence, $|v| > 0$.

If $r = 0$, since $av \equiv r \equiv 0 \pmod{m}$ and $\gcd(a, m) = 1$, we have $v \equiv 0 \pmod{m}$. Taking in account $|v| < m$, we get $v = 0$. Thus, $\mathbf{e} = (v, r) = (0, 0)$ is a contradiction. Hence, $r > 0$. □

Next proposition is the adaptation to our context of the first part of the "Reconstruction Theorem" of Shoup [12, Theorem 4.9]. For the sake of completeness we include the proof, which is (almost) the same.

Proposition 4.2 *Let* $L(m, a)$ *be a satin, and let* $\mathbf{e}_i = (v_i, r_i)$, $i \in \{0, \dots, n+1\}$, *be the vectors of* $E(m, a)$. *Let* $\mathbf{e} = (v, r) \in L(m, a)$ *with* $r > 0$. *If* $j = \min\{i : r \geq r_i\}$, *then,* $|v| \geq |v_j|$ *and* $\|\mathbf{e}\| \geq \|\mathbf{e}_j\|$.

Proof If $v = 0$, the result is immediate with $j = 0$. Then, we can suppose $v \neq 0$.

The sequence $r_0 = m, \dots, r_{n+1} = 0$ is strictly decreasing. Hence j is a well defined integer and $j \geq 1$.

The condition $(v, r) \in L(m, a)$ means that $um + av = r$ for some $u \in \mathbb{Z}$. By Theorem 2.1 (iii), we have $\varepsilon = u_j v_{j-1} - u_{j-1} v_j \in \{\pm 1\}$. Then, the numbers

$$\sigma = \frac{1}{\varepsilon}(v_{j-1}u - u_{j-1}v), \quad \tau = \frac{1}{\varepsilon}(u_j v - v_j u)$$

are integers. We have

$$\begin{aligned} u_j\sigma + u_{j-1}\tau &= \frac{1}{\varepsilon}(u_j v_{j-1} u - u_j u_{j-1} v + u_{j-1} u_j v - u_{j-1} v_j u) \\ &= \frac{1}{\varepsilon}(u(u_j v_{j-1} - u_{j-1} v_j)) \\ &= \frac{1}{\varepsilon} u\varepsilon = u, \end{aligned}$$

and, analogously, one has $v_j\sigma + v_{j-1}\tau = v$.

We have three possible cases. We shall see that in the first two we have $|v| \geq |v_j|$ as required, and that the last one implies a contradiction.

(i) $\tau = 0$. Then $v_j\sigma = v$. Since $v \neq 0$, we have $|v| \geq |v_j|$.

(ii) $\sigma\tau < 0$. From Theorem 2.1, we know that $v_j v_{j-1} \leq 0$. Also, σ and τ have different sign. Then, $v_j\sigma + v_{j-1}\tau = v$ implies $|v| = |v_j| \cdot |\sigma| + |v_{j-1}| \cdot |\tau| \geq |v_j|$.

(iii) $\tau \neq 0$ i $\sigma\tau \geq 0$. Multiplying $u_j\sigma + u_{j-1}\tau = u$ by m and $v_j\sigma + v_{j-1}\tau = v$ by a, we get

$$mu_j\sigma + mu_{j-1}\tau = mu, \quad av_j\sigma + av_{j-1}\tau = av.$$

Adding both equalities, it follows

$$\sigma(mu_j + av_j) + \tau(mu_{j-1} + av_{j-1}) = mu + va = r,$$

that is, $\sigma r_j + \tau r_{j-1} = r$. Since $\sigma\tau \geq 0$ and $r, r_{j-1}, r_j \geq 0$, we have $\sigma > 0$, $\tau > 0$ and $r = \sigma r_j + \tau r_{j-1} \geq \tau r_{j-1} \geq r_{j-1} > r$, which contradicts the definition of j.

Thus, we have $r \geq r_j$ and $|v| \geq |v_j|$. Hence, $\|\mathbf{e}\| \geq \|\mathbf{e}_j\|$. □

As a consequence, we have the following theorem.

Theorem 4.1 *Let $L(m, a)$ be a satin. Then, one of the vectors of $E(m, a)$ is a shortest vector in $L(m, a)$.*

Proof Let $\mathbf{e} = (v, r)$ be a shortest vector of $L(m, a)$ with $r \geq 0$, and let $\mathbf{e}_0, \dots, \mathbf{e}_{n+1}$ be the vectors of $E(m, a)$. From Lemma 4.1 we have $r > 0$. By applying Proposition 4.2 to the vector $\mathbf{e} = (v, r)$, we have $\|\mathbf{e}\| \geq \|\mathbf{e}_j\|$ for some $j \in \{0, \dots, n+1\}$. As $\mathbf{e}$ is a shortest vector, $\|\mathbf{e}_j\| \geq \|\mathbf{e}\|$. Thus, $\|\mathbf{e}_j\| = \|\mathbf{e}\|$ and $\mathbf{e}_j$ is a shortest vector. □

Theorem 4.1 does not explain when, in the execution of Euclid's algorithm, the shortest vector has been reached. The remainder of this section is devoted to precise which of the vectors of $E(m, a)$ is the shortest.

The case of the plain satin is immediate. The lattice $L(2, 1)$ has four shortest vectors: $(1, 1)$, $(-1, 1)$, $(1, -1)$ and $(-1, -1)$, and $E(2, 1)$ has just three vectors $\mathbf{e}_0 = (0, 2)$, $\mathbf{e}_1 = (1, 1)$ and $\mathbf{e}_2 = (-2, 0)$, and $\mathbf{e}_1$ is a shortest vector. An optimal basis is $((1, 1), (-1, 1))$. Thus, to the end of this section we consider only satins different from the plain satin, that is, with $m > 2$.

Next proposition shows some useful properties of the vectors of $E(m, a)$.

Proposition 4.3 *Let $L(m, a)$ with $m > 2$ be a satin and let $\mathbf{e}_i = (v_i, r_i)$, $i \in \{0, \dots, n+1\}$, be the vectors of $E(m, a)$. Then, it holds:*

(i) $\mathbf{e}_{i-1} \cdot \mathbf{e}_i > \mathbf{e}_i \cdot \mathbf{e}_{i+1}$ *for all* $i \in \{1, \dots, n\}$.
(ii) *The number* $\ell = \min\{i : \mathbf{e}_{i-1} \cdot \mathbf{e}_i < 0\}$ *is well defined and it holds* $\mathbf{e}_{i-1} \cdot \mathbf{e}_i \geq 0$ *for* $i \leq \ell - 1$ *and* $\mathbf{e}_{i-1} \cdot \mathbf{e}_i < 0$ *for* $i \geq \ell$.
(iii) *The integer* $k = \min\{i : |v_i| > r_i\}$ *is well defined and* $\ell - 1 \leq k \leq \ell$.
(iv) $\|\mathbf{e}_0\| > \dots > \|\mathbf{e}_{k-2}\|$.
(v) *If* $k = \ell$, *then* $\|\mathbf{e}_k\| < \dots < \|\mathbf{e}_{n+1}\|$.
(vi) *If* $k = \ell - 1$, *then* $\|\mathbf{e}_{k+1}\| < \dots < \|\mathbf{e}_{n+1}\|$.

Proof (i) By definition of $\mathbf{e}_i$, one has

$$\mathbf{e}_{i+1} \cdot \mathbf{e}_i = (\mathbf{e}_{i-1} - q_i \mathbf{e}_i) \cdot \mathbf{e}_i = \mathbf{e}_{i-1} \cdot \mathbf{e}_i - q_i \|\mathbf{e}_i\|^2 < \mathbf{e}_{i-1} \cdot \mathbf{e}_i.$$

(ii) By (i), the sequence of scalar products $\mathbf{e}_{i-1} \cdot \mathbf{e}_i$ is strictly decreasing. Now, $\mathbf{e}_0 \cdot \mathbf{e}_1 = (0, m) \cdot (1, a) = ma > 0$ and $\mathbf{e}_n \cdot \mathbf{e}_{n+1} = (v_n, 1) \cdot (v_{n+1}, 0) = v_n v_{n+1} < 0$. Hence, ℓ is well defined and $\mathbf{e}_{i-1} \cdot \mathbf{e}_i \geq 0$ for $i \leq \ell - 1$ and $\mathbf{e}_{i-1} \cdot \mathbf{e}_i < 0$ for $i \geq \ell$.

(iii) We have $|v_0| = 0 < m = r_0$ and $|v_{n+1}| = m > 0 = r_{n+1}$. Moreover, the sequence (r_i) is strictly decreasing and the sequence $(|v_i|)$ is increasing. Hence, $k = \min\{i : |v_i| > r_i\}$ is well defined and $k \geq 1$.

By definition of k, we have $|v_k| > r_k$ and $|v_{k+1}| > r_{k+1}$. Taking in account that $v_k v_{k+1} < 0$, it follows

$$\mathbf{e}_k \cdot \mathbf{e}_{k+1} = v_k v_{k+1} + r_k r_{k+1} = -|v_k| \cdot |v_{k+1}| + r_k r_{k+1} < 0.$$

This implies $\ell - 1 \leq k$.

If $\ell < k$, we have

$$0 > \mathbf{e}_{\ell-1} \cdot \mathbf{e}_{\ell}, \quad r_{\ell} \geq |v_{\ell}|, \quad r_{\ell-1} > r_{\ell} \geq |v_{\ell}| > |v_{\ell-1}|.$$

Then, it follows

$$0 > \mathbf{e}_{\ell-1} \cdot \mathbf{e}_{\ell} = -|v_{\ell-1}| \cdot |v_{\ell}| + r_{\ell-1} r_{\ell} > 0,$$

a contradiction. Therefore, $k \leq \ell$. So, we have $\ell - 1 \leq k \leq \ell$.

(iv) Certainly, $\|\mathbf{e}_0\| = m^2 > 1 + a^2 = \|\mathbf{e}_1\|$. Suppose $2 \leq i \leq k-2$. Since $k-2 \in \{\ell-3, \ell-2\}$, the scalar product $\mathbf{e}_i \cdot \mathbf{e}_{i+1}$ is not negative and from the equality $\mathbf{e}_{i-1} = q_i \mathbf{e}_i + \mathbf{e}_{i+1}$ it follows

$$\|\mathbf{e}_{i-1}\|^2 = q_i^2 \|\mathbf{e}_i\|^2 + \|\mathbf{e}_{i+1}\|^2 + 2q_i \mathbf{e}_i \cdot \mathbf{e}_{i+1} > q_i \|\mathbf{e}_i\|^2 \geq \|\mathbf{e}_i\|^2.$$

(v) and (vi) Suppose $i \geq \ell$. Since the scalar product $\mathbf{e}_{i-1} \cdot \mathbf{e}_i$ is negative, from $\mathbf{e}_{i+1} = \mathbf{e}_{i-1} - q_i \mathbf{e}_i$, it follows

$$\|\mathbf{e}_{i+1}\|^2 = \|\mathbf{e}_{i-1}\|^2 + q_i^2 \|\mathbf{e}_i\|^2 - 2q_i \mathbf{e}_{i-1} \cdot \mathbf{e}_i > \|\mathbf{e}_{i-1}\| + q_i^2 \|\mathbf{e}_i\|^2 > \|\mathbf{e}_i\|^2.$$

In the case (v) we have $i \geq k = \ell$, and in the case (vi) we have $i \geq k + 1 = \ell$. In both cases, the statement follows. □

Theorem 4.2 *Let $L(m, a)$ be a satin with $m > 2$ and let $\mathbf{e}_i = (v_i, r_i)$, $i \in \{0, \ldots, n+1\}$, be the vectors of $E(m, a)$. Let $k = \min\{i : |v_i| > r_i\}$. Then one of the four vectors $\mathbf{e}_{k-2}$, $\mathbf{e}_{k-1}$, $\mathbf{e}_k$, or $\mathbf{e}_{k+1}$ is a shortest vector of $L(m, a)$. Moreover,*

(i) *if $\mathbf{e}_{k-2}$ is a shortest vector of $L(m, a)$, then either $(\mathbf{e}_{k-2}, \mathbf{e}_{k-1})$ or $(\mathbf{e}_{k-2}, \mathbf{e}_k)$ is an optimal basis;*

(ii) *if $\mathbf{e}_{k+1}$ is a shortest vector of $L(m, a)$, then either $(\mathbf{e}_{k+1}, \mathbf{e}_k)$ or $(\mathbf{e}_{k+1}, \mathbf{e}_{k-1})$ is an optimal basis.*

Proof Note that $\mathbf{e}_0 = (0, m)$ and $\mathbf{e}_1 = (1, a)$. Hence $k \geq 2$. By Theorem 4.1, one of the vectors of $E(m, a)$ is a shortest vector of $L(m, a)$. Thus, it suffices to prove that the vector of $E(m, a)$ with minimum norm is $\mathbf{e}_{k-2}$, $\mathbf{e}_{k-1}$, $\mathbf{e}_k$ or $\mathbf{e}_{k+1}$. By Proposition 4.3 (iv), (v) and (vi), we have

$$\|\mathbf{e}_{k-2}\| = \min\{\|\mathbf{e}_0\|, \ldots, \|\mathbf{e}_{k-2}\|\}, \quad \|\mathbf{e}_{k+1}\| = \min\{\|\mathbf{e}_{k+1}\|, \ldots, \|\mathbf{e}_{n+1}\|\}.$$

Hence

$$\min\{\|\mathbf{e}_0\|, \ldots, \|\mathbf{e}_{n+1}\|\} = \min\{\|\mathbf{e}_{k-2}\|, \|\mathbf{e}_{k-1}\|, \|\mathbf{e}_k\|, \|\mathbf{e}_{k+1}\|\}.$$

(i) The vector $\mathbf{e}_0 = (0, m)$ is not a shortest vector of $L(m, a)$. Then, since $\mathbf{e}_{k-2}$ is a shortest vector, it must be $k \geq 3$ and $|v_{k-2}| > 0$.

Let $\mu = (\mathbf{e}_{k-2} \cdot \mathbf{e}_{k-1}) / \|\mathbf{e}_{k-2}\|^2$ and $h = \lfloor \mu \rceil$. A second shortest vector of $L(m, a)$ is $\mathbf{e} = \mathbf{e}_{k-1} - h\mathbf{e}_{k-2}$.

From Proposition 4.3 (ii) and (iii), we have $0 \leq \mathbf{e}_{k-2} \cdot \mathbf{e}_{k-1}$. Since $v_{k-2} v_{k-1} < 0$, it holds

$$0 \le \mathbf{e}_{k-2} \cdot \mathbf{e}_{k-1} = -|v_{k-2}| \cdot |v_{k-1}| + r_{k-2}r_{k-1} \le r_{k-2}r_{k-1} < r_{k-2}^2 \le \|\mathbf{e}_{k-2}\|^2.$$

Then, $0 \le \mu \le 1$ and $h \in \{0, 1\}$. If $h = 0$, then $(\mathbf{e}_{k-2}, \mathbf{e}_{k-1})$ is an optimal basis. Consider the case $h = 1$. Then, $(\mathbf{e}_{k-2}, \mathbf{e}_{k-1} - \mathbf{e}_{k-2})$ is an optimal basis. If $\mathbf{e} = (v, r) = \mathbf{e}_{k-2} - \mathbf{e}_{k-1}$, then $(\mathbf{e}_{k-2}, \mathbf{e})$ is optimal, too.

Since $(\mathbf{e}_{k-2}, \mathbf{e}_{k-1})$ is not optimal, we have $\|\mathbf{e}_{k-1}\| > \|\mathbf{e}\|$. Note that $r = r_{k-2} - r_{k-1} > 0$. Proposition 4.2 implies that if $j = \min\{i : r \ge r_i\}$, then $\|\mathbf{e}\| \ge \|\mathbf{e}_j\|$. From $r = r_{k-2} - r_{k-1} < r_{k-2}$, it follows $j \ge k - 1$.

We can distinguish four cases $j = k - 1$, $j = k$, $j = k + 1$ and $j > k + 1$. In the cases $j = k$ and $j = k + 1$ we shall proof that $(\mathbf{e}_{k-2}, \mathbf{e}_k)$ is an optimal basis, and that the other two cases are not possible.

If $j = k$, we have $\|\mathbf{e}\| \ge \|\mathbf{e}_k\|$. If $\|\mathbf{e}\| > \|\mathbf{e}_k\|$, then $(\mathbf{e}_{k-2}, \mathbf{e})$ is not optimal. Hence, $\|\mathbf{e}\| = \|\mathbf{e}_k\|$ and $(\mathbf{e}_{k-2}, \mathbf{e}_k)$ is an optimal basis.

If $j = k + 1$, then $r_{k-2} - r_{k-1} = r < r_{k-1}$ and $r_{k-2} < 2r_{k-1}$. It implies $q_{k-1} = 1$, so $\mathbf{e} = \mathbf{e}_{k-2} - \mathbf{e}_{k-1} = \mathbf{e}_{k-2} - q_{k-1}\mathbf{e}_{k-1} = \mathbf{e}_k$. We have that $(\mathbf{e}_{k-2}, \mathbf{e}_k)$ is an optimal basis.

If $j = k - 1$, we have $\|\mathbf{e}\| \ge \|\mathbf{e}_{k-1}\| > \|\mathbf{e}\|$, that is a contradiction.

Finally, if $j > k + 1$, we have $\|\mathbf{e}\| \ge \|\mathbf{e}_j\| > \|\mathbf{e}_{k+1}\|$, again a contradiction.

(ii) Now we assume that $\mathbf{e}_{k+1}$ is a shortest vector. Let $\mu = (\mathbf{e}_k \cdot \mathbf{e}_{k+1})/\|\mathbf{e}_{k+1}\|^2$ and $h = \lfloor \mu \rceil$. A second shortest vector of $L(m, a)$ is $\mathbf{e} = \mathbf{e}_k - h\mathbf{e}_{k+1}$.

Since $v_k v_{k+1} < 0$ and $\mathbf{e}_k \cdot \mathbf{e}_{k+1} < 0$, it follows

$$0 > \mathbf{e}_{k+1} \cdot \mathbf{e}_k = -|v_{k+1}| \cdot |v_k| + r_{k+1}r_k \ge -|v_{k+1}| \cdot |v_k| > -v_{k+1}^2 \ge -\|\mathbf{e}_{k+1}\|^2.$$

Then, $0 > \mu \ \ge -1$ and $h \in \{0, -1\}$. If $h = 0$ then $\mathbf{e} = \mathbf{e}_k$ and $(\mathbf{e}_{k+1}, \mathbf{e}_k)$ is optimal. Consider now the case $h = -1$. If $\mathbf{e} = (v, r) = \mathbf{e}_k + \mathbf{e}_{k+1}$, then $(\mathbf{e}_{k+1}, \mathbf{e})$ is an optimal basis and $\|\mathbf{e}_k\| > \|\mathbf{e}\|$.

As before, let $j = \min\{i : r \ge r_i\}$. We have $\|\mathbf{e}\| \ge \|\mathbf{e}_j\|$. Since $r = r_k + r_{k+1} > r_k$, we have $j \le k$. We can distinguish the four cases $j < k - 2$, $j = k - 2$, $j = k - 1$ and $j = k$. We shall see that only $j = k - 1$ is possible and, in this case $(\mathbf{e}_{k+1}, \mathbf{e}_{k-1})$ is an optimal basis.

If $j = k - 1$, then $\|\mathbf{e}\| \ge \|\mathbf{e}_{k-1}\| \ge \|\mathbf{e}\|$. Hence $\|\mathbf{e}\| = \|\mathbf{e}_{k-1}\|$ and $(\mathbf{e}_{k+1}, \mathbf{e}_{k-1})$ is an optimal basis.

If $j < k - 2$, then $\|\mathbf{e}\| \ge \|\mathbf{e}_j\| > \|\mathbf{e}_{k-2}\|$, which is a contradiction.

If $j = k - 2$, then

$$r_{k+1} + r_k = r \ge r_{k-2} = q_{k-1}r_{k-1} + r_k,$$

and

$$r_{k-1} > r_{k+1} \ge q_{k-1}r_{k-1} + r_k \ge r_{k-1},$$

again a contradiction.

If $j = k$, then $\|\mathbf{e}\| \ge \|\mathbf{e}_k\| > \|\mathbf{e}\|$, a contradiction. □

First part of Theorem 4.2 can be viewed as follows (see Fig. 2). For each vector $\mathbf{e}_i$ of $E(m, a)$, consider the point in the first quadrant $\tilde{\mathbf{e}}_i = (|v_i|, r_i)$. Joining points with consecutive index, we obtain a polygonal from $\tilde{\mathbf{e}}_0 = (0, m)$ with each

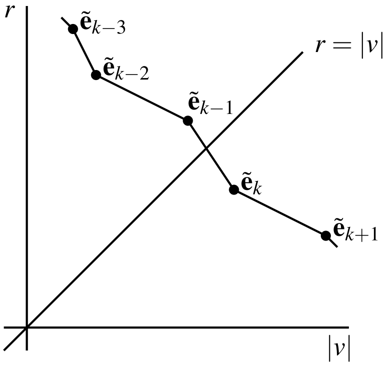
r
$\tilde{\mathbf{e}}_{k-3}$
$\tilde{\mathbf{e}}_{k-2}$
$\tilde{\mathbf{e}}_{k-1}$
$r=|v|$
$\tilde{\mathbf{e}}_{k}$
$\tilde{\mathbf{e}}_{k+1}$
$|v|$

Fig. 2 Ilustration of theorem 4.2

vertex lower and further on the right than the preceding one. The norm of $\mathbf{e}_i$ is the distance from $\tilde{\mathbf{e}}_i$ to the origin. The first point after the polygonal crosses the bisector of the axes corresponds to the index k. The point closest to the origin is one of the four closest points to the bisector.

By Theorem 4.2, a shortest vector of $L(m, a)$ can be found by calculating the vectors $\mathbf{e}_i = (v_i, r_i)$ of $E(m, a)$ till we reach an index $k+1$ such that $|v_k| > r_k$, and select from the four vectors $\mathbf{e}_{k-2}, \mathbf{e}_{k-1}, \mathbf{e}_k$ and $\mathbf{e}_{k+1}$ the one with smaller norm, say $\mathbf{e}_s$. This is a shortest vector of $L(m, a)$. If $s = k-2$, a second shortest vector of $L(m, a)$ is the shortest among the two vectors $\mathbf{e}_{k-1}$ and $\mathbf{e}_k$. Analogously, if $s = k+1$, a second shortest vector of $L(m, a)$ is the shortest among the two vectors $\mathbf{e}_{k-1}$ and $\mathbf{e}_k$. If either $s = k-1$ or $s = k$, we can apply just one step the Lagrange-Gauss algorithm either to the basis $(\mathbf{e}_{k-1}, \mathbf{e}_k)$ if $s = k-1$ or $(\mathbf{e}_k, \mathbf{e}_{k-1})$ if $s = k$ to obtain an optimal basis.

Table 1 Optimal basis of some satins obtained by Euclid's algorithm

m	a	k	Optimal basis
319	48	5	$(\mathbf{e}_{k-2}, \mathbf{e}_{k-1}) = (\mathbf{e}_3, \mathbf{e}_4) = ((7,17), (-13,14))$
291	113	6	$(\mathbf{e}_{k-2}, \mathbf{e}_{k}) = (\mathbf{e}_4, \mathbf{e}_6) = ((-5,17), (-18,3))$
151	20	4	$(\mathbf{e}_{k-1}, \mathbf{e}_{k-2}) = (\mathbf{e}_3, \mathbf{e}_2) = ((8,9), (-7,11))$
34	13	4	$(\mathbf{e}_{k-1}, \mathbf{e}_{k}) = (\mathbf{e}_3, \mathbf{e}_4) = ((3,5), (-5,3))$
79	9	2	$(\mathbf{e}_{k-1}, \mathbf{e}_{k+1}) = (\mathbf{e}_1, \mathbf{e}_3) = ((1,9), (9,2))$
99	41	4	$(\mathbf{e}_{k-1}, \mathbf{e}) = (\mathbf{e}_3, \mathbf{e}) = ((5,7), (-7,10))$
137	14	3	$(\mathbf{e}_{k}, \mathbf{e}_{k-2}) = (\mathbf{e}_3, \mathbf{e}_1) = ((10,3), (1,14))$
71	30	4	$(\mathbf{e}_{k}, \mathbf{e}_{k-1}) = (\mathbf{e}_4, \mathbf{e}_3) = ((-7,3), (5,8))$
175	38	4	$(\mathbf{e}_{k}, \mathbf{e}_{k+1}) = (\mathbf{e}_4, \mathbf{e}_5) = ((-9,8), (14,7))$
37	13	3	$(\mathbf{e}_{k}, \mathbf{e}) = (\mathbf{e}_3, \mathbf{e}) = ((3,2), (-5,9))$
95	11	2	$(\mathbf{e}_{k+1}, \mathbf{e}_{k-1}) = (\mathbf{e}_3, \mathbf{e}_1) = ((9,4), (-8,7))$
313	20	2	$(\mathbf{e}_{k+1}, \mathbf{e}_{k}) = (\mathbf{e}_3, \mathbf{e}_2) = ((16,7), (-15,13))$

Table 1 gives some numerical examples; the values of m, a, k and the optimal basis are shown. When the second shortest vector is not a vector of $E(m, a)$, it is denoted by $\mathbf{e}$ without subindex.

5 Square lattices

Probably square and symmetric satins are the most relevant classes of satins, and they have deserved special attention. For instance, they are the unique classes of the so-called isonemal satins (see Grünbaum and Shephard [6]), and the cited articles by Lucas study square and symmetric satins. We devote this section to square satins and the next one to symmetric satins.

A lattice L is called a *square lattice* if it satisfies one of the following three equivalent conditions:

(a) The lattice L has an optimal basis $(\mathbf{u}, \mathbf{v})$ such that $\mathbf{u} \cdot \mathbf{v} = 0$ and $\|\mathbf{u}\| = \|\mathbf{v}\|$. (Note that in this case $\|\mathbf{u}\|^2 = \|\mathbf{v}\|^2 = |\det(\mathbf{u}, \mathbf{v})|$).
(b) The lattice L is invariant by rotations of angle $\pi/2$ around any point of L.
(c) For all $(v, r) \in L$, we have $(-r, v) \in L$.

Conditions (a)–(c) are of geometric type. For satins $L(m, a)$, they are easily translated into an arithmetic condition.

Assume that a satin $L(m, a)$ is a square lattice. The condition $(1, a) \in L(m, a)$ implies $(-a, 1) \in L(m, a)$. Then $-a^2 \equiv 1 \pmod{m}$. Reciprocally, suposse that $a^2 + 1 \equiv 0 \pmod{m}$. Then $\gcd(m, a) = 1$ and

$$\begin{aligned}(v, r) \in L(m, a) &\Leftrightarrow av \equiv r \pmod{m}\\ &\Leftrightarrow v \equiv -ar \pmod{m}\\ &\Leftrightarrow (-r, v) \in L(m, a).\end{aligned}$$

Thus, if $a^2 + 1 \equiv 0 \pmod{m}$, then $L(m, a)$ is a square lattice. Therefore, a square satin is a satin $L(m, a)$ such that $a^2 + 1 \equiv 0 \pmod{m}$. See the example in Fig. 3.

Historically, the main interest was to find m such that there exist steps a giving squared satins. In arithmetic terms, the problem is to find m such that -1 is a quadratic residue modulus m. It is well known that such m are those with a factorization in product of primes of the form $m = 2^{\alpha_0} p_1^{\alpha_1} \dots p_k^{\alpha_k}$ with $\alpha_0 \in \{0, 1\}$ and

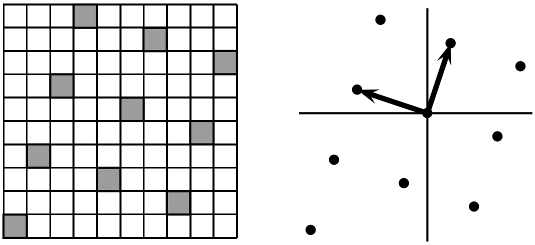

Fig. 3 The draft and an optimal basis of the square lattice L (10, 3)

$p_i \equiv 1 \pmod 4$. Our goal here is to show that if $L(m, a)$ is a square lattice, then the extended Euclid's algorithm gives an optimal basis.

We have the following characterization of square lattices in terms of the penultimate vector of the Euclid's algorithm.

Lemma 5.1 *Let* $\mathbf{e}_i = (v_i, r_i)$, $i \in \{0, \dots, n+1\}$ *be the vectors of* $E(m, a)$. *Assume that* $a < m/2$. *Then the lattice* $L(m, a)$ *is a square lattice if and only if* $v_n = -a$. *In this case*, n *is even.*

Proof Assume that $L(m, a)$ is a square lattice. From the Bézout identity $u_n m + v_n a = 1$ and $a^2 + 1 = xm$ for some integer x, we obtain $u_n m + v_n a = 1 = xm - a^2$ and $(u_n - x)m = -a(a + v_n)$. Since $\gcd(m, a) = 1$, it follows that m divides $|a + v_n|$, that is, $|a + v_n| = mq$ for some integer q. By Theorem 2.1 (xii), we have $|v_n| \leq m/2$. Then,

$$mq = |a + v_n| \leq a + |v_n| < m/2 + m/2 = m.$$

Therefore, $q = 0$ and $v_n = -a < 0$.

Reciprocally, if $v_n = -a$, from $u_n m + v_n a = r_n = 1$, we get $-a^2 \equiv 1 \pmod m$, that is $L(m, a)$ is a square lattice.

By Theorem 2.1 (vi), $v_n = -a < 0$ implies n even. □

If $a = 1$, the lattice $L(m, a)$ is a square lattice only if $m = 2$ (the plain satin) and, in this case, $((1, 1), (-1, 1))$ is an optimal basis. We left apart this case. It is immediate that for $m = 3$ and $m = 4$ there are not square satins. Moreover, as said before, it is not restrictive to assume $a < m/2$. If $m \geq 5$, for the direct twill $a = 1$ we have $a^2 + 1 \equiv 2 \pmod m$, so it is not a square lattice. Then, we can also assume $1 < a$.

Proposition 5.1 *Let* $L(m, a)$ *be a square satin with* $m \geq 5$ *and* $1 < a < m/2$, *and let* $\mathbf{e}_i = (v_i, r_i)$, $i \in \{0, \dots, n+1\}$, *be the vectors of* $E(m, a)$. *Then*:

(i) $|v_{n+1-i}| = r_i$ *for* $i \in \{0, \dots, n+1\}$.
(ii) $\|\mathbf{e}_{n+1-i}\| = \|\mathbf{e}_i\|$ *for* $i \in \{0, \dots, n+1\}$.

Proof (i) By Theorem 2.1 (xi), we have $|v_{n+1}| = m = r_0$. From Lemma 5.1, $r_1 = a = |v_n|$. By Proposition 2.1, $|v_{i-1}|$ is the remainder of dividing $|v_{i+1}|$ by $|v_i|$ and q_i is the quotient (for $i \in \{1, \dots, n\}$). Then, the remainder of dividing $r_0 = |v_{n+1}| = m$ by $r_1 = |v_n| = a$ is $r_2 = |v_{n-1}|$. By induction, $|v_{n+1-i}| = r_i$.

(ii) By (i), we have $r_{n+1-i} = |v_i|$ and $|v_{n+1-i}| = r_i$. It follows

$$\|\mathbf{e}_{n+1-i}\| = r_{n+1-i}^2 + v_{n+1-i}^2 = v_i^2 + r_i^2 = \|\mathbf{e}_i\|^2.$$

□

Theorem 5.1 *Let $L(m, a)$ be a square satin with $m \geq 5$ and $1 < a < m/2$, and let $\mathbf{e}_0, \dots, \mathbf{e}_{n+1}$ be the vectors of $E(m, a)$. Let $k = \min\{i : |v_i| > r_i\}$. Then, $k = (n+2)/2$ and $(\mathbf{e}_{k-1}, \mathbf{e}_k)$ is an optimal basis.*

Proof The number $j = n/2$ is integer since n is even. The equality $|v_{n+1-i}| = r_i$ for $i = j$ and $i = j+1$ gives $|v_{j+1}| = r_j > r_{j+1} = |v_j|$. Thus, $k = j+1 = (n+2)/2$. We have $\|\mathbf{e}_k\| = \|\mathbf{e}_{k-1}\|$. Moreover, $v_{k-1}v_k < 0$ implies

$$\mathbf{e}_{k-1} \cdot \mathbf{e}_k = v_{k-1}v_k + r_{k-1}r_k = -r_k r_{k-1} + r_{k-1}r_k = 0.$$

Hence, $(\mathbf{e}_{k-1}, \mathbf{e}_k)$ is an optimal basis. □

Example 5.1 Consider the square satin $L(65, 18)$. We calculate the vectors $\mathbf{e}_i = (v_i, r_i)$ till $|v_i| > r_i$ or, equivalently, till we obtain a pair of consecutive orthogonal vectors.

v_i	0	1	-3	4	-7
q_i		3	1	1	1
r_i	65	18	11	7	4
	11	7	4	3	

We obtain the optimal basis $((4,7), (-7,4))$. As $65 - 18 = 47$, an optimal basis of the complementary square satin $L(65, 47)$ is $((-4,7), (7,4))$.

6 Symmetric satins

A symmetric lattice is a lattice L such that for all $(x, y) \in \mathbb{Z}^2$, if $(x, y) \in L$, then $(y, x) \in L$. Geometrically, it is a lattice symmetric with respect to the line of equation $y = x$. If a satin $L(m, a)$ is a symmetric lattice, then $(1, a) \in L(m, a)$ implies $(a, 1) \in L(m, a)$ and, then, $a^2 \equiv 1 \pmod{m}$; reciprocally, if $a^2 \equiv 1 \pmod{m}$ then $\gcd(m, a) = 1$ and if $(v, r) \in L(m, a)$, we have $av \equiv r \pmod{m}$ and $v = a^2 v = ar \pmod{m}$, so $(r, v) \in L(m, a)$ and it follows that $L(m, a)$ is a symmetric lattice. Thus, a symmetric satin is a satin $L(m, a)$ such that $a^2 - 1 \equiv 0 \pmod{m}$. See the example in Fig. 4. Twills, for example, are symmetric satins.

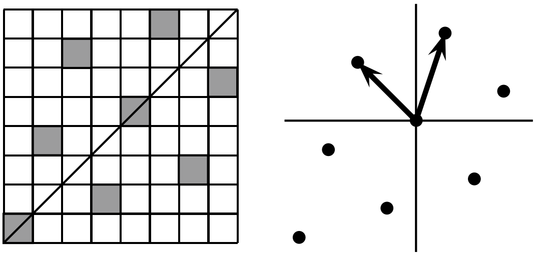

Fig. 4 The draft and an optimal basis of the symmetric satin $L(8, 3)$

A basis $(\mathbf{u}, \mathbf{v})$ of a satin is rectangular if $\mathbf{u} \cdot \mathbf{v} = 0$. Obviously, a rectangular basis is an optimal one. A satin is rectangular if it has a rectangular basis. For instance, twills with even period m are rectangular.

A basis $(\mathbf{u}, \mathbf{v})$ of a satin is rombal if $\|\mathbf{u}\| = \|\mathbf{v}\|$, that is, if the parallelogram of sides $\mathbf{u}$ and $\mathbf{v}$ is a rhombus. A satin is rombal if it has rombal basis. A satin is rombal optimal if it has a rombal optimal basis.

Twills with odd period m have optimal basis which are neither rectangular nor rombal (see Propositions 3.1 and 3.2 above). Nevertheless, they have a rombal basis: a direct twill of period m has second shortest vector $\mathbf{a} = (-(m-1)/2, (m+1)/2)$, and, by symmetry, the vector $\mathbf{b} = ((m+1)/2, -(m-1)/2)$ belongs to the twill too. Moreover, $\det(\mathbf{a}, \mathbf{b}) = m$. Thus, $(\mathbf{a}, \mathbf{b})$ is a rombal basis. Analogously, an indirect twill of period m has a rombal basis $(\mathbf{a}, \mathbf{b})$ where $\mathbf{a} = ((m+1)/2, (m-1)/2))$ and $\mathbf{b} = ((m-1)/2, (m+1)/2)$.

Next Proposition gives examples of rombal optimal basis.

Proposition 6.1 *If* $4 \le a < m-1$, *then* $((1, a), (a, 1))$ *is an optimal basis of the satin* $L(m, a)$ *if and only if* $a^2 - 1 = m$.

Proof If $m = a^2 - 1$, then the satin $L(m, a)$ is symmetric and $(1, a), (a, 1) \in L(m, a)$. Moreover $\det((a, 1), (1, a)) = a^2 - 1 = m$. Hence, $((a, 1), (1, a))$ is a basis. If we apply the Lagrange–Gauss algorithm to this basis, at the first step we heve

$$h = \left\lfloor \frac{2a}{a^2+1} \right\rceil.$$

Now, $a \ge 4$ implies $2a/(a^2+1) \le 1/2$. It follows $h = 0$ and we conclude that the basis $(1, a)$, $(a, 1)$ is optimal. Reciprocally, if $((a, 1), (1, a))$ is a basis, then $m = |\det((a, 1), (1, a))| = a^2 - 1$. □

Remark 6.1 For $a = 3$ and $m = a^2 - 1 = 8$, it is esay to see that the basis $((3, 1), (1, 3))$ is not optimal (the optimal one is $((-2, 2), (1, 3))$). Thus, the bound $4 \le a$ in the Proposition 6.1 is sharp.

It is known that every symmetric satin is rectangular or rombal. Grünbaum and Shepard give a sketch of the proof in [6]. Next, we provide a detailed proof with the goal to obtain, not only the classification, but also an optimal basis, and discriminate when a rombal basis is optimal or not. At the end of the section, we relate these results with the Euclid's algorithm.

The plain $L(2, 1)$ has optimal basis $((1, 1), (-1, 1))$, that is rectangular and rombal, so we exclude this case of the discussion.

Lemma 6.1 *Let* $L(m, a)$ *be a symmetric satin with* $m > 2$, *and set*

$$d = \gcd(m, a+1), \qquad \text{and} \qquad m_1 = m/d.$$

Then, we have:

(i) *The vectors* $\mathbf{d} = (d, d)$ *and* $\mathbf{m_1} = (-m_1, m_1)$ *are in* $L(m, a)$.

(ii) *If* m *is even, then* d *is even and* $\mathbf{w} = (d/2, d/2) \in L(m, a)$ *if and only if* $a^2 - 1 \equiv 0 \pmod{2m}$.

(iii) *If* m *is even and* $a^2 - 1 \not\equiv 0 \pmod{2m}$ *or if* m *is odd, then* $x_1 = (d + m_1)/2$ *is an integer and the vectors* $\mathbf{u} = (d - x_1, x_1)$ *and* $\mathbf{v} = (x_1, d - x_1)$ *are in* $L(m, a)$.

Proof (i) Due to the Bézout identity, one has $um + v(a + 1) = d$ for certain integers u and v. It follows $av + v \equiv d \pmod{m}$. Then, $ad \equiv a(av + v) = a^2v + av \equiv v + av \equiv d$, thus $\mathbf{d} = (d, d) \in L(m, a)$.

Let $a_1 = (a + 1)/d$. We have $(a + 1)m_1 = a_1 d m_1 = a_1 m \equiv 0 \pmod{m}$. Then, $a(-m_1) = -am_1 \equiv m_1 \pmod{m}$ and $\mathbf{m_1} = (-m_1, m_1) \in L(m, a)$.

(ii) Since $\gcd(m, a) = 1$, if m is even, then a is odd and $a + 1$, $a - 1$ and d are even. We have the following equivalences:

$$\begin{aligned}
\mathbf{w} = (d/2, d/2) \in L(m, a) &\Leftrightarrow a\frac{d}{2} \equiv \frac{d}{2} \pmod{m}\\
&\Leftrightarrow (a-1)\frac{d}{2} \equiv 0 \pmod{m}\\
&\Leftrightarrow \frac{a-1}{2} \equiv 0 \pmod{m/d}\\
&\Leftrightarrow a_1\frac{a-1}{2} \equiv 0 \pmod{m/d}\\
&\Leftrightarrow \frac{a+1}{d}\cdot\frac{a-1}{2} \equiv 0 \pmod{m/d}\\
&\Leftrightarrow a^2 - 1 \equiv 0 \pmod{2m}.
\end{aligned}$$

(iii) We shall see that $x_1 = (d + m_1)/2$ is an integer and also that $ax_1 \equiv d - x_1 \pmod{m}$. Note that $d - x_1 = (d - m_1)/2$.

Consider first the case when m is even and $a^2 - 1 \not\equiv 0 \pmod{2m}$; that is, m is even and $a^2 - 1 = qm$ with q an odd integer. We claim that m_1 is even. Indeed,

$$a - 1 = \frac{qm}{a+1} = \frac{qdm_1}{da_1} = \frac{qm_1}{a_1}$$

implies $qm_1 = (a - 1)a_1$. Since $a - 1$ is even, we have that $qm_1 = (a - 1)a_1$ is even, but q is odd. Hence, m_1 is even.

Also, note that from the equality $qm_1 = (a - 1)a_1$ and $\gcd(m_1, a_1) = 1$, it follows $a_1 | q$. Thus, a_1 is odd.

Because d and m_1 are even, the number $x_1 = (d + m_1)/2$ is an integer. We shall see that $ax_1 \equiv d - x_1 \pmod{m}$. From $ad \equiv d \pmod{m}$, it follows $(a - 1)d = \alpha m$ for some integer α. Multiplying by $a + 1$, we get $(a^2 - 1)d = \alpha(a + 1)m$. Then, $qmd = \alpha a_1 dm$, and $q = \alpha a_1$. As q is odd, α is odd too. Analogously, from $am_1 \equiv -m_1 \pmod{m}$ we get $(a + 1)m_1 = \beta m$ for some integer β. Dividing by m_1, we obtain $a + 1 = \beta d$ and $\beta = (a + 1)/d = a_1$, which is odd. Now, α and β are odd, so $\alpha + \beta$ is even, say $\alpha + \beta = 2\gamma$. Then adding, $ad = d + \alpha m$ and $am_1 = -m_1 + \beta m$ we obtain $a(d + m_1) = d - m_1 + (\alpha + \beta)m = d - m_1 + 2\gamma m$ and dividing by 2,

$$ax_1 = a\frac{d+m_1}{2} = \frac{d-m_1}{2} + \gamma m \equiv \frac{d-m_1}{2} = d - x_1 \pmod{m}. \tag{6.1}$$

Consider now the case when m is odd. Then, d and m_1 are odd and $d + m_1$ is even, so $x_1 = (d + m_1)/2$ is an integer. The congruences $ad \equiv d \pmod{m}$ and $am_1 \equiv -m_1 \pmod{m}$ imply $a(d + m_1) - (d - m_1) = \alpha m$ for some integer α. Because d and m_1 are odd, the numbers $d + m_1$ and $d - m_1$ are even and αm is even. But m is odd, hence, α must be even say $\alpha = 2\gamma$. Then, like in (6.1), we have $ax_1 = d - x_1$.

Thus, in both cases, we have that $\mathbf{v} = (x_1, d - x_1)$ and $\mathbf{u} = (d - x_1, x_1)$ are vectors of $L(m, a)$. □

Associated with a symmetric satin $L(m, a)$, we define the parameters and vectors of Lemma 6.1:

$$d = \gcd(m, a+1), \quad \mathbf{d} = (d, d).$$
$$m_1 = m/d, \quad \mathbf{m_1} = (-m_1, m_1).$$
$$\text{If m is even and } a^2 - 1 \equiv 0 \pmod{2m}, \quad \mathbf{w} = (d/2, d/2).$$
$$\text{If m is even and } a^2 - 1 \not\equiv 0 \pmod{2m}, \text{ or if m is odd },$$
$$x_1 = (d + m_1)/2, \quad \mathbf{u} = (d - x_1, x_1), \quad \mathbf{v} = (x_1, d - x_1).$$

Under the above conditions, the following properties are immediate.

(i) $\mathbf{u} + \mathbf{v} = \mathbf{d}$, $\mathbf{u} - \mathbf{v} = \mathbf{m}_1$.

(ii) $\|\mathbf{d}\|^2 = 2d^2$, $\|\mathbf{m_1}\|^2 = 2m_1^2$, $\|\mathbf{u}\|^2 = \|\mathbf{v}\|^2 = (d^2 + m_1^2)/2$.

(iii) $\det(\mathbf{u}, \mathbf{d}) = \det(\mathbf{u}, \mathbf{m}_1) = \det(\mathbf{v}, \mathbf{u}) = m$. In particular, $(\mathbf{d}, \mathbf{u})$, $(\mathbf{m_1}, \mathbf{u})$ and $(\mathbf{v}, \mathbf{u})$ are basis of $L(m, a)$.

(iv) $\mathbf{d} \cdot \mathbf{u} = d^2$, $\mathbf{m_1} \cdot \mathbf{u} = m_1^2$, $\mathbf{u} \cdot \mathbf{v} = (d^2 - m_1^2)/2$.

Lemma 6.2 *The unique symmetric satin with $d = m_1$ is the direct twill of period $m = 4$.*

Proof The condition $d = m_1 = m/d$ implies $m = d^2$. The condition $\mathbf{d} \in L(m, a)$ implies $ad \equiv d \pmod{d^2}$, so $a \equiv 1 \pmod{d}$. Then, $a + 1 = 2 + pd$ for some integer p. Since d divides $a + 1$, we have $d|2$. Hence, $d = 1$ or $d = 2$. If $d = 1$, then $m = d^2 = 1$, a contradiction. If $d = 2$ then $m = 4$, and the condition $2 = d = \gcd(a + 1, m) = (a + 1, 4)$ implies $a = 1$. □

Plane and twill satins have been considered above. Next theorem considers symmetric satins other than plain and twills, so $m \geq 5$ and $1 < a < m - 1$.

Theorem 6.1 *Let $L(m, a)$ be a symmetric satin with $m \geq 5$ and $m - 1 > a > 1$.*

(i) *If m is even and $a^2 - 1 \equiv 0 \pmod{2m}$, then the satin is rectangular. In this case, d is even and $d/2 \neq m_1$. Moreover, an optimal rectangular basis is $(\mathbf{w}, \mathbf{m_1})$ if $d/2 < m_1$ or $(\mathbf{m_1}, \mathbf{w})$ if $m_1 < d/2$.*

(ii) *If m is even and $a^2 - 1 \not\equiv 0 \pmod{2m}$, or if m is odd, then $(\mathbf{u}, \mathbf{v})$ is a rombal basis of $L(m, a)$. In this case, $(\mathbf{d}, \mathbf{u})$ and $(\mathbf{m_1}, \mathbf{u})$ are basis too, the three vectors $\mathbf{d}$, $\mathbf{m_1}$ and $\mathbf{u}$ have different norm, and if $\mathbf{e}$ denotes the one with smallest norm, exactly one of the three cases hold:*

(ii.1) $\mathbf{e} = \mathbf{d}$, $3d^2 < m_1^2$, *and* $(\mathbf{d}, \mathbf{u})$ *is an optimal basis.*

(ii.2) $\mathbf{e} = \mathbf{m_1}$, $3m_1^2 < d^2$, *and* $(\mathbf{m_1}, \mathbf{u})$ *is an optimal basis.*

(ii.3) $\mathbf{e} = \mathbf{u}$, $m_1^2 < 3d^2$, $d^2 < 3m_1^2$, *and* $(\mathbf{u}, \mathbf{v})$ *is an optimal rombal basis.*

Proof (i) By hypothesis, $a^2 - 1 \equiv 0 \pmod{2m}$, so $\mathbf{w} = (d/2, d/2) \in L(m, a)$. We have seen that $\mathbf{m_1} = (-m_1, m_1) \in L(m, a)$. The vectors $\mathbf{w}$ and $\mathbf{m_1}$ are in $L(m, a)$, they are orthogonal and $\det(\mathbf{w}, \mathbf{m_1}) = dm_1/2 + dm_1/2 = dm_1 = m$. Thus, they form a rectangular (and optimal) basis. If $d/2 < m_1$, the shortest vector is $\mathbf{w}$ and the optimal basis is $(\mathbf{w}, \mathbf{m_1})$; if $m_1 < d$, the shortest vector is $\mathbf{m_1}$ and an optimal basis is $(\mathbf{m_1}, \mathbf{w})$. The condition $d/2 = m_1$ is not possible: in this case, $d/2 \equiv a(d/2) = am_1 \equiv -m_1 = -d/2$ and we obtain $d \equiv 0 \pmod{m}$. Then, $m = d \leq a + 1 < m$, a contradiction.

(ii) The vectors $\mathbf{u}$ and $\mathbf{v}$ belong to $L(m, a)$, have the same norm, and $\det(\mathbf{v}, \mathbf{u}) = m$. Therefore, $(\mathbf{u}, \mathbf{v})$ is a rombal basis. Also, we have noticed that $(\mathbf{d}, \mathbf{u})$, $(\mathbf{u}, \mathbf{m_1})$ are basis too. (But $\det(\mathbf{d}, \mathbf{m_1}) = 2dm_1 = 2m$, so $(\mathbf{d}, \mathbf{m_1})$ is not a basis.)

We check that the three norms

$$\|\mathbf{d}\|^2 = 2d^2, \quad \|\mathbf{m}_1\|^2 = 2m_1^2, \quad \|\mathbf{u}\|^2 = \frac{1}{2}(d^2 + m_1^2)$$

are different. Indeed, $\|\mathbf{d}\| = \|\mathbf{m_1}\|$ is not possible by Lemma 6.2. The equality $\|\mathbf{d}\| = \|\mathbf{u}\|$ implies $3d^2 = m_1^2$, but m_1^2 is a square and $3d^2$ is not; thus, $\|\mathbf{d}\| \neq \|\mathbf{u}\|$. Finally, $\|\mathbf{m_1}\| = \|\mathbf{u}\|$ implies $3m_1^2 = d^2$, also a contradiction. Note the equivalences

$$\begin{array}{lll} \mathbf{e} = \mathbf{d} & \Leftrightarrow\ d < m_1 \text{ and } 3d^2 < m_1^2 & \Leftrightarrow\ 3d^2 < m_1^2 \\ \mathbf{e} = \mathbf{m_1} & \Leftrightarrow\ m_1 < d \text{ and } 3m_1^2 < d^2 & \Leftrightarrow\ 3m_1^2 < d^2 \\ \mathbf{e} = \mathbf{u} & \Leftrightarrow\ m_1^2 < 3d^2 \text{ and } d^2 < 3m_1^2. & \end{array}$$

If $\mathbf{e} = \mathbf{d}$, we have

$$\mathbf{d} \cdot \mathbf{u} = d^2 \quad \text{and} \quad h = \left\lfloor \frac{\mathbf{d} \cdot \mathbf{u}}{\|\mathbf{d}\|^2} \right\rceil = \left\lfloor \frac{d^2}{2d^2} \right\rceil = \left\lfloor \frac{1}{2} \right\rceil = 0.$$

Then, $(\mathbf{d}, \mathbf{u})$ is an optimal basis.

If $\mathbf{e} = \mathbf{m}_1$, we have,

$$\mathbf{m}_1 \cdot \mathbf{u} = m_1^2 \quad \text{i} \quad h = \left\lfloor \frac{\mathbf{m}_1 \cdot \mathbf{u}}{\|\mathbf{m}_1\|^2} \right\rceil = \left\lfloor \frac{m_1^2}{2m_1^2} \right\rceil = \left\lfloor \frac{1}{2} \right\rceil = 0.$$

Then, $(\mathbf{m}_1, \mathbf{u})$ is an optimal basis.

If $\mathbf{e} = \mathbf{u}$, we have

$$(d^2 + m_1^2)/2 = \|\mathbf{u}\|^2 < \|\mathbf{d}\|^2 \le 2d^2 \quad \Leftrightarrow \quad m_1^2 < 3d^2. \tag{6.2}$$

and

$$(d^2 + m_1^2)/2 = \|\mathbf{u}\|^2 < \|\mathbf{m_1}\|^2 \le 2m_1^2 \quad \Leftrightarrow \quad d^2 < 3m_1^2. \tag{6.3}$$

Then,

$$\mathbf{u} \cdot \mathbf{v} = \frac{1}{2}(d^2 - m_1^2) \quad \textit{and} \quad h = \left\lfloor \frac{\mathbf{u} \cdot \mathbf{v}}{\|\mathbf{u}\|^2} \right\rceil = \left\lfloor \frac{(d^2 - m_1^2)/2}{(d^2 + m_1^2)/2} \right\rceil = \left\lfloor \frac{d^2 - m_1^2}{d^2 + m_1^2} \right\rceil.$$

To show that $h = 0$, it suffices to proof that

$$\left| \frac{d^2 - m_1^2}{d^2 + m_1^2} \right| < \frac{1}{2}$$

or, equivalently, $2|d^2 - m_1^2| < d^2 + m_1^2$. If $d > m_1$, this condition is equivalent to $2(d^2 - m_1^2) < d^2 + m_1^2$ and to $d^2 < 3m_1^2$, which holds by (6.3). Analogously, if $m_1 > d$, the condition is equivalent to $2(m_1^2 - d^2) < d^2 + m_1^2$ and to $m_1^2 < 3d^2$, which holds by (6.2). Therefore, we conclude that $h = 0$ and that $(\mathbf{u}, \mathbf{v})$ is an optimal rombal basis. □

Example 6.1 Consider the symmetric satin $L(36, 17)$. Since $a^2 - 1 = 288 \equiv 0 \pmod{2 \cdot 36}$, it is a rectangular satin. The parameters are $d = \gcd(m, a + 1) = \gcd(36, 18) = 18$ and $m_1 = m/d = 36/18 = 2$. Then, $\mathbf{w} = (d/2, d/2) = (9, 9)$ and $\mathbf{m_1} = (-2, 2)$. The optimal basis is $(\mathbf{m_1}, \mathbf{u})$.

Example 6.2 Consider the symmetric satin $L(8, 5)$. The period m is even, but $a^2 - 1 = 24 \not\equiv 0 \pmod{16}$. The satin is rombal. The parameters are $d = \gcd(m, a + 1) = \gcd(8, 6) = 2$, $m_1 = m/d = 4$, and $x_1 = (d + m_1)/2 = 6/2 = 3$. The rombal basis is $(\mathbf{u}, \mathbf{v})$ with $\mathbf{u} = (d - x_1, x_1) = (-1, 3)$ and $\mathbf{v} = (3, -1)$. As $3d^2 = 12 < 16 = m_1^2$, the optimal basis is $(\mathbf{d}, \mathbf{u}) = ((2, 2), (-3, 1))$.

Example 6.3 Consider the symmetric satin $L(15, 4)$. The period m is odd, so it is a rombal satin. We have $d = \gcd(m, a + 1) = \gcd(15, 5) = 5$, $m_1 = m/d = 3$ and $x_1 = (d + m_1)/2 = 8/2 = 4$. The rombal basis is $(\mathbf{u}, \mathbf{v}) = ((11, 4), (4, 11))$. As $d^2 = 25 < 27 = 3m_1^2$, and $m_1^2 = 9 < 75 = 3m_1^2$, the optimal basis is the rombal one.

Next, we turn to the Euclid's algorithm again. Next Lemma and Proposition show certain properties of the vectors of $E(m, a)$ for a symmetric satin. We skip the proofs because they are very similar to those of Lemma 5.1 and Proposition 5.1, respectively.

Lemma 6.3 *Let* $\mathbf{e}_i = (v_i, r_i)$, $i \in \{0, \dots, n + 1\}$, *be the vectors of* $E(m, a)$. *Then the lattice* $L(m, a)$ *is a symmetric lattice if and only if* $v_n = a$. *In this case*, n *is odd.*

Proposition 6.2 *Let $L(m, a)$ be a symmetric satin with $1 < a < m/2$ and let $\mathbf{e}_i = (v_i, r_i)$, $i \in \{0, \dots, n+1\}$, be the vectors of $E(m, a)$. Then, we have:*

(i) $|v_{n+1-i}| = r_i$ *for* $i \in \{0, \dots, n+1\}$.
(ii) $|v_j| = r_j$ *for* $j = (n+1)/2$.
(iii) $\|\mathbf{e}_{n+1-i}\| = \|\mathbf{e}_i\|$ *for* $i \in \{0, \dots, n+1\}$.

Theorem 6.2 *Let $L(m, a)$ be a symmetric satin with $1 < a < m/2$ and let $\mathbf{e}_i = (v_i, r_i)$, $i \in \{0, \dots, n+1\}$, be the vectors of $E(m, a)$. Let $k = \min\{i : |v_i| > r_i\}$. Then, we have:*

(i) $k = (n+3)/2$.
(ii) *If* $\mathbf{e}_{k-2}$ *is a shortest vector, then* $(\mathbf{e}_{k-2}, \mathbf{e}_k)$ *is an optimal rombal basis of* $L(m, a)$.

Proof (i) By Proposition 6.2, if $j = (n+1)/2$ we have $|v_j| = r_j$. Hence $k = j + 1 = (n+3)/2$.

(ii) If $\mathbf{e}_{k-2}$ is the shortest vector, then $\|\mathbf{e}_k\| = \|\mathbf{e}_{k-2}\|$ and $\mathbf{e}_k$ is a shortest vector too. Then, one has

$$\|\mathbf{e}_k\|^2 = \|\mathbf{e}_{k-2}\|^2 + q_{k-1}^2\|\mathbf{e}_{k-1}\|^2 - 2q_{k-1}\mathbf{e}_{k-2} \cdot \mathbf{e}_{k-1}.$$

Simplifying, and using that $\mathbf{e}_{k-2}$ and $\mathbf{e}_{k-1}$ are linear independent, we get

$$q_{k-1}\|\mathbf{e}_{k-1}\|^2 = 2|\mathbf{e}_{k-2} \cdot \mathbf{e}_{k-1}| < 2|\|\mathbf{e}_{k-1}\|^2.$$

Thus, $q_{k-1} = 1$ and

$$|\det(\mathbf{e}_{k-2}, \mathbf{e}_k)| = |\det(\mathbf{e}_{k-2}, \mathbf{e}_k - \mathbf{e}_{k-1})| = |\det(\mathbf{e}_{k-2}, \mathbf{e}_{k-1})| = m.$$

This means that $(\mathbf{e}_{k-2}, \mathbf{e}_k)$ is a rombal optimal basis. □

Acknowledgements We are grateful to Carles Lladó, whose knowledge of satins and their mathematical models has been an inspiration for this work. We would also like to thank Jordi Nadal for sharing his extensive knowledge of fabrics with us. Finally, we thank the referee for his/her valuable comments and suggestions.

Funding Open Access funding provided thanks to the CRUE-CSIC agreement with Springer Nature.

References

1. Cerruti, F.: Nuovo metodo per la classificazione dei tessuti. L'Ingegneria Civile e le Arti Industriali, Anno V, Num. **10**, 157–159 (1870)
2. Crowe, D.W.: The Mosaic patterns of H. J. Woods. Comp. Math. Appl. **12B**(Nos. I/2), 407–411 (1986)
3. Galbraith, S. D.: Mathematics of public key cryptography. Version 2.0. https://www.math.auckland.ac.nz/~sgal018/crypto-book/main.pdf (2018). Accessed 18 Sept 2020
4. Gand, E.: Nouvelles méthodes de construction des satins réguliers, pairs et impairs. 1-Théorie des nombres premiers appliqueé aux pointés de ces armures. Bull. Soc. Ind. Amiens. 57–88 (1867)
5. Gand, E.: Nouvelles méthodes de construction des satins réguliers, pairs et impairs. 2-Armures-tissu – Armures-dessin – Mosaïques. Bull. Soc. Ind. Amiens. 257–300 (1867)
6. Grünbaum, B., Shephard, G.C.: An introduction to the geometry of fabrics. Math. Mag. **53**(3), 139–161 (1980)
7. Grünbaum, B., Shephard, G.C.: An extension to the catalogue of isonemal fabrics. Discret. Math. **60**, 155–192 (1986)
8. Hoffstein, J., Pipher, J., Silverman, J.H.: An introduction to mathematical cryptography. Undergraduate Texts on Mathematics, Springer, Berlin (2008)
9. Lucas, E.: Aplication de l'arithmétique a la construction de l'armure des satins réguliers. Gustave Retaux, Librairie-Éditeur. Paris (1867)
10. Lucas, E.: Principii fondamentali della geometria dei tessuti. L'Ingegneria Civile e le Arti Industriali. Geometria Aplicata All'Industria. Anno VI, Num. **7**, 104–111 (1880)
11. Lucas, E.: Principii fondamentali della geometria dei tessuti. Appendice. L'Ingegneria Civile e le Arti Industriali. Geometria Aplicata All'Industria. Anno VI, Num. **8**, 113–115 (1880)
12. Shoup, V.A.: Computational introduction to number theory and algebra, (Version 2). https://shoup.net/ntb/ntb-v2.pdf. (2008) Accessed 18 Sept 2020
13. Shorter, S.A.: The mathematical theory of the sateen arrangement. Math. Gaz. **10**(147), 92–97 (1920)
14. Woods, H.J.: 19-The geometrical basis of pattern design. Part I. Points and line symmetry in simple figures and borders. J. Text. Inst. **26**, T197–T210 (1935). (**Transactions**)
15. Woods, H.J.: 25-The geometrical basis of pattern design. Part II. Nets and sateens. J. Text. Inst. **26**, T293–T308 (1935). (**Transactions**)
16. Woods, H.J.: 28-The geometrical basis of pattern design. Part III. Geometrical symmetry in plane patterns. J. Text. Inst. **26**, T341–T357 (1935). (**Transactions**)
17. Woods, H.J.: 29-The geometrical basis of pattern design. Part IV. Countercharge symmetry in plane patterns. J. Text. Inst. **27**, T305–T320 (1936). (**Transactions**)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.