A CLASS OF FIBONACCI IDEAL LATTICES IN $\mathbb{Z}[\zeta_{12}]$

Michele Elia
Dipartimento di Elettronica, Politecnico di Torino, Corso Duca degli Abruzzi 24, I-10129 Torino, Italy

J. Carmelo Interlando*
Departamento de Matemática, Universidade Estadual Paulista - UNESP
Rua Cristóvão Colombo, 2265, 15054-000, São José do Rio Preto, SP, Brazil
(Submitted April 2001-Final Revision July 2001)

1. INTRODUCTION

Lattices occur in many different areas of science and engineering. They are used to define dense sphere packings in n-dimensional spaces [5], and direct applications of them are found in number theory, in particular, to solve Diophantine equations [1]. There are further applications found in numerical analysis, for example, when evaluating n-dimensional integrals [5, p. 11-12]. In modern digital communication systems, lattice constellations are used to send encoded information through noisy channels, [3, 5, 10]. In this application, lattices with dense sphere packings are desirable. Recently it has been shown that algebraic lattices (those originating from rings of integers via canonical embedding of number fields) can be linearly labeled by elements of a finite field, facilitating the encoding and decoding processes [6]. From the mid-nineties on, concrete applications of lattices began appearing in cryptography [9]. In particular, the NP-hardness of the famous lattices shortest vector problem, namely the problem of finding a lattice point nearest to the origin, was proved by Ajtai [2] in 1997. Similar tools were used to study the hardness of the most significant bits of the secret keys in the Diffie-Hellman and related schemes in prime fields [9, p. 14]. Recall the Diffie-Hellman key exchange protocol: Alice and Bob fix a finite cyclic group G and a generator g. They respectively pick random $a, b \in [1, |G|]$ and exchange g^a and g^b. The secret key is g^{ab}. An interesting realization of this public key exchange is based on quadratic number fields with large class number [8, p. 261] where the cyclic group is provided by the class groups. Proving the security of the Diffie-Hellman protocal has been a challenging problem in cryptography.

It has long been known that several dense lattices are algebraic and, in particular, originate from ideals in rings of integers. We refer to these lattices as *ideal lattices*. Remarkably, the densest four-dimensional lattice, namely D_4, is generated by the ideal $(1-\zeta_8)\mathbb{Z}[\zeta_8]$ where ζ_8 is a primitive eighth root of unity. A good measure of packing density is the center density, defined as the ratio between the lattice density (the proportion of the maximum space that is occupied by nonoverlapping spheres centered in lattice points) and the volume of a sphere of radius one [5, p. 13].

Let $\mathbb{F}$ be an algebraic number field generated by a root of $m(x)$, an irreducible polynomial of degree n over $\mathbb{Q}$. Let us assume that $m(x)$ has r_1 real roots and $2r_2$ complex roots. The center density γ of an ideal lattice of $\mathbb{F}$ is given by

$$\gamma = \left(\frac{d_m}{2}\right)^n \frac{1}{N_{\mathbb{F}}(\mathcal{J})\sqrt{d(\mathbb{F})/2^{2r_2}}}$$

*This work has been supported by the Fundação de Amparo à Pesquisa do Estado de São Paulo-FAAESP, under grant 99/02695-7, Brazil.

where $d(\mathbb{F})$ is the field discriminant, $N_{\mathbb{F}}(\mathcal{J})$ is the ideal norm, and d_m^2 is the minimum square Euclidean distance between lattice points, see [5, p. 10] or [7, Exercise 2.43]. D_4 is the only four-dimensional lattice possessing a center density equal to $\frac{1}{8}$, [5, p.9], the maximum achievable in that dimension. On the other hand, in this paper we exhibit a sequence of lattice (Λ_n) generated by principal ideals $(F_n - \zeta_{12}F_{n+2})\mathbb{Z}[\zeta_{12}]$ in $\mathbb{Z}[\zeta_{12}]$ whose center densities approach $\frac{1}{8}$ asymptotically. The sequence (z_n) of complex numbers where $z_n = F_n - \zeta_{12}F_{n+2}$, $z_0 = -\zeta_{12}$, and $z_1 = 1 - 2\zeta_{12}$ satisfies Fibonacci's recurrence (see [4]), and so we refer to Λ_n as *Fibonacci ideal lattices.* We show that the center density γ_n of Λ_n is a rational number $\frac{\delta_n^2}{48\cdot\Delta_n}$ which approaches $\frac{1}{8}$ asymptotically as n goes to infinity. The integers δ_n and Δ_n satisfy two linear recurring sequences related to Fibonacci and Lucas numbers. The theta series [5, p.45] $\Theta_{\Lambda_n}(z) = \sum_{x\in\Lambda_n} q^{x\cdot x}$, where z is a complex variable and $q = e^{\pi i z}$, is an expression made of Jacobi theta functions. The Λ_n are definitively different from D_4 because the respective kissing numbers are 12 and 24. The kissing number of a sphere packing in any dimension is defined as the number of spheres that touch one sphere [5]. Given a lattice Λ in $\mathbb{R}^N$ with minimum distance d_m, we can think of the points of Λ as being centers of equal nonoverlapping N-spheres of radius $d_m/2$. Then the kissing number of Λ is the kissing number of this packing just described. Notice that the theta series of Λ provides us with the kissing number τ of Λ, since $\Theta(z) = 1 + \tau q^{d_m^2} + \ldots$ [5].

The following sequences related to Fibonacci and Lucas numbers will be used in the proofs:

$$a_n = F_n^2 + F_{n+2}^2 = \frac{1}{5}(3L_{2n+2} + 4(-1)^{n+1}); \tag{1}$$

$$b_n = F_nF_{n+2} = F_{n+1}^2 + (-1)^{n+1} = \frac{1}{5}(L_{2n+2} + 3(-1)^{n+1}); \tag{2}$$

$$a_n - 3b_n = (-1)^n. \tag{3}$$

The golden section $\omega = \frac{1+\sqrt{5}}{2}$ and $\overline{\omega} = 1 - w$ are the roots of $x^2 - x - 1$ [11].

2. CENTER DENSITY

An integral basis for the ring $\mathbb{Z}[\zeta_{12}]$ is $\mathcal{B} = \{1, \zeta_{12}, \zeta_{12}^2, \zeta_{12}^3\}$ where ζ_{12} is a root of the clyclotomic polynomial $x^4 - x^2 + 1$. A real embedding σ yields the generator matrix of Λ_0

$$B_0 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ \frac{\sqrt{3}}{2} & \frac{1}{2} & -\frac{\sqrt{3}}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{\sqrt{3}}{2} & \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ 0 & 1 & 0 & 1 \end{bmatrix}.$$

A generator matrix B_n of Λ_n is obtained as the product $B_0M(z_n)$, where $M(z_n)$ belongs to an integral matrix representation of $\mathbb{Z}[\zeta_{12}]$ with respect to basis $\mathcal{B}$. We have

$$M(\zeta_{12}) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 1 & 0 \end{bmatrix}, \qquad M(z_n) = \begin{bmatrix} F_n & -F_{n+2} & 0 & 0 \\ 0 & F_n & -F_{n+2} & 0 \\ 0 & 0 & F_n & -F_{n+2} \\ F_{n+2} & 0 & -F_{n+2} & F_n \end{bmatrix},$$

and

$$B_n = B_0M(z_n) = \begin{bmatrix} F_n & -F_{n+2} & F_n & -F_{n+2} \\ \frac{\sqrt{3}}{2}F_n + \frac{1}{2}F_{n+2} & -\frac{\sqrt{3}}{2}F_{n+2} + \frac{1}{2}F_n & -F_{n-2} - \frac{\sqrt{3}}{2}F_n & \frac{\sqrt{3}}{2}F_{n+2} + \frac{1}{2}F_n \\ -\frac{\sqrt{3}}{2}F_{n+2} + \frac{1}{2}F_n & \frac{\sqrt{3}}{2}F_n - \frac{1}{2}F_{n+2} & \frac{1}{2}F_n & -\frac{\sqrt{3}}{2}F_n - \frac{1}{2}F_{n+2} \\ F_{n+2} & F_n & -2F_{n+2} & F_n \end{bmatrix}$$

The squared Euclidean norm in Λ_n is given by the quadratic form $Q(x) = x^T B_n^T B_n x$ with $x \in \mathbb{Z}^4$. The positive definite symmetric matrix of this quadratic form results in

$$A_n = B_n^T B_n = \begin{bmatrix} 2(F_n^2 + F_{n+2}^2) & -3F_nF_{n+2} & F_n^2 + F_{n+2}^2 & 0 \\ -3F_nF_{n+2} & 2(F_n^2 + F_{n+2}^2) & -3F_nF_{n+2} & F_n^2 + F_{n+2}^2 \\ F_n^2 + F_{n+2}^2 & -3F_nF_{n+2} & 2(F_n^2 + F_{n+2}^2) & -3F_nF_{n+2} \\ 0 & F_n^2 + F_{n+2}^2 & -3F_nF_{n+2} & 2(F_n^2 + F_{n+2}^2) \end{bmatrix}.$$

Writing $Q(x) = x^T A_n x = x^T (U^{-1})^T U^T A_n U U^{-1} x = x^T (U^{-1})^T C_n U^{-1} x$, we consider the transformation of A_n by the matrices

$$U = \begin{bmatrix} 1 & 0 & -\frac{1}{2} & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -\frac{1}{2} & 0 & 1 \end{bmatrix} \quad \text{and} \quad U^{-1} = \begin{bmatrix} 1 & 0 & \frac{1}{2} & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & \frac{1}{2} & 0 & 1 \end{bmatrix},$$

to produce a block diagonal matrix

$$C_n = \begin{bmatrix} 2(F_n^2 + F_{n+2}^2) & -3F_nF_{n+2} & 0 & 0 \\ -3F_nF_{n+2} & \frac{3}{2}(F_n^2 + F_{n+2}^2) & 0 & 0 \\ 0 & 0 & \frac{3}{2}(F_n^2 + F_{n+2}^2) & -3F_nF_{n+2} \\ 0 & 0 & -3F_nF_{n+2} & 2(F_n^2F_{n+2}) \end{bmatrix}.$$

Thus, setting $g_n = 2a_n^2 + 2(-1)^n a_n - 1$ and making use of the identity (3), $Q(x)$ is written as a linear combination of four squares

$$Q(x) = \frac{1}{2a_n}\{[a_n(2x_1+x_3-x_2)+(-1)^n x_2]^2+g_n x_2^2+g_n x_3^2+[a_n(2x_4+x_2-x_3)+(-1)^n x_3]^2\}. \quad (4)$$

This expression is conveniently written as $Q(x) = Q(x_1, x_3, x_2) + Q(x_4, x_2, x_3)$, by defining

$$Q(u_1, u_2, u_3) = \frac{1}{2a_n}\{[a_n(2u_1 + u_2 - u_3) + (-1)^n u_3]^2 + g_n u_3^2\}.$$

The center density γ_n of a Fibonacci ideal lattice is $\gamma_n = \frac{d_m^4}{4N_{\mathbb{F}}(z_n)\sqrt{d(\mathbb{F})}}$, where $d(\mathbb{F}) = 144$, the norm of the principal ideal $z_n\mathbb{Z}[\zeta_{12}]$ is the field norm of z_n

$$N_{\mathbb{F}}(z_n) = \Delta_n = F_n^4 - F_n^2F_{n+2}^2 + F_{n+2}^4 = a_n^2 - 3b_n^2,$$

and, given (4), the squared minimum distance is

$$d_m^2 = \delta_n = 2(F_n^2 + F_{n+2}^2) - (1 - (-1)^n) = 2a_n - 1 + (-1)^n. \quad (5)$$

Therefore,

$$\gamma_n = \frac{[2a_n - (1 - (-1)^n)]^2}{16 \cdot [3a_n^2 - 9b_n^2]} = \frac{[2a_n - (1 - (-1)^n)]^2}{48 \cdot [2a_n^2 + 2(-1)^n a_n - 1]} = \frac{\delta_n^2}{48 \cdot \Delta_n} \asymp \frac{1}{8} + O\left(\frac{1}{a_n}\right),$$

where the asymptotic expression shows that the convergence is exponential as n goes to infinity. Some initial terms are

$$\gamma_0 = \frac{1}{12}, \gamma_1 = \frac{4}{39}, \gamma_2 = \frac{25}{219}, \gamma_3 = \frac{196}{1623}, \gamma_4 = \frac{5329}{43212}, \gamma_5 = \frac{37249}{299532}, \gamma_6 = \frac{255025}{2044236}.$$

Sequence Δ_n. The sequence $\Delta_n = F_n^4 - F_n^2F_{n+2}^2 + F_{n+2}^4 = (F_n^2 + F_{n+2}^2)^2 - 3F_n^2F_{n+2}^2$ satisfies a fifth order linear recurrence

$$\Delta_{n+5} = 5\Delta_{n+4} + 15\Delta_{n+3} - 15\Delta_{n+2} - 5\Delta_{n+1} + \Delta_n,$$

with initial values $\Delta_0 = 1$, $\Delta_1 = 13$, $\Delta_2 = 73$, $\Delta_3 = 541$, and $\Delta_4 = 3601$. In fact, the equation

$$\Delta_n = \frac{1}{25}[6L_{2n+2}^2 + 6L_{2n+2}(-1)^{n+1} + 25]$$

$$= \frac{1}{25}[6(\omega^4)^{n+1} + 6(\overline{\omega}^{\,4})^{n+1} + 6(-\omega^2)^{n+1} + 6(-\overline{\omega}^{\,2})^{n+1} + 27]$$

shows that $\omega^4, \overline{\omega}^4, -\omega^2, -\overline{\omega}^2$, and 1 are the roots of

$$g_\Delta(x) = (x^2 - L_4x + 1)(x^2 + L_2x + 1)(x - 1) = x^5 - 5x^4 - 15x^3 + 15x^2 + 5x - 1,$$

which is a characteristic polynomial of a fifth order linear recurrence.

Sequence δ_n. The squared minimum distance $d_m^2(n) = \delta_n = 2a_n - (1 - (-1)^n)$ satisfies a fourth order recurrence

$$\delta_{n+4} = 3\delta_{n+3} - 3\delta_{n+1} + \delta_n,$$

with initial values $\delta_0 = 2, \delta_1 = 8, \delta_2 = 20$, and $\delta_3 = 56$. In fact, the equation

$$\delta_n = \frac{6}{5}L_{2n+2} - \frac{3}{5}(-1)^n - 1 = \frac{1}{5}[6(\omega^2)^{n+1} + 6(\overline{\omega}^2)^{n+1} - 3(-1)^n - 5]$$

shows that $\omega^2, \overline{\omega}^2, -1$, and 1 are the roots of

$$g_\delta(x) = (x^2 - L_2x + 1)(x + 1)(x - 1) = (x^2 - 3x + 1)(x + 1)(x - 1) = x^4 - 3x^3 + 3x - 1,$$

which is a characteristic polynomial of a fourth order linear recurrence.

3. THETA SERIES

In Chapter 4 of [5], Conway and Sloane describe basic techniques for theta series manipulations. Their enlightening example of the hexagonal lattice [5, p. 110] helps us to study Λ_0. This lattice has the following theta series

$$\Theta_{\Lambda_0}(q) = 1 + 12q^2 + 36q^4 + 12q^6 + 84q^8 + 72q^{10} + 36q^{12} + \ldots$$

which is obtained using the quadratic form with symmetric matrix

$$A_0 = \begin{bmatrix} 2 & 0 & 1 & 0 \\ 0 & 2 & 0 & 1 \\ 1 & 0 & 2 & 0 \\ 0 & 1 & 0 & 2 \end{bmatrix}.$$

A direct computation yields

$$\Theta_{\Lambda_0}(q) = \sum_{x \in \Lambda_0} q^{x \cdot x} = \sum_{x \in \Lambda_0} q^{2(x_1^2 + x_3^2 + x_1x_3 + x_2^2 + x_4^2 + x_2x_4)} = \left(\sum_{x_1, x_3 \in \mathbb{Z}} q^{2(x_1^2 + x_3^2 + x_1x_3)} \right)^2 = \Theta_{\Lambda_{exa}}^2(q^2).$$

Furthermore, it is known [5, p. 111] that

$$\Theta_{\Lambda_{exa}}(q) = \theta_2(z)\theta_2(3z) + \theta_3(z)\theta_3(3z), \tag{6}$$

where $\theta_i(z) = \theta_i(0|z), i = 2, 3$, are Jacobi theta functions with $q = e^{\pi i z}$.

Theorem 1 *For every n, the theta series of Λ_n*

$$\Theta_{\Lambda_n}(q) = \sum_{x \in \mathbb{Z}^4} q^{x^T U^{-1} C_n (U^T)^{-1} x} = \sum_{x_1, x_2, x_3, x_4 \in \mathbb{Z}} q^{Q(x_1, x_3, x_2) + Q(x_4, x_2, x_3)}$$

can be written in the following form

$$\Theta_{\Lambda_n}(q) = \Theta_{00}(n, q)^2 + \Theta_{01}(n, q)^2 + 2\Theta_{11}(n, q) \cdot \Theta_{10}(n, q), \tag{7}$$

where $\Theta_{r_3 r_2}(n, q), r_2, r_3 \in \{0, 1\}$ can be expressed in terms of Jacobi theta functions

$$\theta_1(\xi|z) = \theta_2(\xi - \frac{\pi}{2}|z), \quad \theta_2(\xi|z) = \sum_{m=-\infty}^{\infty} e^{(2m+1)i\xi + i\pi z(m+\frac{1}{2})^2}$$

$$\theta_3(\xi|z) = \sum_{m=-\infty}^{\infty} e^{2im\xi + i\pi z m^2}, \text{ and } \theta_4(\xi|z) = \theta_3(\xi + \frac{\pi}{2}|z).$$

Proof: In $Q(x_1, x_3, x_2)$ and $Q(x_4, x_2, x_3)$, the expressions $2x_1 + x_3 - x_2$ and $2x_4 - x_3 + x_2$ are even numbers if x_3 and x_2 have the same parity, otherwise they are odd. Setting $x_2 = 2z_2 + r_2$ and $x_3 = 2z_3 + r_3$, where $r_2, r_3 \in \{0, 1\}$ and $z_2, z_3 \in \mathbb{Z}$, we have

$$Q(x_1, x_3, x_2) = \frac{1}{2a_n}[(a_n(2[x_1 + z_3 - z_2] + r_3) + 2z_2 + r_2)^2 + g_n(2z_2 + r_2)^2]$$

$$Q(x_4, x_2, x_3) = \frac{1}{2a_n}[(a_n(2[x_4 + z_2 - z_3] + r_2) + 2z_3 + r_3)^2 + g_n(2z_3 + r_3)^2].$$

The transformation $m_1 = x_1 + z_3 - z_2, m_2 = z_2, m_3 = z_3$, and $m_4 = x_4 + z_2 - z_3$ is unimodular, thus for r_3 and r_2 fixed in

$$Q(x_1, x_3, x_2) = \frac{1}{2a_n}[(a_n(2m_1 + r_3 - r_2) + 2m_2 + r_2)^2 + g_n(2m_2 + r_2)^2]$$

$$Q(x_4, x_2, x_3) = \frac{1}{2a_n}[(a_n(2m_4 + r_2 - r_3) + 2m_3 + r_3)^2 + g_n(2m_3 + r_3)^2],$$

the four variables m_1, m_2, m_3, m_4 range independently over $\mathbb{Z}$. Therefore (7) is obtained defining

$$\Theta_{r_3 r_2}(n,q) = \sum_{m_1,m_2\in\mathbb{Z}} q^{\frac{1}{2a_n}[(a_n(2m_1+r_3-r_2)+2m_2+r_2)^2+g_n(2m_2+r_2)^2]} \quad r_2, r_3 = 0, 1.$$

Now, setting $m_2 = a_n m + r$ and $\ell = m_1 + m$, with $r \in \{0, 1, \ldots, a_n - 1\}$, we obtain

$$\Theta_{r_3 r_2}(n,q) = \sum_{r=0}^{a_n-1} \sum_{m_1,\ell\in\mathbb{Z}} q^{\frac{1}{2a_n}[(a_n(2\ell+r_3-r_2)+2r+r_2)^2+g_n(2a_n m+2r+r_2)^2]} \quad r_2, r_3 = 0, 1.$$

The infinite sums

$$\sum_{m_1,\ell\in\mathbb{Z}} q^{\frac{1}{2a_n}[(a_n(2\ell+r_3-r_2)+2r+r_2)^2+g_n(2a_n m+2r+r_2)^2]} \quad r_2, r_3 = 0, 1, \quad r = 0, \ldots, a_n - 1$$

are actually products of Jacobi theta functions. This will be proved considering the exponent of q as a sum of three terms

$$E_1 = 2a_n\ell^2 + 2(a_n r_3 + 2r + r_2)\ell$$
$$E_2 = 2a_n g_n m^2 + 2g_n(2r + r_2)m$$

$$E_3 = \frac{a_n r_3^2}{2} + (a_n + (-1)^n)(2r + r_2)^2 + r_3(2r + r_2).$$

Assuming $q = e^{\pi i z}$, from [5, p. 103] we have

$$\sum_{m=-\infty}^{\infty} q^{2mB+Am^2} = \sum_{m=-\infty}^{\infty} e^{2\pi i m B z + \pi i z A m^2} = \theta_3(\pi B z | A z) = (-iAz)^{-1/2} e^{\frac{\pi B^2 z}{iA}} \theta_3\left(\frac{\pi B}{A} | -\frac{1}{Az}\right).$$

Therefore, two forms for $\Theta_{r_3 r_2}(n,q)$ are possible, based on either of the two forms occurring in Poisson-Jacobi identity, that is,

$$\frac{-1}{2a_n\sqrt{g_n}z} \sum_{r=0}^{a_n-1} \theta_3\left(\pi\frac{a_n r_3 + 2r + r_2}{2a_n} | \frac{-1}{2a_n z}\right) \theta_3\left(\pi\frac{2r + r_2}{2a_n} | \frac{-1}{2a_n g_n z}\right)$$

and

$$\sum_{r=0}^{a_n-1} \theta_3(\pi z(a_n r_3+2r+r_2)|2a_n z)\theta_3(\pi g_n z(2r+r_2)|2a_n g_n z) e^{\pi i z(\frac{a_n r_3^2}{2}+(a_n+(-1)^n)(2r+r_2)^2+r_3(2r+r_2))}. \quad \square$$

For example, taking $n \equiv 0, 1 \bmod 3$ we get four fairly symmetric expressions for $\Theta_{ij}(n,q)$ in terms of Jacobi theta functions. With the restriction on n, a_n is odd, therefore $-(2r+1)[(a_n-1)/2]$ runs over a full remainder set along with r. Thus, using the properties $\theta_4(\xi|z) = \theta_3(\xi + \frac{\pi}{2}|z)$ and $\theta_3(\xi + \pi|z) = \theta_3(\xi|z)$ [12], we obtain

$$\Theta_{00}(n,q) = \frac{-1}{2a_n\sqrt{g_n}z} \sum_{r=0}^{a_n-1} \theta_3\left(\pi\frac{r}{a_n}|\frac{-1}{2a_nz}\right)\theta_3\left(\pi\frac{r}{a_n}|\frac{-1}{2a_ng_nz}\right)$$

$$\Theta_{01}(n,q) = \frac{-1}{2a_n\sqrt{g_n}z} \sum_{r=0}^{a_n-1} \theta_4\left(\pi\frac{r}{a_n}|\frac{-1}{2a_nz}\right)\theta_4\left(\pi\frac{r}{a_n}|\frac{-1}{2a_ng_nz}\right)$$

$$\Theta_{10}(n,q) = \frac{-1}{2a_n\sqrt{g_n}z} \sum_{r=0}^{a_n-1} \theta_4\left(\pi\frac{r}{a_n}|\frac{-1}{2a_nz}\right)\theta_3\left(\pi\frac{r}{a_n}|\frac{-1}{2a_ng_nz}\right)$$

$$\Theta_{11}(n,q) = \frac{-1}{2a_n\sqrt{g_n}z} \sum_{r=0}^{a_n-1} \theta_3\left(\pi\frac{r}{a_n}|\frac{-1}{2a_nz}\right)\theta_4\left(\pi\frac{r}{a_n}|\frac{-1}{2a_ng_nz}\right).$$

4. CONCLUDING REMARKS

We conclude with an example and a few remarks on open problems related to the construction of n-dimensional lattices with maximum center density.

Fibonacci ideal lattices have been used to design good signal constellations for sending information over communication channels [6]. The goal is to choose a constellation of M points in a space of dimension n with maximum normalized minimum squared distance $\kappa = \frac{d^2_{\min}}{E_{\text{av}}} \log_2 M$, where E_{av} is the average squared norm of the points of the constellation, and $d^2_{\min}$ is the minimum squared distance between points of the constellation. For example, the ideal $(2-5\zeta_{12})\mathbb{Z}[\zeta_{12}]$ may be used to construct a constellation of 37 points. A basis for Λ, the lattice generated by $\mathbb{Z}[\zeta_{12}]$, is given by the rows of the following matrix:

$$B = \begin{bmatrix} 1 & 0 & 1 & 0 \\ \frac{\sqrt{3}}{2} & \frac{1}{2} & -\frac{\sqrt{3}}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{\sqrt{3}}{2} & \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ 0 & 1 & 0 & 1 \end{bmatrix},$$

whereas a basis for the Fibonacci ideal lattice Λ_3 is obtained by left multiplying B by the matrix associated to the ideal $(2 - 5\zeta_{12})$

$$\begin{bmatrix} 2 & -5 & 0 & 0 \\ 0 & 2 & -5 & 0 \\ 0 & 0 & 2 & -5 \\ 5 & 0 & -5 & 2 \end{bmatrix}.$$

The center densities of Λ and Λ_3 are $\gamma = 0.0833$ and $\gamma_3 = 0.1207$ respectively.

The rational prime 37 splits in $\mathbb{Z}[\zeta_{12}]$ as $37 = p_1p_2p_3p_4$, where $p_1 = \langle -1 + 2\zeta_{12} + 2\zeta_{12}^2 \rangle$, and the other primes p_2, p_3, and p_4 are obtained by conjugation, namely, substituting ζ_{12} with $\zeta_{12}^5, \zeta_{12}^7$, and ζ_{12}^{11} respectively. Thus, the set of 37 elements modulo p_1 is $\mathbb{Z}[\zeta_{12}]$ is a field isomorphic to $\mathbb{Z}_{37}$ the set of remainders modulo 37. The following table

ℓ	x_1	x_2	x_3	x_4	ℓ	x_1	x_2	x_3	x_4	ℓ	x_1	x_2	x_3	x_4
0	0	0	0	0	1	1	0	0	0	2	−2	−1	1	1
3	−1	−1	1	1	4	0	0	−1	−1	5	1	0	−1	−1
6	0	0	0	1	7	−1	−1	0	0	8	0	−1	0	0
9	−1	−1	1	2	10	0	0	−1	0	11	1	0	−1	0
12	0	−1	−1	−1	13	−1	−1	0	1	14	0	−1	0	1
15	1	0	−2	−1	16	1	2	0	−1	17	−1	−1	−1	0
18	0	−1	−1	0	19	0	1	1	0	20	1	1	1	0
21	−1	−2	0	1	22	−1	0	2	1	23	0	1	0	−1
24	1	1	0	−1	25	0	1	1	1	26	−1	0	1	0
27	0	0	1	0	28	1	1	−1	−2	29	0	1	0	0
30	1	1	0	0	31	0	0	0	−1	32	−1	0	1	1
33	0	0	1	1	34	1	1	−1	−1	35	2	1	−1	−1
36	−1	0	0	0										

identitifies the constellations where a point with coordinates (x_1, x_2, x_3, x_4) in different bases, namely, $\mathcal{B}_1 = \{1, \zeta_{12}\zeta_{12}^2, \zeta_{12}^3\}$ and $\mathcal{B}_2 = \{-1 + 2\zeta_{12} + 2\zeta_{12}^2, -\zeta_{12} + 2\zeta_{12}^2 - 2\zeta_{12}^2 + 2\zeta_{12}^3, -2 + \zeta_{12}^2 + 2\zeta_{12}^3, -2 - 2\zeta_{12} + 2\zeta_{12}^2 + \zeta_{12}^3\}$, receives the same label $\ell = x_1 - 8x_2 + (-8)^2x_2 - 8^3x_3 = x_1 + 29x_2 + 27x_2 + 6x_3 \mod 37$. The maximum normalized minimum squared distances of constellations with 37 points in Λ and Λ_3 are $\kappa = 3.21$ and $\kappa_3 = 3.98$ respectively.

In dimension four, we have seen that an ideal lattice with maximum center density exists along with a class of ideal lattices achieving the same maximal density asymptotically. For a given m-dimensional space, it would be interesting to ascertain whether the maximum center

density is achievable finitely or asymptotically. The theta series $\Theta_{\Lambda_n}(q)$ of a Fibonacci ideal lattice can be expressed by means of Jacobi theta functions. It is also of interest to know whether $\Theta_{\Lambda_n}(q)$ can be expressed in terms of a finite initial set of theta series $\Theta_{\Lambda_0}, \ldots, \Theta_{\Lambda_s}$.

5. ACKNOWLEDGMENT

The authors wish to thank the anonymous referee for suggestions that led to an improvement in paper readability.

REFERENCES

[1] K. Aardal, C.A.J. Hurkens, and A.K. Lenstra. "Solving a System of Diophantine Equations with Lower and Upper Bounds on the Variables." *Mathematics of Operations Research* **25** (2000): 427-442.

[2] M. Ajtai. "The Shortest Vector Problem in L_2 is NP-hard for Randomized Reductions." *Proc. of 30th STOC.* ACM, 1998.

[3] I.F. Blake. "The Leech Lattice as a Code for the Gaussian Channel." *Informaiton and Control* **19.1** (1971): 66-74.

[4] Brother A. Brousseau. *Linear Recursion and Fibonacci Sequences*, The Fibonacci Association, San Jose Calif., 1971.

[5] J.H. Conway and N.J.A. Sloane. *Sphere Packings, Lattices and Groups*, New York: Springer-Verlag, 1988.

[6] J.C. Interlando, M. Elia, and T.P. da Nóbrega Neto. "On the Optimality of Finite Constellations from Algebraic Lattices." *Electronic Journal on Discrete Mathematics*, Proceedings of WCC2001, Paris, January 2001, 201-210.

[7] R.A. Mollin. *Algebraic Number Theory* Boca Raton, FL: Chapman & Hall/CRC, 1999.

[8] R.A. Mollin. *Quadratics*, Boca Raton, FL: Chapman & Hall/CRC 1996.

[9] P.Q. Nguyen and J. Stern. "Lattice Reduction in Cryptology: An Update." *Algorithmic Number Theory.* Proceedings of the 4th International Symposium, ANTS-IV, Linden, The Netherlands, July 2000. Springer-Verlag, Lecture Notes in Computer Science, Vol. 1838, W. Bosma (Ed.), 2000.

[10] N.J.A. Sloane. "A Note on the Leech Lattice as a Code for the Gaussian Channel." *Information and Control* **46** (1980): 270-272.

[11] S. Vajda. *Fibonacci and Lucas Numbers, and the Golden Section.* New York: Wiley, 1989.

[12] E.T. Whittaker and G.N. Watson. *A Course in Modern Analysis*, Cambridge University Press, 4th ed., 1969.

AMS Classification Numbers: 11R04, 11B39

✠ ✠ ✠