Multivariate Lucas polynomials and ideal classes inquadratic number fields

AYBERK ZEYTİN

Recommended Citation

ZEYTİN, AYBERK (2018) "Multivariate Lucas polynomials and ideal classes inquadratic number fields," *Turkish Journal of Mathematics*: Vol. 42: No. 4, Article 1. https://doi.org/10.3906/mat-1608-65
Available at: https://journals.tubitak.gov.tr/math/vol42/iss4/1

Multivariate Lucas polynomials and ideal classes in quadratic number fields

Ayberk ZEYTİN[*]
Department of Mathematics, Galatasaray University, İstanbul, Turkey

Abstract: In this work, by using Pauli matrices, we introduce four families of polynomials indexed over the positive integers. These polynomials have rational or imaginary rational coefficients. It turns out that two of these families are closely related to classical Lucas and Fibonacci polynomial sequences and hence to Lucas and Fibonacci numbers. We use one of these families to give a geometric interpretation of the 200-year-old class number problems of Gauß, which is equivalent to the study of narrow ideal classes in real quadratic number fields.

Key words: Pauli matrices, Fibonacci polynomials, Lucas polynomials, çarks, çark hypersurfaces, indefinite binary quadratic forms, class number problems of Gauß, real quadratic number fields, narrow ideal classes

1. Introduction

A number field, K, is a finite extension of $\mathbf{Q}$. Elements of K that are roots of monic polynomials with integral coefficients form a subring of K called the *ring of integers* of K, denoted by $\mathbf{Z}_K$. Being an extension of $\mathbf{Z}$, $\mathbf{Z}_K$ shares many properties with $\mathbf{Z}$. However, determining for which K $\mathbf{Z}_K$ is a unique factorization domain (which is in this case equivalent to being a principal ideal domain) is one of the most fundamental open questions of algebraic number theory. A measure for this property is the class number of K, denoted h_K, that is the order of the ideal class group $H(K)$, which is the multiplicative group of ideals of $\mathbf{Z}_K$ modulo the subgroup of principal ideals. The class number $h_K = 1$ if and only if $\mathbf{Z}_K$ is a unique factorization domain.

As $\mathbf{Z}_K$ is a Dedekind domain, every fractional ideal of K can be generated by at most two elements. Hence, one has a map from projectivized ordered pairs of elements of $\mathbf{Z}_K$, which is a group under ideal multiplication denoted by $H^+(K)$, to H_K. This map is bijective exactly when $\mathbf{Z}_K$ admits a unit of norm -1. Otherwise, this map becomes a 2-to-1 map and the group $H^+(K)$ is called the *narrow class group*. Analogously, the order of $H^+(K)$, denoted $h^+(K)$, is called the *narrow class number*.

Let us now restrict the extension degree to 2, i.e. consider the quadratic case. Any such number field K is equal to $\mathbf{Q}(\sqrt{d})$ for some square-free integer d. In this case, both the narrow class group and the class group are computed using the corresponding binary quadratic forms of Gauß [4]. Whenever $d > 0$, K is called real quadratic, and whenever $d < 0$, K is called imaginary. In fact, for the imaginary quadratic case Gauß determined "almost" all such number fields with class number one. It turns out that $\mathbf{Z}_K$ is a principal ideal domain if and only if $d \in \{-3, -4, -7, -8, -11, -19, -43, -67, -163\}$. However, the question of determining real quadratic number fields of class number one is still open and is referred to as the class number one problem

---

[*]Correspondence: azeytin@gsu.edu.tr

of Gauß. It must be noted that the number of such number fields is expected to be infinite.

In this paper, we introduce four families of multivariate polynomials named A_k, B_k, C_k, and D_k. This work is focused on studying the family A_k, though we point out properties of the remaining three polynomial families, too. For instance, we will see that the polynomial family B_k is closely related to Fibonacci polynomials. The family A_k will be called multivariate Lucas polynomials. This naming stems from the fact that if one reduces these polynomials to one variable, then the classical Lucas polynomials are obtained. A similar phenomenon occurs for the family B_k; that is, they restrict to classical Fibonacci polynomials. Our main motivation for introducing such a family of polynomials is that given any real quadratic number field K we use multivariate Lucas polynomials to define an affine surface, called the *çark surface* of K, whose integral points are in one-to-one correspondence with narrow ideal classes in K. This allows us to access the more than 200 years old class number problems of Gauß from a completely different point of view. Indeed, çark surfaces produce high degree projective surfaces, which are conjecturally Kobayashi hyperbolic. By a conjecture of Lang they have finitely many **Q**-rational points. The reader is suggested to consult [13] and the references therein for further details on this point of view.

This paper is organized as follows: the next section is devoted to defining and establishing basic properties of the aforementioned polynomial sequences. In particular, multivariate Lucas and Fibonacci polynomials are defined. In the last section, after a quick review of narrow ideal classes and the narrow ideal class group of a quadratic number field, we define the automorphism group of a narrow ideal class. In the real quadratic case, this group is isomorphic to **Z** generated by a hyperbolic element of $\mathrm{PSL}_2(\mathbf{Z})$. Using this we attach an infinite bipartite ribbon graph, called çark in a joint work of the author with Uludağ and Durmuş [11], to a narrow ideal class and show how they give rise to integral points of an appropriate affine surface.

2. Multivariate Lucas and Fibonacci polynomials

In this section, we will introduce four families of polynomials, A_k, B_k, C_k, and D_k, indexed over positive integers. These polynomials have either rational or imaginary rational coefficients. The second part is devoted to listing certain properties that will be required in upcoming sections.

2.1. The families A_k, B_k, C_k, and D_k

Pauli matrices, which have proven themselves to be useful tools in the context of quantum mechanics, are defined as

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 0 & -\sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

They are of order two and satisfy $\sigma_1 \sigma_2 \sigma_3 = \sqrt{-1}$. They are traceless and their determinant is -1; hence, their eigenvalues are ± 1.

Together with the identity matrix Pauli matrices form a basis for the vector space of matrices of size 2×2 with complex entries. In particular, for the matrix $M(x, y) = \begin{pmatrix} 1 + xy & x \\ y & 1 \end{pmatrix}$ with x and y being complex variables, the coefficients of I, σ_1, σ_2, and σ_3 become $A = \frac{1}{2}(2 + xy)$, $B = \frac{1}{2}(x + y)$, $C = \frac{\sqrt{-1}}{2}(x - y)$, and $D = \frac{xy}{2}$, respectively. More generally, for a sequence of even number of complex numbers $x_1, y_1, \ldots, x_k, y_k$ we define

$$M(x_1, y_1, \ldots, x_k, y_k) := M(x_1, y_1) \cdot \ldots \cdot M(x_k, y_k).$$

Then there should exist polynomials $A_k, B_k, C_k,$ and D_k in $x_1, y_1, \ldots, x_k, y_k$ so that

$$M = A_k \cdot I + B_k \cdot \sigma_1 + C_k \cdot \sigma_2 + D_k \cdot \sigma_3.$$

For instance, for $M(x_1, y_1, x_2, y_2)$, one finds immediately that

$$A_2(x_1, y_1, x_2, y_2) = \frac{1}{2}(2 + (x_1 + x_2)(y_1 + y_2) + x_1 x_2 y_1 y_2),$$

$$B_2(x_1, y_1, x_2, y_2) = \frac{1}{2}((x_1 + x_2) + (y_1 + y_2) + x_2 y_1(x_1 + y_2)),$$

$$C_2(x_1, y_1, x_2, y_2) = \frac{\sqrt{-1}}{2}((x_1 + x_2) - (y_1 + y_2) + x_2 y_1(x_1 - y_2)),$$

$$D_2(x_1, y_1, x_2, y_2) = \frac{1}{2}(x_1(y_1 + y_2) - x_2(y_1 - y_2) + x_1 x_2 y_1 y_2).$$

The four families of polynomials satisfy the following recursive relations:

$$A_{k+1}^{1,2,\ldots,k+1} = A_k^{1,2,\ldots,k} A_1^{k+1} + B_k^{1,2,\ldots,k} B_1^{k+1} + C_k^{1,2,\ldots,k} C_1^{k+1} + D_k^{1,2,\ldots,n} D_1^{k+1}$$

$$B_{k+1}^{1,2,\ldots,k+1} = B_k^{1,2,\ldots,k} A_1^{k+1} + A_k^{1,2,\ldots,k} B_1^{k+1} + \sqrt{-1}(C_k^{1,2,\ldots,k} D_1^{k+1} - D_k^{1,2,\ldots,n} C_1^{k+1})$$

$$C_{k+1}^{1,2,\ldots,k+1} = C_k^{1,2,\ldots,k} A_1^{k+1} + A_k^{1,2,\ldots,k} C_1^{k+1} + \sqrt{-1}(D_k^{1,2,\ldots,k} B_1^{k+1} - B_k^{1,2,\ldots,n} D_1^{k+1})$$

$$D_{k+1}^{1,2,\ldots,k+1} = D_k^{1,2,\ldots,k} A_1^{k+1} + A_k^{1,2,\ldots,k} D_1^{k+1} + \sqrt{-1}(B_k^{1,2,\ldots,k} C_1^{k+1} - C_k^{1,2,\ldots,n} B_1^{k+1});$$

where $A_k^{i_1,i_2,\ldots,i_k}$ stands for $A_k(x_{i_1}, y_{i_1}, \ldots, x_{i_k}, y_{i_k})$. This set of relations can be obtained directly from the relations among Pauli matrices. It must be pointed out that this is not the only set of equations that define the families $A_k, B_k, C_k,$ and D_k. In fact, if we let $p(k)$ denote the number of partitions of the positive integer k, then there are $\frac{1}{2}p(k)$-many different such formulations.

We refer to Tables 1, 2, 3, and 4 for the first four members of these families, in which to avoid rational coefficients we multiplied each polynomial by 2.

Table 1. First few members of the family A_k.

$2A_1$	$x_1 y_1 + 2$
$2A_2$	$x_1 x_2 y_1 y_2 + x_1 y_1 + x_2 y_1 + x_1 y_2 + x_2 y_2 + 2$
$2A_3$	$x_1 x_2 x_3 y_1 y_2 y_3 + x_1 x_2 y_1 y_2 + x_2 x_3 y_1 y_2 + x_1 x_2 y_1 y_3 + x_1 x_3 y_1 y_3 + x_1 x_3 y_2 y_3 +$ $x_2 x_3 y_2 y_3 + x_1 y_1 + x_2 y_1 + x_3 y_1 + x_1 y_2 + x_2 y_2 + x_3 y_2 + x_1 y_3 + x_2 y_3 + x_3 y_3 + 2$
$2A_4$	$x_1 x_2 x_3 x_4 y_1 y_2 y_3 y_4 + x_1 x_2 x_3 y_1 y_2 y_3 + x_2 x_3 x_4 y_1 y_2 y_3 + x_1 x_2 x_3 y_1 y_2 y_4 +$ $x_1 x_2 x_4 y_1 y_2 y_4 + x_1 x_2 x_4 y_1 y_3 y_4 + x_1 x_3 x_4 y_1 y_3 y_4 + x_1 x_3 x_4 y_2 y_3 y_4 +$ $x_2 x_3 x_4 y_2 y_3 y_4 + x_1 x_2 y_1 y_2 + x_2 x_3 y_1 y_2 + x_2 x_4 y_1 y_2 + x_1 x_2 y_1 y_3 + x_1 x_3 y_1 y_3 +$ $x_2 x_4 y_1 y_3 + x_3 x_4 y_1 y_3 + x_1 x_3 y_2 y_3 + x_2 x_3 y_2 y_3 + x_3 x_4 y_2 y_3 + x_1 x_2 y_1 y_4 +$ $x_1 x_3 y_1 y_4 + x_1 x_4 y_1 y_4 + x_1 x_3 y_2 y_4 + x_2 x_3 y_2 y_4 + x_1 x_4 y_2 y_4 + x_2 x_4 y_2 y_4 +$ $x_1 x_4 y_3 y_4 + x_2 x_4 y_3 y_4 + x_3 x_4 y_3 y_4 + x_1 y_1 + x_2 y_1 + x_3 y_1 + x_4 y_1 + x_1 y_2 +$ $x_2 y_2 + x_3 y_2 + x_4 y_2 + x_1 y_3 + x_2 y_3 + x_3 y_3 + x_4 y_3 + x_1 y_4 + x_2 y_4 + x_3 y_4 +$ $x_4 y_4 + 2$

Table 2. First few members of the family B_k.

$2B_1$	$x_1 + y_1$
$2B_2$	$x_1x_2y_1 + x_2y_1y_2 + x_1 + x_2 + y_1 + y_2$
$2B_3$	$x_1x_2x_3y_1y_2 + x_2x_3y_1y_2y_3 + x_1x_2y_1 + x_1x_3y_1 + x_1x_3y_2 + x_2x_3y_2 + x_2y_1y_2 +$ $x_2y_1y_3 + x_3y_1y_3 + x_3y_2y_3 + x_1 + x_2 + x_3 + y_1 + y_2 + y_3$
$2B_4$	$x_1x_2x_3x_4y_1y_2y_3 + x_2x_3x_4y_1y_2y_3y_4 + x_1x_2x_3y_1y_2 + x_1x_2x_4y_1y_2 +$ $x_1x_2x_4y_1y_3 + x_1x_3x_4y_1y_3 + x_1x_3x_4y_2y_3 + x_2x_3x_4y_2y_3 + x_2x_3y_1y_2y_3 +$ $x_2x_3y_1y_2y_4 + x_2x_4y_1y_2y_4 + x_2x_4y_1y_3y_4 + x_3x_4y_1y_3y_4 + x_3x_4y_2y_3y_4 +$ $x_1x_2y_1 + x_1x_3y_1 + x_1x_4y_1 + x_1x_3y_2 + x_2x_3y_2 + x_1x_4y_2 + x_2x_4y_2 + x_2y_1y_2 +$ $x_1x_4y_3 + x_2x_4y_3 + x_3x_4y_3 + x_2y_1y_3 + x_3y_1y_3 + x_3y_2y_3 + x_2y_1y_4 + x_3y_1y_4 +$ $x_4y_1y_4 + x_3y_2y_4 + x_4y_2y_4 + x_4y_3y_4 + x_1 + x_2 + x_3 + x_4 + y_1 + y_2 + y_3 + y_4$

Table 3. First few members of the family C_k.

$2C_1$	$\sqrt{-1}(x_1 - y_1)$
$2C_2$	$\sqrt{-1}(x_1x_2y_1 - x_2y_1y_2 + x_1 + x_2 - y_1 - y_2)$
$2C_3$	$\sqrt{-1}(x_1x_2x_3y_1y_2 - x_2x_3y_1y_2y_3 + x_1x_2y_1 + x_1x_3y_1 + x_1x_3y_2 + x_2x_3y_2 -$ $x_2y_1y_2 - x_2y_1y_3 - x_3y_1y_3 - x_3y_2y_3 + x_1 + x_2 + x_3 - y_1 - y_2 - y_3)$
$2C_4$	$\sqrt{-1}(x_1x_2x_3x_4y_1y_2y_3 - x_2x_3x_4y_1y_2y_3y_4 + x_1x_2x_3y_1y_2 + x_1x_2x_4y_1y_2 +$ $x_1x_2x_4y_1y_3 + x_1x_3x_4y_1y_3 + x_1x_3x_4y_2y_3 + x_2x_3x_4y_2y_3 - x_2x_3y_1y_2y_3 -$ $x_2x_3y_1y_2y_4 - x_2x_4y_1y_2y_4 - x_2x_4y_1y_3y_4 - x_3x_4y_1y_3y_4 - x_3x_4y_2y_3y_4 +$ $x_1x_2y_1 + x_1x_3y_1 + x_1x_4y_1 + x_1x_3y_2 + x_2x_3y_2 + x_1x_4y_2 + x_2x_4y_2 - x_2y_1y_2 +$ $x_1x_4y_3 + x_2x_4y_3 + x_3x_4y_3 - x_2y_1y_3 - x_3y_1y_3 - x_3y_2y_3 - x_2y_1y_4 - x_3y_1y_4 -$ $x_4y_1y_4 - x_3y_2y_4 - x_4y_2y_4 - x_4y_3y_4 + x_1 + x_2 + x_3 + x_4 - y_1 - y_2 - y_3 - y_4)$

Table 4. First few members of the family D_k.

$2D_1$	x_1y_1
$2D_2$	$x_1x_2y_1y_2 + x_1y_1 - x_2y_1 + x_1y_2 + x_2y_2$
$2D_3$	$x_1x_2x_3y_1y_2y_3 + x_1x_2y_1y_2 - x_2x_3y_1y_2 + x_1x_2y_1y_3 + x_1x_3y_1y_3 + x_1x_3y_2y_3 +$ $x_2x_3y_2y_3 + x_1y_1 - x_2y_1 - x_3y_1 + x_1y_2 + x_2y_2 - x_3y_2 + x_1y_3 + x_2y_3 + x_3y_3$
$2D_4$	$x_1x_2x_3x_4y_1y_2y_3y_4 + x_1x_2x_3y_1y_2y_3 - x_2x_3x_4y_1y_2y_3 + x_1x_2x_3y_1y_2y_4 +$ $x_1x_2x_4y_1y_2y_4 + x_1x_2x_4y_1y_3y_4 + x_1x_3x_4y_1y_3y_4 + x_1x_3x_4y_2y_3y_4 +$ $x_2x_3x_4y_2y_3y_4 + x_1x_2y_1y_2 - x_2x_3y_1y_2 - x_2x_4y_1y_2 + x_1x_2y_1y_3 + x_1x_3y_1y_3 -$ $x_2x_4y_1y_3 - x_3x_4y_1y_3 + x_1x_3y_2y_3 + x_2x_3y_2y_3 - x_3x_4y_2y_3 + x_1x_2y_1y_4 +$ $x_1x_3y_1y_4 + x_1x_4y_1y_4 + x_1x_3y_2y_4 + x_2x_3y_2y_4 + x_1x_4y_2y_4 + x_2x_4y_2y_4 +$ $x_1x_4y_3y_4 + x_2x_4y_3y_4 + x_3x_4y_3y_4 + x_1y_1 - x_2y_1 - x_3y_1 - x_4y_1 + x_1y_2 +$ $x_2y_2 - x_3y_2 - x_4y_2 + x_1y_3 + x_2y_3 + x_3y_3 - x_4y_3 + x_1y_4 + x_2y_4 + x_3y_4 + x_4y_4$

2.2. Properties

The following is a list of properties satisfied by these polynomials:

- B_k, C_k, and D_k do not have any degree 0 term. That of A_k is equal to $\frac{1}{2} \cdot 2$.

- For any integer $k > 1$ neither of the families contain a term of the form x_i^k or y_i^k.

- The families of polynomials $A_k(x, y, x, y, \ldots, x, y)$ and $D_k(x, y, x, y, \ldots, x, y)$ comprise only monomials of the form $x^l y^l$ for every $1 \le l \le k$. As a result, all monomials in A_k and D_k are of even degree.

- The families of polynomials $B_k(x, y, x, y, \ldots, x, y)$ and $C_k(x, y, x, y, \ldots, x, y)$ comprise only monomials of the form $x^l y^{l+1}$ for every $1 \leq l \leq k-1$ and $x^{l+1} y^l$ for every $1 \leq l \leq k-1$. Moreover, the number of terms of the form $x^l y^{l+1}$ is equal to the number of terms of the form $x^{l+1} y^l$. As a result, all monomials in B_k and C_k are of odd degree.

- The degrees of A_k and D_k are $2k$, whereas those of B_k and C_k are $2k - 1$.

- $2A_k, 2B_k, \frac{2}{\sqrt{-1}} C_k$, and $2D_k$ are elements of the ring $\mathbf{Z}[x_1, y_1, \ldots, x_k, y_k]$ and are irreducible in this ring.

Proofs of the facts listed above can be obtained by induction, which we leave to the reader. The proof of the following theorem exemplifies arguments involved in such proofs. For its statement let us recall that the kth Lucas polynomial, $L_k(x)$, is defined as $L_k(x) = 2^{-k}((x - \sqrt{x^2 + 4})^k + (x + \sqrt{x^2 + 4})^k)$. For $k \geq 1$, Lucas polynomials satisfy the recursion $L_{k+1}(x) = xL_k(x) + L_{k-1}(x)$, with initial conditions being $L_0(x) = 2$ and $L_1(x) = x$. The first few Lucas polynomials are $L_2(x) = x^2 + 2$, $L_3(x) = x^3 + 3x$, $L_4(x) = x^4 + 4x^2 + 2$.

Theorem 2.1 *The polynomial* $2A_k(x, x, \ldots, x)$ *is equal to the* $2k^{\text{th}}$ *Lucas polynomial, denoted by* $L_{2k}(x)$.

Proof We know that $L_{2k}(x) = xL_{2k-1}(x) + L_{2(k-1)}(x)$. Writing the same recursion formula for $L_{2k-1}(x)$, multiplying by x, and subtracting from the first, we obtain $L_{2k}(x) = (x^2 + 1)L_{2(k-1)} + xL_{2k-3}(x)$. Solving for $xL_{2k-3}(x)$ from the recursion for $L_{2(k-1)}(x)$ we finally obtain the recursion formula for the even terms in the Lucas polynomial sequence, which reads $L_{2k}(x) = (x^2 + 2)L_{2(k-1)}(x) - L_{2(k-2)}(x)$ for $k \geq 2$. On the other hand, by definition, we have $M(x, x, \ldots, x) = M(x, x)^k$. As noted above for $k = 1$, $2A = 2 + x^2$, $B = 2x$, $C = 0$, and $2D = x^2$. Suppose that $M^{k-1} = f_{k-1}(x) + Bg_{k-1}(x)\sigma_1 + Cg_{k-1}(x)\sigma_2 + Dg_{k-1}(x)\sigma_3$. If we write M^k with respect to the basis consisting of identity and the Pauli matrices then we obtain the following set of equations:

$$
\begin{aligned}
f_k(x) &= Af_{k-1}(x) + B^2 g_{k-1}(x) + C^2 g_{k-1}(x) + D^2 g_{k-1}(x)), \\
g_k(x) &= Ag_{k-1}(x) + f_{k-1}(x).
\end{aligned}
$$

We rewrite the first equality using $\det(M) = 1 = A^2 - (B^2 + C^2 + D^2)$ and get $f_k(x) = Af_{k-1}(x) + (A^2 - 1)g_{k-1}(x)$. This establishes the fact that there are polynomial families f_k and g_k indexed over the set of positive integers so that $M^k = f_k(x) + Bg_k(x)\sigma_1 + Cg_k(x)\sigma_2 + Dg_k(x)\sigma_3$. A short algebraic manipulation of these equations gives us the recurrence relation $f_{k+1}(x) = 2Af_k(x) - f_{k-1}(x)$, subject to the initial conditions of $f_0(x) = 1$ and $f_1(x) = 2A = 2 + x^2$. □

Let us remark that the above method can be applied in a slightly more general setup where one obtains polynomials f_k and g_k of A and $\det(M)$; see [5]. One may immediately ask analogous questions for the remaining polynomial families. It is immediate to prove that $C_k(x, x, \ldots, x) = 0$ for any positive integer k. The probably more interesting result is the following result, whose proof is almost identical (the only essential difference being determining the initial condition) to the proof of Theorem 2.1 and therefore will be omitted. For the statement of the theorem let us note that the kth Fibonacci polynomial is defined as $F_k(x) = 2^{-k} \frac{(x+\sqrt{x^2+4})^k - (x-\sqrt{x^2+4})^k}{\sqrt{x^2+4}}$. For $k \geq 1$ Fibonacci polynomials satisfy the recursion $F_{k+1}(x) = xF_k(x) + F_{k-1}(x)$

subject to the initial conditions $F_0(x) = 0$ and $F_1(x) = 1$. The first few Fibonacci polynomials are $F_2(x) = x$, $F_3(x) = x^2 + 1$, $F_4(x) = x^3 + 2x$.

Theorem 2.2 *The polynomial* $B_k(x, x, \ldots, x)$ *is the* $2k^{th}$ *Fibonacci polynomial, denoted by* $F_{2k}(x)$.

Encouraged by Theorem 2.1, we give the following:

Definition 2.3 *For* $k \in \mathbf{Z}_{\geq 1}$ *we call the polynomial* $2A_k$ *the* $2k^{th}$ multivariate Lucas polynomial *and denote it by* $\mathcal{L}_{2k}$. *Similarly, we define the* $2k^{th}$ multivariate Fibonacci polynomial *as* B_k *and denote it by* $\mathcal{F}_{2k}$.

To answer the analogous question for D_k we note the following:

Proposition 2.4 *For any positive integer* k *we have*

$$\frac{B_k(x, x, \ldots, x)}{2x} = \frac{D_k(x, x, \ldots, x)}{x^2}.$$

Proof [Sketch of proof.] Using the method above, one obtains a recursion formula for the polynomial $\frac{2D_k(x, x, \ldots, x)}{x}$, which is exactly the same as Fibonacci polynomials with the same initial conditions. □

Lucas numbers are defined recursively as $L_1 = 1$, $L_2 = 3$ and $L_{k+1} = L_k + L_{k-1}$. The multivariate Lucas and Fibonacci polynomial families enjoy the *expected* properties of their one variable versions, which are consequences of Theorems 2.2 and 2.1. For instance, $\mathcal{L}_{2k}(0, 0, \ldots, 0) = 2$, $\mathcal{L}_{2k}(1, 1, \ldots, 1) = L_{2k}$, where L_{2k} denotes the $2k^{\text{th}}$ Lucas number. We also have:

$$\mathcal{L}_{2k}(x_1, y_1, \ldots, x_{k-1}, y_{k-1}, 0, 0) = \mathcal{L}_{2(k-1)}(x_1, y_1, \ldots, x_{k-1}, y_{k-1}).$$

We may then obtain the following using induction:

Lemma 2.5 *For any positive integer* l *we have*

$$\mathcal{L}_{2(k+l)}(x_1, y_1, \ldots, x_k, y_k, \underbrace{0, 0, \ldots, 0, 0}_{2l-many}) = \mathcal{L}_{2k}(x_1, y_1, \ldots, x_k, y_k).$$

Fibonacci numbers are defined recusively as $F_{k+1} = F_k + F_{k-1}$ subject to the initial conditions $F_0 = 0$ and $F_1 = 1$. Similar properties hold also for the Fibonacci family $\mathcal{F}_{2k}$. Namely, $\mathcal{F}_{2k}(1, 1, \ldots, 1) = F_{2k}$, where F_{2k} stands for the $2k^{\text{th}}$ Fibonacci number. We finally have

$$\mathcal{F}_{2k}(x_1, y_1, \ldots, x_{k-1}, y_{k-1}, 0, 0) = \mathcal{F}_{2(k-1)}(x_1, y_1, \ldots, x_{k-1}, y_{k-1}).$$

We invite the reader to discover the related phenomenon for the families C_k and D_k.

The generator 1 of the group $\mathbf{Z}/k\mathbf{Z}$ acts on the ordered pair $(x_1, y_1, \ldots, x_k, y_k)$ by sending it to $(x_k, y_k, x_1, y_1, \ldots, x_{k-1}, y_{k-1})$. This action leaves $\mathcal{L}_{2k}$ invariant; that is,

$$\mathcal{L}_{2k}(1 \cdot (x_1, y_1, \ldots, x_k, y_k)) = \mathcal{L}_{2k}(x_1, y_1, \ldots, x_k, y_k). \tag{2.1}$$

Indeed, this symmetry can be seen easily by considering the action on the matrix $M(x_1, y_1, \ldots, x_k, y_k)$ and noting that the trace is invariant within a conjugacy class. This property has the consequence that for any $1 \le i \le k$:

$$\mathcal{L}_{2k}(x_1, y_1, \ldots, x_{i-1}, y_{i-1}, 0, 0, x_{i+1}, y_{i+1}, \ldots, x_k, y_k)$$
$$= \mathcal{L}_{2(k-1)}(x_1, y_1, \ldots, x_{k-1}, y_{k-1}).$$

Although B_k and C_k do not enjoy such a property, let us state, without the proof, the following symmetry of D_k:

$$1 \cdot D_k(y_1, x_1, \ldots, y_k, x_k) = D_k(x_1, y_1, \ldots, x_k, y_k).$$

3. Çark surfaces

The main aim in this section is to define çark surfaces using the multivariate Lucas polynomials and obtain a one-to-one correspondence between integral points of these surfaces and narrow ideal classes. Throughout K stands for a real quadratic number field. We will only explain the theory of narrow ideal classes in such fields, although a much more general theory exists. Interested readers may consult [6–8].

3.1. Narrow ideal classes.

For such a number field K, there is a square-free positive integer d so that $K = \mathbf{Q}(\sqrt{d})$. Since the extension degree is two its Galois group is of order 2, and for any element $\alpha \in K$, by $\overline{\alpha}$ we denote the image of α under the unique nontrivial element. The ring of integers, $\mathbf{Z}_K$, of $K = \mathbf{Q}(\sqrt{d})$ depends on d. More precisely, $\mathbf{Z}_K = 1 \cdot \mathbf{Z} + \sqrt{d} \cdot \mathbf{Z}$ whenever $d \equiv 2, 3 \mod 4$ and $\mathbf{Z}_K = 1 \cdot \mathbf{Z} + \frac{1+\sqrt{d}}{2} \mathbf{Z}$ if $d \equiv 1 \mod 4$. A subset $\mathfrak{a}$ of K is called a *fractional ideal* of $\mathbf{Z}_K$ (or K) if $\mathfrak{a}$ is a 2-dimensional $\mathbf{Z}$-module and for which there is an integer $\xi \in \mathbf{Z}$ so that $\xi\mathfrak{a} \subset \mathbf{Z}_K$. Note that the product of two fractional ideals is again a fractional ideal. The norm of a fractional ideal $\mathfrak{a}$, denoted by $N(\mathfrak{a})$, is defined as $\frac{1}{\xi^2}[\mathbf{Z}_K : \xi\mathfrak{a}]$, where $[\mathbf{Z}_K : \xi\mathfrak{a}]$ stands for the index of $\xi\mathfrak{a}$ in $\mathbf{Z}_K$. As $\xi\mathfrak{a}$ is an ideal in a Dedekind domain, there are at most two elements $\alpha, \beta \in \xi\mathfrak{a}$ so that $(\alpha, \beta) = \xi\mathfrak{a}$. In this case, we say that $\mathfrak{a} = (\frac{\alpha}{\xi}, \frac{\beta}{\xi})$ and the elements are called the generators of $\mathfrak{a}$.

For a fractional ideal $\mathfrak{a}$ generated by $\alpha, \beta \in K$, the function $f_{\mathfrak{a}}$ defined on the ideal $\mathfrak{a}$ sending any element $\nu \in \mathfrak{a}$ to $\frac{\nu\overline{\nu}}{N(\mathfrak{a})}$ is an integral valued binary quadratic form on $\mathfrak{a}$. If we write $\nu = X\alpha + Y\beta$ then we have $f_{\mathfrak{a}}(X, Y) = aX^2 + bXY + cY^2$, where $a = \frac{\alpha\overline{\alpha}}{N(\mathfrak{a})}$, $b = \frac{\alpha\overline{\beta} + \overline{\alpha}\beta}{N(\mathfrak{a})}$, and $c = \frac{\beta\overline{\beta}}{N(\mathfrak{a})}$. One finds that the discriminant of this form, $\Delta(f_{\mathfrak{a}}) := b^2 - 4ac$, is equal to $4d$ if $d \equiv 2, 3 \mod 4$ and is equal to d if $d \equiv 1 \mod 4$, i.e. is equal to the discriminant of K. Given a square-free d, the discriminant of the corresponding number field is called a *fundamental discriminant*. As a result of the choice of α and β, $f_{\mathfrak{a}}$ is integral; that is, $a, b, c \in \mathbf{Z}$ and as $d > 0$ the form $f_{\mathfrak{a}}$ is indefinite. The binary quadratic form $f_{\mathfrak{a}}$ is, in addition, *primitive*, i.e. the greatest common divisor of the coefficients a, b, and c is 1.

To avoid ambiguity caused by the ordering of generators, we say that a basis (α, β) of $\mathfrak{a}$ is oriented if $\overline{\alpha}\beta - \alpha\overline{\beta} > 0$. Any element of K of positive norm, say λ, maps an oriented basis to an oriented basis via sending (α, β) to $(\lambda\alpha, \lambda\beta)$. We define two fractional ideals $\mathfrak{a}$ and $\mathfrak{b}$ to be equivalent if there is an element $\lambda \in K$ of positive norm so that $\mathfrak{a} = \lambda\mathfrak{b}$. The set of equivalence classes of fractional ideals in K is denoted by

$H^+(K)$ and is a group under multiplication called the *narrow class group*. An element of $H^+(K)$ is denoted by $[\mathfrak{a}] = [\alpha, \beta]$ and is called a *narrow ideal class*. Note that whenever $\mathbf{Z}_K$ has a unit of norm -1, $H^+(K)$ turns out to be isomorphic to the classical ideal class group $H(K)$, or else it is a degree two extension of the class group. In either case, we say that a narrow ideal class of $[\mathfrak{a}]$ in $H^+(K)$ lies above its ideal class in $H(K)$.

We refer to [12] for details and proofs of the facts above.

3.2. Automorphisms of narrow ideal classes

The group $\mathrm{PSL}_2(\mathbf{Z})$ acts on the set of indefinite integral primitive binary quadratic forms via change of variable. The $\mathrm{PSL}_2(\mathbf{Z})$-orbit of f is denoted by $[f]$. For such a form $f(X, Y) = aX^2 + bXY + cY^2$ its stabilizer is isomorphic to $\mathbf{Z}$. We call the equation $X^2 - \Delta Z^2 = 4$ the corresponding Pell equation, where Δ is the discriminant of f. The map sending an integral solution (x, z) to the matrix $W(x, z) = \begin{pmatrix} \frac{x-zb}{2} & -cz \\ az & \frac{x+zb}{2} \end{pmatrix}$ gives a bijection from the set of integral solutions of the corresponding Pell equation and the stabilizer of f. By (x_o, z_o) we denote the solution that has the smallest positive second component among all solutions. It is called the *fundamental solution*. The matrix $W_f = W(x_o, z_o)$ is called the *fundamental automorphism* of f, which is the generator of the stabilizer of f [1, Theorem 2.5.5]. The other generator is $W_f^{-1} = W(x_o, -z_o)$. A direct result of this is the following:

Corollary 3.1 *If f is an integral primitive indefinite binary quadratic form of discriminant Δ and W is an automorphism of f, then $\mathrm{tr}(W)^2 - 4 = z^2 \Delta$ for some $z \in \mathbf{Z}$.*

If $f = f_{\mathfrak{a}}$ for some narrow ideal class $\mathfrak{a}$ of K, then an element W of the stabilizer $\langle W_f \rangle$ is called an *automorphism of* $\mathfrak{a}$ and the matrix $W(x_o, z_o)$ (with $z_o > 0$) is called the *fundamental automorphism* of $\mathfrak{a}$. We remark that the fundamental automorphism of all narrow ideal classes of K arises from the same solution; hence, the fundamental solution (x_o, z_o) is an invariant of the number field.

The two matrices $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $L = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$ generate the modular group $\mathrm{PSL}_2(\mathbf{Z})$ freely and therefore induce the isomorphism $\mathrm{PSL}_2(\mathbf{Z}) \cong \mathbf{Z}/2\mathbf{Z} * \mathbf{Z}/3\mathbf{Z}$. In particular, W_f can be written as a word in S, L, and L^2. Without loss of generality, we may assume that W_f has no cancellations.

The action of $\mathrm{PSL}_2(\mathbf{Z})$ on the set of narrow ideal classes of K is defined as $\gamma \cdot (\alpha, \beta) \mapsto (p\alpha + q\beta, r\alpha + s\beta)$, where $\gamma = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$. Note that $f_{\gamma \cdot \mathfrak{a}} = \gamma \cdot f_{\mathfrak{a}}$. The correspondence defined as $[\mathfrak{a}] \mapsto [f_{\mathfrak{a}}]$ is one-to-one; see [12, §10, Satz]. This correspondence is far from being onto as there are many primitive forms of the non-square-free discriminant. For instance, if $f = (a, b, c)$ is an indefinite binary quadratic form arising from $\mathbf{Q}(\sqrt{d})$ with d being square-free (hence, its discriminant Δ is either d or $4d$ depending on the class of $d \in \mathbf{Z}/4\mathbf{Z}$), then for any prime number $p > 2$ not dividing a, the form (a, bp, cp^2) is a primitive form of discriminant $p^2 \Delta$.

One can also prove that the correspondence $[\mathfrak{a}] \mapsto [W_{f_{\mathfrak{a}}}]$, where $[W_{f_{\mathfrak{a}}}]$ stands for the conjugacy class of the stabilizer of $f_{\mathfrak{a}}$, is one-to-one [11, Proposition 2.1]. As above, this correspondence is not surjective even when one restricts to primitive elements (i.e. elements that are not powers of other elements).

3.3. Çarks

The modular group $\mathrm{PSL}_2(\mathbf{Z})$ acts on the upper half plane $\mathfrak{h} = \{z \in \mathbf{C} \colon \mathrm{Im}(z) > 0\}$. An element $\gamma = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$ sends an element $z \in \mathfrak{h}$ to $\frac{pz+q}{rz+s} \in \mathfrak{h}$. Fixed points of the matrices S and L are $\sqrt{-1}$ and $\zeta_3 = e^{2\pi\sqrt{-1}/3}$, respectively. We mark $\sqrt{-1}$ by a $\circ$ and ζ_3 by $\bullet$. These points are on the unit circle centered at $0 \in \mathbf{C}$. The $\mathrm{PSL}_2(\mathbf{Z})$ orbit (in $\mathfrak{h}$) of the part of the circle between $\circ$ and $\bullet$ is defined as the Farey tree, which will be denoted by $\mathcal{F}$; see Figure 1.
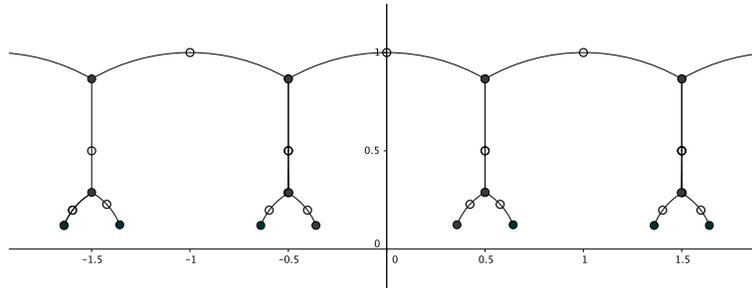

Figure 1. The Farey tree, $\mathcal{F}$.

The Farey tree is by construction bipartite and planar. Moreover, it admits a free action of $\mathrm{PSL}_2(\mathbf{Z})$ in such a fashion that edges of the Farey tree can be identified with elements of $\mathrm{PSL}_2(\mathbf{Z})$. A similar correspondence holds between vertices of type $\circ$ (resp. $\bullet$) and cosets of the torsion subgroup $\{I, S\}$ (resp. $\{I, L, L^2\}$). Hence, for any subgroup Γ of $\mathrm{PSL}_2(\mathbf{Z})$, one may talk about the quotient graph, $\Gamma\backslash\mathcal{F}$, which is again bipartite but not necessarily planar as a ribbon graph. In such a graph, every vertex of type $\bullet$ is of order 1 or 3 and every vertex of type $\circ$ is of order 1 or 2. In particular, the full quotient, $\mathrm{PSL}_2(\mathbf{Z})\backslash\mathfrak{h}$, is called the modular orbifold. Let us remark that the covering category consisting of étale covers of the modular orbifold is so rich that the whole absolute Galois group can be recovered from it; see [10]. In [9], a project that outlines a is discussed. The quotient $\mathrm{PSL}_2(\mathbf{Z})\backslash\mathcal{F}$ has only two vertices; one is $\circ$ and the other is $\bullet$ with a single edge joining the two.

The conjugation action of $\mathrm{PSL}_2(\mathbf{Z})$ on its subgroups is equivalent to the translation action of $\mathrm{PSL}_2(\mathbf{Z})$ on the set of edges of the corresponding graph, [11, Theorem 2.2]. Let us give the following:

Definition 3.2 *Let* $\mathfrak{a}$ *be a narrow ideal class in* K. *Then the graph* $\langle W_{f_{\mathfrak{a}}} \rangle\backslash\mathcal{F}$ *is called the* çark *corresponding to* $\mathfrak{a}$. *This graph is denoted by* $\mathfrak{C}_{\mathfrak{a}}$.

Similar to other correspondences stated, this is again one to one but far from being surjective, as there are çarks that come from binary quadratic forms of the non-square-free discriminant. Nevertheless, çarks that come from a narrow ideal class inherit all invariants of ideal classes and corresponding binary quadratic forms, e.g., discriminants and traces. The graph $\mathfrak{C}_{\mathfrak{a}}$ is planar, can be embedded in an annulus conformally, see[11, §3.2], and has a unique cycle called a *spine*. The number of vertices on the spine is finite and the number of vertices of type $\circ$ on the spine is equal to the number of vertices of type $\bullet$. The graph $\mathfrak{C}_{\mathfrak{a}}$ is then formed by attaching Farey trees to all vertices of type $\bullet$ on the spine so that they should expand both *inside* and *outside* the spine. Each such attached Farey tree is called a Farey branch. The number of consecutive Farey branches that point in the same direction is called a Farey bunch. The graph $\mathfrak{C}_{\mathfrak{a}}$ and hence the conjugacy class of $W_{f_{\mathfrak{a}}}$ is completely determined by the formation of these Farey bunches and the number of Farey branches within these bunches.
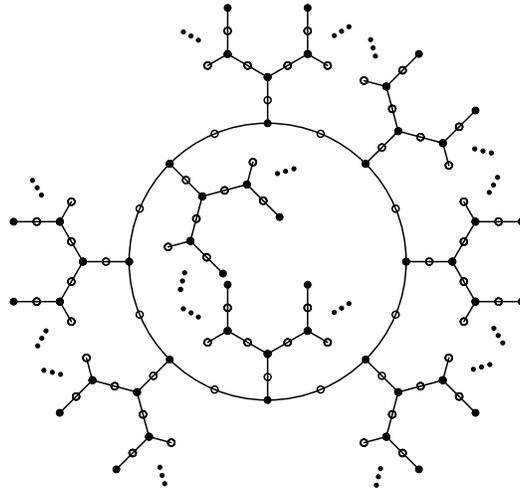
Figure 2. The çark representing $\mathfrak{a} = (2, \sqrt{30})$.

Example 3.3 *For $K = \mathbf{Q}(\sqrt{30})$, we set $\mathfrak{a} = (2, \sqrt{30})$. $N(\mathfrak{a}) = 2$. This gives rise to the indefinite binary quadratic form $f_\mathfrak{a}(X, Y) = 2X^2 - 15Y^2$. We have $W_{f_\mathfrak{a}} = \begin{pmatrix} 11 & 30 \\ 4 & 11 \end{pmatrix}$ and in terms of the generators one has $W_{f_\mathfrak{a}} = (LS)^2 L^2 S(LS)^2 L^2 S(LS)^2$. Figure 2 depicts the corresponding çark.*

3.4. Çarks as integral points

Let $\mathfrak{a}$ be a narrow ideal class in K and $W_{f_\mathfrak{a}} \in \mathrm{PSL}_2(\mathbf{Z})$ be its fundamental automorphism. Elements in the conjugacy class $[W_{f_\mathfrak{a}}]$ can be partially ordered according to their lengths (i.e. number of letters S, L, and L^2 that appear). Under the correspondence between the edges of the çark $\mathfrak{C}_\mathfrak{a}$ and $[W_{f_\mathfrak{a}}]$ one may observe that those that are of smallest length (called *minimal words*) correspond exactly to edges on the spine. Minimal words are not unique because if W is such a word then so is SWS. In fact, minimal words can be written as a disjoint union of those that start with S and those that start either with L or with L^2. Among the latter there are those that can be written of the form $(LS)^{m_1}(L^2 S)^{n_1} \ldots (LS)^{m_k}(L^2 S)^{n_k}$, where $m_1, n_1, \ldots, m_k, n_k \geq 1$. To each such element in the conjugacy class, we associate the ordered pair $(m_1, n_1, \ldots, m_k, n_k)$ and call k the length of the çark. Observe that the integers m_i represent the number of Farey trees in consecutive Farey bunches that expand in the direction of the outer boundary. Analogously n_i stands for the number of Farey tree in the Farey bunches that expand in the direction of the inner boundary.

A couple of remarks are in order. If the conjugacy class of a word W gives rise to the sequence $(m_1, n_1, \ldots, m_k, n_k)$, then W^l gives rise to the same sequence repeated l times, and in particular it is represented by a $2kl$-tuple. Let us define a çark to be *primitive* if it is not a repetition of a shorter çark. Therefore, although W and W^l give rise to the same binary quadratic form, their çarks are different. Secondly, the number $k_\mathfrak{a} := k$ is fixed for a narrow ideal class $\mathfrak{a}$ and the length of the minimal word is equal to $2\sum_{i=1}^{k}(m_i + n_i)$. However, different narrow ideal classes of the same number field K may be represented by minimal words of different lengths, e.g., for $K = \mathbf{Q}(\sqrt{30})$ $H^+(K) \cong (\mathbf{Z}/2\mathbf{Z})^2$, with two narrow ideal classes that lie above the class of the principal ideal being represented by a 2-tuple, and as we have seen earlier (Example 3.3), the two narrow ideal

classes lying above $[(2, \sqrt{30})]$ being represented by a 4-tuple. We are now ready to prove our main theorem:

Theorem 3.4 *Let K be a real quadratic number field of discriminant Δ. Then each narrow ideal class in K gives rise to an integral solution of the equation*

$$\mathcal{L}_{2k}(x_1, y_1, \ldots, x_k, y_k)^2 - 4 = z^2 \Delta, \tag{3.1}$$

for some positive integer k and for some $z \in \mathbf{Z}$, which depends only on K.

Proof We let $k = k_K$ be the maximum of $k_{\mathfrak{a}}$ as $\mathfrak{a}$ runs through $H^+(K)$ and let Δ be the discriminant of K. Set (x_o, z_o) to be the fundamental solution of the corresponding Pell equation $X^2 - \Delta Z^2 = 4$. Remark that for any narrow ideal class, the fundamental automorphism will be obtained using (x_o, z_o). For each çark represented by a $2l$-tuple, say $(m_{\mathfrak{a},1}, n_{\mathfrak{a},1}, \ldots m_{\mathfrak{a},l}, n_{\mathfrak{a},l})$, for $l < k$ we complete it to a $2k$-tuple by appending $2(k-l)$ many zeros to the end of the tuple and obtain $(m_{\mathfrak{a},1}, n_{\mathfrak{a},1}, \ldots m_{\mathfrak{a},l}, n_{\mathfrak{a},l}, 0, \ldots, 0)$. Given such a $2k$-tuple, say $(m_1, n_1, \ldots, m_k n_k)$, we set:

$$W = (LS)^{m_1} (L^2 S)^{n_1} \ldots (LS)^{m_k} (L^2 S)^{n_k}.$$

By construction the matrix $W \in \mathrm{PSL}_2(\mathbf{Z})$ is a fundamental automorphism of the binary quadratic form $f_{\mathfrak{a}}$. Using the correspondence between automorphisms and solutions of the Pell equation $X^2 + \Delta Z^2 = 4$, see Section 3.2, we obtain $\mathrm{tr}(W) = x = x_o$ and this satisfies $x_o^2 - 4 = \Delta z_o^2$.

Now we observe that $M(m, n) = (LS)^m (L^2 S)^n$. The multivariate Lucas polynomial $\mathcal{L}_{2k} = 2A_k$ is merely the trace of the matrix $M(x_1, y_1, \ldots, x_k, y_k)$ and hence the trace of the matrix W is equal to $\mathcal{L}_{2k}(m_1, n_1, \ldots, m_k, n_k)$. □

Definition 3.5 *We let $C_K \subset \mathbf{C}^{2k_K}$ denote the solution set of the equation*

$$\mathcal{L}_{2k_K}(x_1, y_1, \ldots, x_{k_K}, y_{k_K})^2 - 4 = z^2 \Delta;$$

we refer to it as the affine çark hypersurface.

Recall that there is an action of $\mathbf{Z}/k\mathbf{Z}$ on $\mathcal{L}_{2k}$. This means that the set C_K admits an action of $\mathbf{Z}/k_K\mathbf{Z}$; see Equation 2.1.

Definition 3.6 *The* affine çark surface *of K is defined as the quotient $C_K/(\mathbf{Z}/k_K\mathbf{Z})$. This surface will be denoted by $\mathcal{C}_K$.*

Corollary 3.7 *Let K be a real quadratic number field. Then there is a one to one correspondence between integral points of the çark surface $\mathcal{C}_K$ and narrow ideal classes in K.*

Proof One way this correspondence can be obtained is by using Theorem 3.4 and noting the fact that the action of $\mathbf{Z}/k_K\mathbf{Z}$ does not change the conjugacy class of the fundamental automorphism of narrow ideal classes.

Conversely, if $(m_1, n_1, \ldots, m_{k_K}, m_{k_K})$ is an integral point on $\mathcal{C}_K$, one can construct the element

$$W = (LS)^{m_1} (L^2 S)^{n_1} \ldots (LS)^{m_k} (L^2 S)^{n_k}$$

and look at the narrow ideal class that arises from the binary quadratic form whose fundamental automorphism is W; namely, if $W = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$ then the corresponding indefinite primitive binary quadratic form is $f(X, Y) = \frac{1}{\delta}\left(rX^2 + (s-p)XY - qY^2\right)$, where δ is the greatest common divisor of r, $s-p$, and q. Since this point is a solution of Equation 3.1, where by definition z_o is minimal, the discriminant of this form must be square-free. $\square$

Let us conclude the paper with a few remarks. Instead of considering the *fundamental solution* we may consider other z arising from nonfundamental solutions of the corresponding Pell equation. Even more generally, we may treat z as variable in the equation and consider the affine hypersurface with equation

$$\mathcal{L}_{2k}(x_1, y_1, \ldots, x_k, y_k)^2 - 4 = z^2 \Delta$$

in $\mathbf{C}^{2k+1}$. Each integral point on the quotient of this hypersurface with the obvious action of $\mathbf{Z}/k\mathbf{Z}$ gives rise to a binary quadratic form whose discriminant's square-free part is equal to Δ. Such integral points give rise to nonmaximal orders in $\mathbf{Z}_K$. One may then intersect the hypersurface with $z = \lambda$ planes, where $\lambda \in \mathbf{Z}$, and then consider integral points of the intersection. In this case, again each integral point gives rise to a narrow ideal class in an appropriate class group; see [2, Theorem 5.2.9]. One may generalize Corollary 3.7 immediately to this case. Indeed, assuming one can compute the class number for K, or almost equivalently find the number of integral points on the çark surface of K, one can determine the number of integral points of this surface; see [3, Corollary 7.28].

Acknowledgments

References

[1] Buchmann J, Vollmer U. Binary Quadratic Forms: An Algorithmic Approach. Berlin, Germany: Springer, 2007.

[2] Cohen H. A Course in Computational Algebraic Number Theory. Berlin, Germany: Springer-Verlag, 1993.

[3] Cox DA. Primes of the Form $x^2 + ny^2$. Pure and Applied Mathematics (Hoboken). Hoboken, NJ, USA: John Wiley & Sons, Inc., 2013.

[4] Gauss CF. Disquisitiones arithmeticae. Translated into English by Arthur A. Clarke. New Haven, CT: Yale University Press, 1966.

[5] Herpin A. Sur une nouvelle méthode d'introduction des polynômes de Lucas. C R Acad Sci Paris 1947; 225: 17-19 (in French).

[6] Lang S. Algebraic Number Theory. New York, NY, USA: Springer-Verlag, 1994.

[7] Neukirch J. Algebraic Number Theory. Berlin, Germany: Springer-Verlag, 1999.

[8] Stewart I, Tall D. Algebraic Number Theory and Fermat's Last Theorem. Natick, MA, USA: A K Peters Ltd., 2002.

[9] Uludağ M, Sağlam I. Hypergeometric Galois actions. In Papadopoulos, A, editor. Handbook of Teichmüller Theory, No. VI. Zurich, Switzerland: European Mathematical Society, 2016, pp. 467-500.

[10] Uludağ M, Zeytin A. A panorama of the fundamental group of the modular orbifold. In Papadopoulos, A, editor. Handbook of Teichmüller Theory, No. VI. Zurich, Switzerland: European Mathematical Society, 2016, pp. 501-519.

[11] Uludağ M, Zeytin A, Durmuş M. Binary quadratic forms as dessins. J. Théor Nombres Bordx., 2017, 29:445–469.

[12] Zagier DB. Zetafunktionen und quadratische Körper. Eine Einführung in die höhere Zahlentheorie. Berlin, Germany: Springer-Verlag, 1981.

[13] Zeytin A. Class number problems and Lang conjectures. In Mourtada, H, et al., editors. Algebraic geometry and number theory. Summer school, Galatasaray University, Istanbul, Turkey, June 2–13, 2014, Basel: Birkhäuser/Springer, 2016, pp. 211-232.