The Fibonacci Quarterly 2001 (39,2): 107-115

DERIVED SEQUENCES, THE TRIBONACCI RECURRENCE AND CUBIC FORMS

Michele Elia
Dipartimento di Elettronica, Politecnico di Torino
Corso Duca degli Abruzzi 24, I-10129 Torino, Italy
e-mail: elia@polito.it

(*Submitted January 1999*)

1. INTRODUCTION

Integer representations by forms are sources of a series of very interesting Diophantine equations. For instance, the cubic form $x^3+y^3+z^3$ represents 1 and 2 in an infinite number of ways, whereas only two representations $(1,1,1)$ and $(4,4,-5)$ are known for the number 3 and it is unknown whether there are other representations. Number 4 has no representations, as was proved using congruential arguments. But, in general, we do not know a definitive criterion for testing if a number is representable as a sum of three cubes, nor a method for finding such a representation (see [12]). For the quadratic forms, the situation is different; Gauss developed his theory of quadratic forms [7] and solved the related integer representation problem. In particular, quadratic forms, computed as first derived sequences using the Simson determinant, are invariant for some second-order linear recurrent sequence. Therefore, each representable integer admits an infinite number of representations deduced from the recurrent sequence (see [17], [6]).

In this paper we discuss integer representations by a cubic form associated with a third-order recurrence known as the Tribonacci recurrence [9]. The technique of derived sequences is used to define an invariant cubic form, computed as second derived sequences [5] of a third-order linear recurrent sequence. Therefore, an infinite number of representations is produced whenever a representation exists. Before stating the problem, let us briefly review the properties of a third-order linear recurrent sequence $\{T_0, T_1, T_2, \ldots\}$ defined by the recurrence

$$T_{n+3} = pT_{n+2} + qT_{n+1} + rT_n, \quad p,q,r \in \mathbb{Z}, \tag{1}$$

over $\mathbb{Z}$, the ring of rational integers, with initial integer values $T_2 = c$, $T_1 = b$, and $T_0 = a$. The characteristic polynomial of recurrence (1) is $\Lambda(x) = x^3 - px^2 - qx - r$, and expressions that allow us to directly compute T_n are

$$T_n = \begin{cases} A\alpha^n + B\beta^n + C\gamma^n, \\ (A+Bn)\alpha^n + C\gamma^n, \\ (A+Bn+Cn^2)\alpha^n, \end{cases} \tag{2}$$

according to whether $\Lambda(x)$ has three simple roots α, β, γ, a double root $\alpha = \beta$ and γ, or a triple root $\alpha = \beta = \gamma$. The second derived sequence $T_n^{(2)}$ (see [5], Vol. I, p. 410) of a third-order recurrent sequence is defined by

$$T_n^{(2)} = \begin{vmatrix} T_n & T_{n+1} & T_{n+2} \\ T_{n+1} & T_{n+2} & T_{n+3} \\ T_{n+2} & T_{n+3} & T_{n+4} \end{vmatrix}.$$

The development of this determinant, using the recurrence (1) to eliminate T_{n+3} and T_{n+4}, yields a cubic form in three variables, T_n, T_{n+1}, and T_{n+2}:

$$\begin{aligned}-T_n^3r^2-(pq+r)T_{n+1}^3-T_{n+2}^3+(3r-pq)T_nT_{n+1}T_{n+2}-2qrT_n^2T_{n+1}-prT_n^2T_{n+2}\\ -(pr+q^2)T_nT_{n+1}^2+qT_nT_{n+2}^2+(q-p^2)T_{n+1}^2T_{n+2}+2pT_{n+1}T_{n+2}^2.\end{aligned} \tag{3}$$

Whereas a closed-form expression for the sequence $T_n^{(2)}$ as a function of n is obtained using (2) before expanding the determinant:

$$T_n^{(2)}=\begin{cases}-r^nABC[(\alpha-\beta)(\beta-\gamma)(\gamma-\alpha)]^2,\\ -r^nB^2C[(\alpha-\gamma)^2\alpha]^2,\\ -r^n8C^3\alpha^6,\end{cases} \tag{4}$$

according to the three situations of simple, double, or triple roots.

From expression (4) we can conclude that, whatever may be the root multiplicity of $\Lambda(x)$, $T_n^{(2)}$ satisfies the first-order recurrence $T_n^{(2)}=rT_{n-1}^{(2)}$. From the same equation (4) we can see that the cubic form (3) is an invariant for the sequence T_n if and only if $r=1$. Rewriting expression (3) with $r=1$, and substituting the variables x, y, and z for T_n, T_{n+1}, and T_{n+2}, respectively, we obtain the invariant cubic form $\mathscr{C}(x,y,z)$:

$$-x^3-y^3(pq+1)-z^3+xyz(3-pq)-2qx^2y-px^2z-(p+q^2)xy^2+qxz^2+(q-p^2)zy^2+2pyz^2. \tag{5}$$

The integer representation problem consists of finding all triples $(x_0,y_0,z_0)\in\mathbb{Z}^3$ that are solutions of the Diophantine equation $\mathscr{C}(x_0,y_0,z_0)=m$ $\forall m\in\mathbb{Z}$. If a triple (x_0,y_0,z_0) exists, it is called a representation of m and $\mathscr{C}(x,y,z)$ is said to represent m. Otherwise, it is said that $\mathscr{C}(x,y,z)$ does not represent m. From the invariance of $\mathscr{C}(x,y,z)$ it is evident that, using a triple (x_0,y_0,z_0) as an initial condition in the recurrence (1), we get an infinite number of representations for m.

When $p=q=r=1$, expression (1) is known as the Tribonacci recurrence, and the sequences with initial conditions $T_2=1$, $T_1=1$, $T_0=0$, and $T_2=3$, $T_1=1$ $T_0=3$ are called the Tribonacci sequence K_n and the generalized Lucas sequence S_n, respectively (see [9]).

In this paper we investigate the properties of the Tribonacci cubic form $\mathscr{T}(x,y,z)$, which we define as the opposite of the expression obtained by setting $p=q=1$ in (5), namely,

$$\mathscr{T}(x,y,z)=x^3+2y^3+z^3-2xyz+2yx^2+zx^2+2xy^2-xz^2-2yz^2. \tag{6}$$

The related representation problem is fully solved. With this aim, the paper is organized as follows: Section 2 collects the main properties of the Tribonacci recurrence and a related ring that we will call the *Tribonacci ring*; Section 3 studies the Tribonacci cubic form; Section 4 solves the integer representation problem for the Tribonacci cubic form; Section 5 comments on related and open problems.

2. THE TRIBONACCI RECURRENCE AND CUBIC RINGS

Let $\Theta(x)=x^3-x^2-x-1$ denote the characteristic polynomial, called *Tribonacci polynomial*, of the Tribonacci recurrence. The polynomial $\Theta(x)$ is irreducible over the rational field $\mathbb{Q}$ with Galois group $\mathscr{G}_\Theta$ isomorphic to $\mathscr{S}_3$, the symmetric group on three elements. Let us denote by τ the real root and with τ_1 and τ_2 the complex conjugate roots of $\Theta(x)$. These roots, expressed by means of the Tartaglia-Lagrange formulas, are

$$\begin{cases} \tau = \frac{1}{3}\left[1+\sqrt[3]{19+3\sqrt{33}}+\sqrt[3]{19-3\sqrt{33}}\right], \\ \tau_1 = \frac{1}{3}\left[1+\omega\sqrt[3]{19+3\sqrt{33}}+\omega^2\sqrt[3]{19-3\sqrt{33}}\right], \\ \tau_2 = \frac{1}{3}\left[1+\omega^2\sqrt[3]{19+3\sqrt{33}}+\omega\sqrt[3]{19-3\sqrt{33}}\right], \end{cases}$$

where $\omega = \frac{-1+i\sqrt{3}}{2}$ is a primitive cube root of unity.

Let $\mathbb{Q}[\tau]$ denote a cubic field generated by the real root τ of the Tribonacci polynomial. The field $\mathbb{Q}[\omega, \tau]$ of complete reducibility for $\Theta(x)$ is obtained from $\mathbb{Q}[\tau]$ by the adjunction of ω. Using (2) and the roots of the Tribonacci polynomial, we get the following explicit expressions for the Tribonacci and the generalized Lucas sequence, respectively:

$$\begin{cases} K_n = \dfrac{\tau^{n+1}}{(\tau-\tau_1)(\tau-\tau_2)} + \dfrac{\tau_1^{n+1}}{(\tau_1-\tau)(\tau_1-\tau_2)} + \dfrac{\tau_2^{n+1}}{(\tau_2-\tau)(\tau_2-\tau_1)}, \\ S_n = \tau^n + \tau_1^n + \tau_2^n. \end{cases}$$

Notice that S_n is the n-power symmetric function of τ, τ_1, and τ_2.

In a ring, the solution of the representation problem for decomposable forms is based on ring factoring properties [1]. In the case of the Tribonacci cubic form, the solution depends on the integral ring of $\mathbb{Q}[\tau]$ that we will call the *Tribonacci ring*.

2.1 The Tribonacci Ring

In this section we will prove two main properties of the integral ring of $\mathbb{Q}[\tau]$:

i) the ring of integers in $\mathbb{Q}[\tau]$ is $\mathbb{Z}[\tau]$, the extension of $\mathbb{Z}$ by the adjunction of τ;

ii) $\mathbb{Z}[\tau]$ is a principal ideal domain (PID).

Let us recall that the norm in $\mathbb{Q}[\tau]$ is defined as

$$\begin{aligned} Nr(a+b\tau+c\tau^2) &= (a+b\tau+c\tau^2)(a+b\tau_1+c\tau_1^2)(a+b\tau_2+c\tau_2^2) \\ &= a^3+b^3+c^3-4abc-c^2(b+a)+b^2(c-a)+a^2(3c+b), \end{aligned} \tag{7}$$

where the product expansion turns out to be an irreducible cubic form ([1], p. 80) over $\mathbb{Z}$.

A direct calculation shows that the basis discriminant is $D[1, \tau, \tau^2] = -44$. Since the norm of τ is unity, i.e., $Nr(\tau) = \tau \cdot \tau_1 \cdot \tau_2 = 1$, then τ is a unit, and the triple $\{1, \tau, \tau^2\}$, hereinafter called *polynomial basis*, is an integral basis for $\mathbb{Q}[\tau]$.

Theorem 1: The triple $\{1, \tau, \tau^2\}$ is an integral basis for the integer ring of $\mathbb{Q}[\tau]$.

Proof: Let us consider an integral basis $\{\omega_1, \omega_2, \omega_3\}$ for the ring of integers in $\mathbb{Q}[\tau]$. Since τ is an integer, then a 3×3 matrix $C = (c_{hj})$ with $c_{hj} \in \mathbb{Z}$ exists such that

$$\begin{cases} 1 = c_{11}\omega_1 + c_{12}\omega_2 + c_{13}\omega_3, \\ \tau = c_{21}\omega_1 + c_{22}\omega_2 + c_{23}\omega_3, \\ \tau^2 = c_{31}\omega_1 + c_{32}\omega_2 + c_{33}\omega_3. \end{cases} \tag{8}$$

The determinant $\det(C)$ is an integer, and (see [14], p. 67) we have

$$D[1, \tau, \tau^2] = \det(C)^2 D[\omega_1, \omega_2, \omega_3] = -2^2 \cdot 11;$$

hence, possible values for $\det(C)$ are ± 1 and ± 2. Let us first observe that it is sufficient to consider positive values for $\det(C)$, since negative values only correspond to a different ordering of the basis elements. Let $C_{jh} \in \mathbb{Z}$ denote the cofactor of c_{hj}. If $\det(C) = 1$, then, inverting (8), we have

$$\begin{cases} \omega_1 = C_{11}\cdot 1 + C_{12}\tau + C_{13}\tau^2, \\ \omega_2 = C_{21}\cdot 1 + C_{22}\tau + C_{23}\tau^2, \\ \omega_3 = C_{31}\cdot 1 + C_{32}\tau + C_{33}\tau^2, \end{cases} \tag{9}$$

and $\{1, \tau, \tau^2\}$ is evidently an integral basis for $\mathbb{Q}[\tau]$.

If $\det(C) = 2$, then, inverting (8), we obtain

$$\begin{cases} \omega_1 = \dfrac{C_{11}\cdot 1 + C_{12}\tau + C_{13}\tau^2}{2}, \\ \omega_2 = \dfrac{C_{21}\cdot 1 + C_{22}\tau + C_{23}\tau^2}{2}, \\ \omega_3 = \dfrac{C_{31}\cdot 1 + C_{32}\tau + C_{33}\tau^2}{2}, \end{cases} \tag{10}$$

where at least one of the coefficients C_{jh} is an odd number, otherwise $\det(C^{-1})$ is an integer, contrary to the assumption that $\det(C^{-1}) = 1/2$.

To demonstrate that $\det(C) = 2$ is not possible, let us compute the norm $Nr(\omega_j) = \frac{1}{8}\Omega$, where Ω is the cubic form

$$C_{j1}^3 + C_{j2}^3 + C_{j3}^3 - 4C_{j1}C_{j2}C_{j3} - C_{j3}^2(C_{j2} + C_{j1}) + C_{j2}^2(C_{j3} - C_{j1}) + C_{j1}^2(3C_{j3} + C_{j2}).$$

Since $Nr(\omega_j)$ is an integer, Ω must be a multiple of 8, which will turn out to be impossible unless all C_{jh} are even, a case already excluded. In fact, taking the congruence modulo 2 of the expression between square brackets, we find the condition $C_{j1} + C_{j2} + C_{j3} = 0$, $j = 1, 2, 3$, where, for at least one j, one addend is even and two addends are odd. For instance, let $C_{j1} = 2a$, $C_{j2} = 2b+1$, and $C_{j3} = 2c+1$ be substituted in the above bracketed expression, then, taking the congruence modulo 4 of the resulting expression, we have

$$(2b+1)^3 + (2c+1)^3 - (2c+1)^2(2b+1+2a) + (2b+1)^2(2c+1-2a) = 2 \mod 4.$$

This result shows that Ω is twice an odd number; hence, it cannot be a multiple of 8. The other two cases, $C_{j1} = 2a+1, C_{j2} = 2b, C_{j3} = 2c+1$ and $C_{j1} = 2a+1, C_{j2} = 2b+1, C_{j3} = 2c$, respectively, yield the same conclusion. Therefore, $\det(C) = 2$ is not possible. Thus, the ring of integers in $\mathbb{Q}[\tau]$ is the integral extension $\mathbb{Z}[\tau]$, and any integer in $\mathbb{Q}[\tau]$ is of the form $a + b\tau + c\tau^2$, with $a, b, c \in \mathbb{Z}$. □

It follows from the above proposition that the field discriminant is $D_{\mathbb{Q}[\tau]/\mathbb{Q}} = -44$. Moreover, we have already observed that $Nr(\tau) = 1$. Since $\Theta(x)$ has one real root and two complex roots, Dirichlet's theorem ([1], p. 112) allows us to conclude that the multiplicative group $\mathbb{U}[\tau]$ of the units in $\mathbb{Z}[\tau]$ is an Abelian group generated by -1 and τ. In other terms, $\mathbb{U}[\tau] = \mathbb{C}_2 \times \mathbb{C}_\infty$, where $\mathbb{C}_2 = \{1, -1\}$ and $\mathbb{C}_\infty$ is a cyclic group of infinite order isomorphic to the additive group of $\mathbb{Z}$.

We end this section by showing that $\mathbb{Z}[\tau]$ is a principal ideal domain (PID), consequently, $\mathbb{Z}[\tau]$ is a unique factorization domain. For this purpose, let us recall three basic concepts:

- In $\mathbb{Q}[\tau]$, a notion of ideal equivalence is introduced by defining two ideals $\mathcal{V}_1$ and $\mathcal{V}_2$ as equivalent if a rational number $u \in \mathbb{Q}$ exists such that $\mathcal{V}_1 = u\mathcal{V}_2$.
- Given a nonzero ideal $\mathcal{B}$ of a ring $\mathbb{R}$, we call the number card $(\mathbb{R}/\mathcal{B})$ (the cardinality of the quotient $\mathbb{R}/\mathcal{B}$) the norm of $\mathcal{B}$ and denote it by $Nr(\mathcal{B})$ (see [15], p. 52).
- $\mathbb{Z}[\tau]$ is the only ideal with norm 1 in $\mathbb{Q}[\tau]$.

Theorem 2: The ring $\mathbb{Z}[\tau]$ is a principal ideal domain.

Proof: The ring $\mathbb{Z}[\tau]$ is a Dedekind ring; hence, it is integrally closed and, by Corollary 1 on page 58 of [15], every ideal class contains an integral ideal $\mathcal{B}$ such that

$$Nr(\mathcal{B}) \le \left(\frac{4}{\pi}\right)\frac{3!}{3^3}|-44|^{1/2} \le 1.877 < 2,$$

and this means that $\mathbb{Z}[\tau]$ belongs to every ideal class, so that in $\mathbb{Z}[\tau]$ every ideal is principal (see [1], p. 231). □

Remark 1: Dedekind gave a pictorial description of an ideal number in his masterful survey paper on the theory of algebraic integers [4]. Ideal numbers were introduced by Dirichlet and Kummer in order to recover unique factorization in algebraic number fields. A "true" ideal number "*is never defined in its own right, but only as a divisor of actual number* ω" ([4], p. 94) in the ring. If the unique factorization holds in the ring of integers of an algebraic number field, then no ideal number exists and all ideals belong to a single equivalence class. Whereas, if unique factorization does not hold true, then a "true" ideal number of Kummer occurs. "True" ideal numbers produce different classes of ideals in the algebraic number field, and these classes cannot contain the integral ring as an element.

3. THE TRIBONACCI CUBIC FORM

We defined the Tribonacci cubic form $\mathcal{T}(x, y, z)$ as having a positive x^3 coefficient. This assumption is not restrictive, since a sign change of the three variables corresponds to a sign change of the form, that is,

$$\mathcal{T}(-x, -y, -z) = -\mathcal{T}(x, y, z). \tag{11}$$

The transformation (11) belongs to a set of variable substitutions that specify the equivalence of forms. This concept, together with the notions of reducibility and decomposability of forms, is elemental to classify $\mathcal{T}(x, y, z)$. Let us recall, for the sake of reference, their definitions from [1].

Definition 1: Let all cubic forms considered have coefficients in $\mathbb{Z}$:

i) Two cubic forms $\mathcal{C}'(y_1, y_2, y_3)$ and $\mathcal{C}(x_1, x_2, x_3)$ are called *equivalent* if there is a nonsingular linear change of variables which takes one form to the other. The transformation is characterized by a matrix with integer entries and its determinant is ±1.

ii) A cubic form is said to be *irreducible* over $\mathbb{Q}$ if it cannot be written as a product of a linear form and a quadratic form with coefficients in $\mathbb{Q}$.

iii) A cubic form is said to be *decomposable* over $\mathbb{Q}$ if it can be written as a product of linear forms with coefficients in some finite algebraic extension of $\mathbb{Q}$; it is called nondecomposable otherwise.

The above definition has its nearly direct consequence in the following facts:

1. Equivalence of forms is an equivalence relation.
2. The variable transformation is invertible, and the matrix of the inverse transformation has integer coefficients.
3. Equivalent forms represent the same set of integers.
4. Any cubic form is always equivalent to a form with at most eight nonzero coefficients.
5. Reducible cubic forms with integer coefficients are reducible over $\mathbb{Z}$.
6. Cubic forms with integer coefficients, which are decomposable in a finite algebraic extension $\mathcal{Q}$ of $\mathbb{Q}$, are decomposable in the integral ring of $\mathcal{Q}$.

Proposition 1: The Tribonacci cubic form $\mathcal{T}(x,y,z)$ is irreducible in $\mathbb{Q}$, decomposable in $\mathbb{Q}[\tau,\omega]$ and equivalent to a form $\mathcal{C}(t,u,v)$ with eight nonzero coefficients.

Proof: The equivalent form $\mathcal{C}(t,u,v)$ with eight nonzero coefficients,

$$u^3+4v^3-7t^3-2tuv+9ut^2+2vt^2-5tu^2-4uv^2, \tag{12}$$

is obtained performing on $\mathcal{T}(x,y,z)$ the variable substitution

$$\begin{cases} x=-t+v, \\ y=v, \\ z=-2t+v+u. \end{cases}$$

Irreducibility is easily proved by setting $y=0$ and $z=-1$ to obtain the irreducible polynomial $\mathcal{T}(x,0,-1)=x^3-x^2-x-1$ in a single variable.

Decomposability is proved by factoring $\mathcal{T}(x,y,z)$ into a linear and a quadratic form over the real field $\mathbb{Q}[\tau]$. The full decomposition into three linear forms over $\mathbb{Q}[\omega,\tau]$ is obtained by taking the conjugate of the linear factor under the Galois group $\mathcal{G}_\Theta$.

Let us consider the real decomposition

$$\mathcal{T}(x,y,z)=(x+ay+bz)(x^2+cy^2+dz^2+exy+fyz+gxz); \tag{13}$$

therefore, we obtain the following system of nine equations in seven variables from the comparison of the coefficients in their expanded version with the coefficients of equal monomials in (6):

$$\begin{cases} ac=2 & \Rightarrow & c=2/a=a^2-2a+2, \\ bd=1 & \Rightarrow & d=b^2-b-1, \\ ag+be+f=-2 & \Rightarrow & f=-2-a-2b+2ab, \\ e+a=2 & \Rightarrow & e=2-a, \\ c+ae=2 & \Rightarrow & a^3-2a^2+2a-2=0, \\ af+bc=0 & \Rightarrow & f=-b(a^2-a), \\ ad+bf=-2 & \Rightarrow & f=-2(b^2-b-1)-a(2b-b^2), \\ d+bg=-1 & \Rightarrow & b^3-b^2-b-1=0, \\ b+g=1 & \Rightarrow & g=1-b. \end{cases}$$

The system is compatible. Moreover, the factorization (13) takes place in $\mathbb{Q}[\tau]$ because we can express both b and a in terms of τ. Actually, we have $b=\tau$ and, from the birational substitution $b=1/(a-1)$ that transforms the equation $\Theta(b)=b^3-b^2-b-1=0$ into the equation $a^3-2a^2+2a-2=0$, we get $a=(1+b)/b=(1+\tau)/\tau$. The coefficients of the decomposition (13) are explicitly

$$a=\frac{\tau+1}{\tau}=(\tau-1)\tau,\ b=\tau,\ c=2\frac{\tau}{\tau+1}=-\tau^2+2\tau+1,\ d=\tau^2-\tau-1,$$
$$e=\frac{\tau-1}{\tau}=-\tau^2+\tau+2,\ f=-\tau^2-1,\ g=1-\tau.$$

Over the complex extension $\mathbb{Q}[\omega,\tau]$, $\mathcal{T}(x,y,z)$ decomposes into three linear factors as

$$\mathcal{T}(x,y,z)=(\tau x+(1+\tau)y+\tau^2z)(\tau_1x+(1+\tau_1)y+\tau_1^2z)(\tau_2x+(1+\tau_2)y+\tau_2^2z). \tag{14}$$

It is evident that the Tribonacci cubic is a norm in $\mathbb{Q}[\tau]$ with respect to the integral basis $\{\tau, 1+\tau, \tau^2\}$, hereinafter called *Tribonacci basis*.

Remark 2: Along with a cubic form, it is interesting to consider the cubic curve in a complex projective plane with homogeneous coordinates x, y, and z, defined by the equation $\mathcal{C}(x,y,z)=0$ (see [11]). Whenever the cubic curve has a singular point, a translation of the singular point into the origin usually yields to a simpler expression of cubic form. However, the curve $\mathcal{T}(x,y,z)=0$ has no singular point, in fact it is a degenerate curve which is the product of three straight lines that are not concurrent in a single point. Since the Tribonacci cubic form cannot be simplified using this artifice, it is likely that the reduced form (12) with eight coefficients is the simplest one possible.

4. THE TRIBONACCI CUBIC AND REPRESENTATION OF INTEGERS

The Tribonacci cubic gives infinitely many representations for $m=-1$ and $m=-44$ by Tribonacci and generalized Lucas sequences, respectively, and no representation for $m=3$. As a consequence of (14), the representation problem for the Tribonacci cubic can be completely solved, since $\mathbb{Z}[\tau]$ is a PID. In particular, it is evident that rational primes, which are still primes in $\mathbb{Z}[\tau]$, are not represented by the Tribonacci cubic. The following theorem fully characterizes the rational primes of $\mathbb{Z}[\tau]$.

Theorem 3: A prime p in $\mathbb{Z}$ is also prime in $\mathbb{Z}[\tau]$ if and only if $\Theta(x)$ is irreducible over $\mathbb{Z}_p$.

Proof: First, let us assume that p is a rational prime in $\mathbb{Z}[\tau]$, then the set of residues$\mathbb{Z}[\tau]_p$ modulo p is a field isomorphic to $GF(p^3)$ with basis $\{1, \tau, \tau^2\}$, so $\Theta(x)$ is irreducible over $\mathbb{Z}_p$.

Second, let us assume that $\Theta(x)$ is irreducible over $\mathbb{Z}_p$; therefore, the Galois field $GF(p^3)$ is generated by a root of $\Theta(x)$. If we assume that p factors properly in $\mathbb{Z}[\tau]$, then we have a decomposition

$$p=(a_0+a_1\tau+a_2\tau^2)\cdot[(a_0^2-a_1^2+a_0a_1+3a_0a_2-2a_1a_2)$$
$$+(-a_1^2+2a_2^2-a_0a_1-a_1a_2)\tau+(a_1^2-a_2^2-a_0a_2+a_1a_2)\tau^2],$$

where $a_0, a_1, a_2 \in \mathbb{Z}$. Taking the congruence modulo p, we see that $(\tilde{a}_0+\tilde{a}_1\tau+\tilde{a}_2\tau^2)$, where $\tilde{a}_0, \tilde{a}_1, \tilde{a}_2 \in \mathbb{Z}_p$ is a zero divisor in $GF(p^3)$, a contradiction. Thus, p is a prime in $\mathbb{Z}[\tau]$. □

Remark 3: Theorem 3 is a reformulation adapted to our cubic field of the well-known fact that rational Gaussian primes are primes $p\ (=4k+3)$ for which -1 is a quadratic nonresidue; in other words, the polynomial x^2+1 is irreducible over $\mathbb{Z}_p$. Whereas, for primes $p=4k+1$, since -1 is a quadratic residue, the polynomial x^2+1 is reducible over $\mathbb{Z}_p$. Hence, p factors over $\mathbb{Z}[i]$, i.e., $p=x^2+y^2$ has a solution in rational integers x and y (see [4]).

Remark 4: It is easy to check whether an integral polynomial $m(x)$ is irreducible over $GF(p)$ by computing the greatest common civisor (GCD), via the Euclidean algorithm, with $x^{p-1}-1$. If the GCD is 1, then $m(x)$ is irreducible, otherwise we get the product of its linear irreducible factors, possibly $m(x)$ itself.

It follows from Theorem 3 that 3, 5, 23, 31, 37, ... are primes in $\mathbb{Z}[\tau]$; therefore, they are not represented by the Tribonacci cubic. In the next table, we summarize the representation of the rational primes up to 29 that factor in $\mathbb{Z}[\tau]$. The prime factors are explicitly written in the polynomial basis, whereas the representing triples are given in the Tribonacci basis, which is useful to initiate the Tribonacci recurrence generating an infinite number of representations. The rational primes 2 and 11 are factors of the discriminant D; hence, they are the only primes that ramify in $\mathbb{Z}[\tau]$ (see [15], Theorem 1, p. 58). In particular, they are the only rational primes divisible by a square of a prime in $\mathbb{Z}[\tau]$.

$$\begin{array}{rcll}
2 & = & (1+\tau)(1-\tau)^2 & \Rightarrow (0,1,0), \\
2^s & = & (1+\tau)^s(1-\tau)^{2s} & \Rightarrow (a,b,c), \\
11 & = & (3+4\tau+4\tau^2)(3-2\tau)^2 & \Rightarrow (1,3,4), \\
7 & = & (1+2\tau)(-1-6\tau+4\tau^2) & \Rightarrow (1,1,0), \\
13 & = & (3+\tau-\tau^2)(4-\tau+2\tau^2) & \Rightarrow (-2,3,-1), \\
17 & = & (-1+2\tau^2)(-5+8\tau-2\tau^2) & \Rightarrow (1,-1,2), \\
19 & = & (-2-\tau+2\tau^2)(-3+7\tau-1\tau^2) & \Rightarrow (1,-2,2), \\
29 & = & (2+3\tau)(1-15\tau+9\tau^2) & \Rightarrow (1,2,0).
\end{array}$$

Finally, we give conditions that are necessary and sufficient to represent an integer M by the Tribonacci form.

Theorem 4: A rational integer $M \in \mathbb{Z}$ is represented by the Tribonacci form if and only if its prime decomposition is

$$M = \pm 2^a 11^b \prod_{j=1}^{s} p_j^{m_j} \prod_{h=1}^{r} q_h^{3n_h},$$

where p_j are distinct rational primes that factor in $\mathbb{Z}[\tau]$, and q_h are distinct rational primes in $\mathbb{Z}[\tau]$ with $a, b \geq 0$.

Proof: From the norm product property, it follows that a representation for M is obtained as a product of the prime power factor representations. Therefore, the conclusion stems from the following facts:

a) $\mathbb{Z}[\tau]$ is a PID;

b) let (a_j, b_j, c_j) be a representation of p_j, then $N(a_j\tau + b_j(\tau+1) + c_j\tau^2) = p_j$;

c) any cube $q_h^{3n_h}$ is represented as $(q_h^{n_h}, 0, 0)$, given that 1 is represented as $(1, 0, 0)$;

d) neither $q_h^{3n_h+1}$ nor $q_h^{3n_h+2}$ is represented, because q_h is not represented, and they are not cube-powers. □

5. REMARKS AND CONCLUSIONS

In this paper we have introduced the Tribonacci cubic form $\mathcal{T}(x, y, z)$ and solved the related representation problem. To this end, we have described the Tribonacci ring, namely, the ring of integers in the real cubic field $\mathbb{Q}[\tau]$ containing the real root τ of the Tribonacci polynomial x^3-x^2-x-1. In particular, we have computed the integral basis, the discriminant, the group of the units, and we have shown that the integral ring $\mathbb{Z}[\tau]$ is a principal ideal ring.

The integer representation problem for cubic forms, in general, has unpredictable features, unlike the one for binary quadratic forms. For instance, the equation $z(x^2+y^2)=m$ has a finite number $N(m)$ of solutions for every m, depending on the factorization of m, a solution being the triple $(1,0,m)$. In the Introduction we recalled that the cubic $x^3+y^3+z^3$ despite numerous attempts still remains unsolved (see [12]). Unfortunately, this cubic is neither a Tribonacci cubic nor does it seem to be equivalent to any invariant cubic of a third-order recurrence. Therefore, in this context, cubic forms like the Tribonacci cubic, yielding none or infinitely many representations for every integer, have a rather regular behavior.

In conclusion, although Gauss began the study of integer representations by cubic forms, the theory is far from complete, unlike the theory of binary quadratic forms, but this is a challenging source of beautiful problems.

REFERENCES

1. Z. I. Borevich & I. R. Shafarevich. *Number Theory*. London: Academic Press, 1966.
2. H. Cohn. *Advanced Number Theory*. New York: Dover, 1980.
3. H. Davenport. *The Higher Arithmetic*. New York: Dover, 1983.
4. R. Dedekind. *Theory of Algebraic Integers*. Cambridge: Cambridge University Press, 1996.
5. L. E. Dickson. *History of the Theory of Numbers*. New York: Dover, 1971.
6. F. W. Dodd. *Number Theory in the Quadratic Field with Golden Section Unit*. Passaic: Polygonal Publ. House, 1983.
7. C. F. Gauss. *Disquisitiones Arithmeticae*. New York: Springer-Verlag, 1986.
8. M. D. Hirschhorn. "An Amazing Identity of Ramanujan." *Math. Magazine* **68.3** (1995): 199-201.
9. F. T. Howard. "Generalizations of a Fibonacci Identity." In *Applications of Fibonacci Numbers* **8**:201-11. Ed. G. E. Bergum et al. Dordrecht: Kluwer, 1999.
10. E. Lucas. *Théorie des Nombres*. Paris: Blanchard, 1961.
11. G. A. Miller, H. F. Blichfeldt, & L. E. Dickson. *Theory and Applications of Finite Groups*. New York: Dover, 1961.
12. L. J. Mordel. *Diophantine Equations*. London: Academic Press, 1969.
13. T. Nagel. *Introduction to Number Theory*. New York: Chelsea, 1981.
14. H. Pollard & H. G. Diamond. *The Theory of Algebraic Numbers*. MAA, 1975.
15. P. Samuel. *Algebraic Theory of Numbers*. Paris: Hermann, 1970.
16. S. Vajda. *Fibonacci & Lucas Numbers, and the Golden Section*. Chichester (UK): Ellis Horwood, 1989.
17. B. A. Venkov. *Elementary Number Theory*. Gronigen: Wolters-Noordhoff, 1970.

AMS Classification Numbers: 39A99, 13A17, 13G05

❖❖❖