FUNCTIONAL EQUATION RELATED TO QUADRATIC AND NORM FORMS

G. Alkauskas

The School of Mathematical Sciences, The University of Nottingham, University Park, Nottingham, NG7 2RD, England
(e-mail: giedrius.alkauskas@maths.nottingham.ac.uk)

Abstract. Let $T(a_1, a_2, \dots, a_n)$ be a norm form of some finite proper extension of $\mathbb{Q}$ in a certain fixed integral basis, or even some integer form satisfying certain conditions. We are interested in two problems. One is finding all functions $f\colon \mathbb{Z} \to \mathbb{C}$ satisfying the integer functional equation $f(T(a_1, a_2, \dots, a_n)) = T(f(a_1), f(a_2), \dots, f(a_n))$. Another closely related problem is finding all functions $f\colon \mathbb{Z} \to \mathbb{C}$ such that $T(f(a_1), f(a_2), \dots, f(a_n))$ depends only on the value of $T(a_1, a_2, \dots, a_n)$. The second question was studied before for special quadratic forms. We extend these investigations to other types of quadratic forms and, thus, partially solve the second problem for them. The solution of the first problem for one cubic field is also presented. Finally, we give the corresponding conjecture for the first problem and, additionally, several remarks concerning the choice of norm forms.

Keywords: norm form, square additive functions, integer functional equation.

1. THE FORMULATION OF THE PROBLEM

The questions considered in this article find their origin in the following problem which appeared in “American Mathematical Monthly” (1991) **8**, Problem E 3458:

Find all functions $f\colon \mathbb{N} \to \mathbb{C}$ *satisfying the following integer functional equation*:

$$f\bigl(n^2 + m^2\bigr) = f^2(n) + f^2(m) \quad \textit{for all } n, m \in \mathbb{N},\ n, m \geqslant n_0. \tag{1}$$

If $n_0 = 0$, the problem is a simple exercise in elementary number theory (for a discussion, see the popular article [5]). The case $n_0 = 1$ can be dealt in a similar way, though the proof is longer and more tedious. For arbitrary n_0, the problem can be solved using another method: we first need to derive from (1) (or related equation) a linear recurrence relation satisfied by $f^2(n)$ and then to employ the formal generating power series. This related functional equation appears naturally: if the function f satisfies (1), it certainly implies at least that $f^2(n) + f^2(m)$ depends only on the value of $n^2 + m^2$. Hence, the first task is to solve the related (and, as appears, much more interesting) problem

Find all functions $f\colon \mathbb{N} \to \mathbb{C}$ *satisfying the following integer functional equation*:

$$a^2 + b^2 = c^2 + d^2 \Rightarrow f^2(a) + f^2(b) = f^2(c) + f^2(d) \quad \textit{for integers } a, b, c, d \geqslant n_0. \tag{2}$$

Published in Lietuvos Matematikos Rinkinys, Vol. 45, No. 2, pp. 153–172, April–June, 2005. Original article submitted April 15, 2005.

This type of questions is discussed in [3]. The author introduces the notion of (a,c)-square additive function: a function $G\colon \mathbb{N}\to\mathbb{R}$ is called (a,c)-square additive if the following is satisfied:

$$ax^2+cy^2=au^2+cv^2 \Rightarrow aG(x)+cG(y)=aG(u)+cG(v) \quad \text{for all } x,y,u,v\in\mathbb{N}. \tag{3}$$

Here we can also require that the relation is satisfied only for $x,y,u,v\geqslant n_0$, since this does not give any new essential difficulties in the solution. The (1, 1)-square additive functions are simply called square additive. Then this condition is, of course, nothing else than (2) for $G(n)=f^2(n)$ (without loss of generality, complex numbers can certainly be replaced by real, due to linearity). The author proves, for example, among other things, that:

(i) There are six linearly independent square additive functions;

(ii) every square additive function satisfies the linear recurrence

$$\begin{aligned}G(x+12)&=G(x+9)+G(x+8)+G(x+7)\\&\quad-G(x+5)-G(x+4)-G(x+3)+G(x),\end{aligned}$$

and no linear recurrence of degree less than 12 is satisfied by all square-additive functions;

(iii) if $a>c$ are coprime positive integers, then the set of (a,c)-square additive functions forms a finite dimensional vector space over $\mathbb{R}$.

The first two propositions are already contained in the solution of the problem in discussion in "American Mathematical Monthly." With the kind permission of the author U. Zannier, we reproduce it here, since this unpublished manuscript was written 6 years earlier. The author of [3] also introduces the notion of Pythagorean or P-additive functions. A function $G\colon\mathbb{N}\to\mathbb{R}$ is called P-additive, if

$$z^2=x^2+y^2\Rightarrow G(z)=G(x)+G(y)$$

for integers x,y,z. Then there are at least 17 linearly independent P-additive functions. In addition to the results of [3], in [2], it is proved that if G is P-additive and periodic, then only the primes 2, 3, 5, and 13 can be periods. This question also plays a certain role in our generalization for the above task to other quadratic forms (mainly determining the possible periods of the function $g(n)$ in Theorem below).

These questions give, therefore, impetus for posing more general problems. Here, incidentally, only quadratic forms are involved. Naturally, we can ask the same question for integer forms in several variables. In some cases, we confine ourselves to norm forms in number fields. There are some reasons for that, and these are explained at the end. Hence, we can formulate the two main problems:

PROBLEM 1. *Let $T(a_1,a_2,\dots,a_n)$ be a norm form in some integral basis of some proper field extension of $\mathbb{Q}$ of degree n. Find all functions $f\colon\mathbb{Z}\to\mathbb{C}$ such that*

$$f\bigl(T(a_1,a_2,\dots,a_n)\bigr)=T\bigl(f(a_1),f(a_2),\dots,f(a_n)\bigr). \tag{4}$$

PROBLEM 2. *Let $T(a_1,a_2,\dots,a_n)$ be a norm form in some integral basis of some proper field extension of $\mathbb{Q}$ of degree n. Find all functions $f\colon\mathbb{Z}\to\mathbb{C}$ such that*

$$T\bigl(f(a_1),f(a_2),\dots,f(a_n)\bigr) \text{ depends only on the value of } T(a_1,a_2,\dots,a_n). \tag{5}$$

Here we choose norm forms as slightly more convenient. In fact, the second question can be formulated for any irreducible quadratic form with all three coefficients coprime.

This paper is organized as follows. In Section 2, we give a complete solution for both questions for the form X^2+Y^2. In Section 3, we introduce one special type of quadratic forms

$$q^2X^2+(q^2-2p^2)XY+2p^2Y^2$$

and prove one result on solutions of functional equation

$$G(aX+bY)+G(bX-aY)=G(aX-bY)+G(bX+aY),$$

where $G\colon \mathbb{Z}\to\mathbb{C}$. This result allows us to deduce some important information for Problem 2 for these forms, though it is of independent interest. In another paper on this subject, we will apply these results on Problem 2 to some concrete examples such as the quadratic form $X^2+XY+2Y^2$. In Section 4, the outline for possible solution for general quadratic norm forms is presented, though its implementation would lead to some tiresome calculations. Section 5 is devoted to the complete solution of the first problem for one cubic field generated by the root α of the polynomial X^3-3X+1, with the integral basis $\{1,\alpha,\alpha'\}$, where α' is another root of this polynomial. Finally, in Section 6, we give the corresponding conjecture on the first problem having enough evidence for this. Further, several other questions concerning the second problem are given, and, moreover, several remarks concerning our choice of norm forms are presented. For reference, we formulate the second question for quadratic forms separately.

PROBLEM 2′. *Find all functions $f\colon \mathbb{Z}\to\mathbb{C}$ such that, for all integers X, Y, W, Z,*

$$\begin{aligned}uX^2+vXY+wY^2 &= uZ^2+vZW+wW^2\\ &\Rightarrow uf^2(X)+vf(X)f(Y)+wf^2(Y)\\ &= uf^2(Z)+vf(Z)f(W)+wf^2(W),\end{aligned} \tag{6}$$

where $uX^2+vXY+wY^2$ is an irreducible quadratic form.

2. SOLUTION FOR ONE GAUSSIAN QUADRATIC FORM

As mentioned in Section 1, here we reproduce without changes the solution for both questions for the special Gaussian form X^2+Y^2. We use the unpublished manuscript of U. Zannier (1992), with his kind permission. The result of Proposition 1 is contained in [3], though the latter paper was published 6 years later. In fact, this result also is a partial case of Theorem.

PROPOSITION 1. *Let a function $G\colon \mathbb{N}\to\mathbb{C}$ satisfy the relation: whenever $a^2+b^2=c^2+d^2$ for integers $a,b,c,d\geqslant n_0$, one has $G(a)+G(b)=G(c)+G(d)$. Then*

$$G(n)=An^2+B+C(-1)^n+D(i^n+i^{-n})+E\Big(\frac{n}{3}\Big)^2+F\Big(\frac{n}{5}\Big),$$

where A, B, C, D, E, F are complex constants.

Here $(\frac{n}{p})$ stands for the usual Legendre symbol, and we use its square for brevity simply to get 1 unless $p|n$ when it is 0.

Proof. We have the identity

$$(2n+r)^2+(n-2r)^2=(2n-r)^2+(n+2r)^2.$$

It implies that, for large n and fixed r,

$$G(2n+r)+G(n-2r)=G(2n-r)+G(n+2r). \tag{7}$$

Let us first set $r=1$, then $n-1$, n, $n+1$ in place of n and take the sum of the resulting three equations, obtaining

$$G(2n+3)+G(n-1)+G(n-2)+G(n-3)=G(2n-3)+G(n+1)+G(n+2)+G(n+3).$$

Now set $r=3$ in (7) and subtract from the last equality. We get

$$G(n+6)+G(n-1)+G(n-2)+G(n-3)=G(n-6)+G(n+1)+G(n+2)+G(n+3).$$

Let

$$H(x)=\sum_{n=0}^{\infty}G(n)x^n.$$

Thus, we are working in the field $\mathbb{C}((x))$. The above identity means that $P(x)H(x)$ is a polynomial, where

$$P(x)=x^{12}-x^9-x^8-x^7+x^5+x^4+x^3-1=(x^3-1)(x^4-1)(x^5-1).$$

Hence, $H(x)$ is a rational function with denominator $P(x)$. Expanding it into partial fractions we readily obtain, in view of the factorization of $P(x)$, that, for large n, the following holds:

$$G(n)=An^2+Ln+B+h_3(n)+h_4(n)+h_5(n), \tag{8}$$

where $h_j(n)$ is a periodic function of period j. Putting this into (7), we readily find $L=0$ and, due to the fact that $3,4$, and 5 are pairwise coprime, we deduce that h_j satisfies (7) in place of G for $j=3,4,5$. A brief inspection shows the exact appearance of each of these periodic functions, which completes the proof of Proposition 1, and, therefore, the second question for the form X^2+Y^2. Using this result, we can solve the first question.

PROPOSITION 2. *Let $f\colon\mathbb{N}\to\mathbb{C}$ satisfy*

$$f\big(a^2+b^2\big)=f^2(a)+f^2(b)$$

for all integers $a,b\geqslant n_0$. Then, for large n, either $f^2(n)=n^2$, either $f(n)\equiv 0$, or $f^2(n)\equiv 1/4$.

Proof. Formula (8), together with $L=0$, is, anyway, sufficient for the proof of this statement, the precise form of h_j being immaterial for our purpose. In fact, the function $G(n)=f^2(n)$ satisfies the above hypotheses, whence, for large n,

$$f^2(n)=An^2+h(n), \tag{9}$$

$h(n)$ being a periodic function with period 60 (we can, of course, incorporate the constant B into this periodic function). Now fix $b,c\geqslant n_0$. Set then $a=60n+c$. Due to the condition on f and (9), the function

$$P(n)=f^2\big(a^2+b^2\big)=A\big((60n+c)^2+b^2\big)^2+h\big(a^2+b^2\big)$$

is a square of the polynomial in n

$$Q(n)=f^2(a)+f^2(b)=A(60n+c)^2+h(c)+f^2(b).$$

Suppose now that f is unbounded, that is, $A\neq 0$. Denoting by R^2 the first square in the expression of P, we derive

$$\big(\sqrt{A}R\big)^2+h\big(a^2+b^2\big)=Q^2.$$

Since both R and Q are quadratic polynomials, we verily derive $h(a^2+b^2)=0$, whence

$$A\big(x^2+b^2\big)^2=\big(Ax^2+h(c)+f^2(b)\big)^2.$$

So $A=1$ and, since the left-hand side is independent of c, h must be constant, necessarily equal to 0 (since already $h(a^2+b^2)=0$). This completes the proof in the case $A\neq 0$. Formula (8) enables one also to deal with the case $A=0$: a straightforward inspection shows that then $f^2(n)$ necessarily is a constant (0 or $1/4$) for large n. This completes the proof of Proposition 2 and, hence, the first problem for the form X^2+Y^2.

3. A SPECIAL TYPE OF QUADRATIC FORMS

As mentioned above, in [3], it is proved that all functions $G\colon \mathbb{N} \to \mathbb{C}$ satisfying (3) with a and c coprime, form a finite-dimensional vector space over $\mathbb{C}$. Here we prove a similar result for one special type of quadratic forms. We begin with introductory notes explaining why we deal here with this special type.

Let $uX^2 + vXY + wY^2$ with $v \neq 0$ be a quadratic form satisfying the identity

$$u(aX+bY)^2 - v(aX+bY)(aX-bY) + w(aX-bY)^2 = uX^2 + vXY + wY^2 \tag{10}$$

for certain rational a and b. If a function f satisfies (6), then

$$f(X)f(-Y) = f(X)f(-Y)$$

(since $u+v+w \neq 0$, otherwise, $v^2 - 4uv$ is a perfect square). Then, first taking the equation

$$\begin{aligned} &f^2(aX+bY) + vf(-aX-bY)f(aX-bY) + wf^2(aX+aY) \\ &\quad = uf^2(X) + vf(X)f(Y) + wf^2(Y), \end{aligned}$$

second, the same equation with $-Y$ instead of Y, third, two more equations obtained from these by exchanging the roles of X and Y, and, finally, adding all four with suitable signs, we, thus, obtain (having in mind the identity $f^2(X) = f^2(-X)$)

$$(u-w)\big(f^2(aX+bY) - f^2(aX-bY) - f^2(bX+aY) + f^2(bX-aY)\big) = 0. \tag{11}$$

Thus, unless $u - w = 0$, we are able to treat this identity in a similar way as in Section 2, first multiplying, of course, (10) by the square of the common denominator of a and b.

In order to exist rational a and b satisfying identity (10), the following system of linear equations should have a nonzero solution:

$$\begin{cases} (a^2-1)u - a^2v + a^2w = 0, \\ b^2u + b^2v + (b^2-1)w = 0, \\ 2abu - v - 2abw = 0. \end{cases}$$

The determinant is

$$-(2ab-1)(2ab+a+b+1)(2ab-a-b+1).$$

If the second or third multiplier is 0, then the corresponding solutions u, v, and w give a degenerate quadratic form. The remaining case $a = 1/2b$ gives $u = r$, $v = (1-2b^2)r$, and $w = 2b^2r$. Since here $u \neq w$, thus, we obtain the special type of quadratic forms

$$q^2X^2 + (q^2 - 2p^2)XY + 2p^2Y^2$$

(p and q are coprime integers, q odd) for which this trick works with $a = q^2$ and $b = 2p^2$: that is, starting from the identity

$$\begin{aligned} &q^2(q^2X+2p^2Y)^2 - (q^2-2p^2)(q^2X+2p^2Y)(q^2X-2p^2Y) + 2p^2(q^2X-2p^2Y)^2 \\ &\quad = q^2(2pqX)^2 + (q^2-2p^2)(2pqX)(2pqY) + 2p^2(2pqY)^2, \end{aligned}$$

we, thus, obtain identity (11) in the above way. This type includes, for example, the following quadratic forms:

$$X^2 - XY + 2Y^2 \quad \text{with discriminant } D = -7;$$

$$9X^2 + XY + 8Y^2 \quad \text{with } D = -71;$$

$$X^2 - 7XY + 8Y^2 \quad \text{with } D = 17.$$

These forms generally are not norm forms for negative discriminants, except the first case, though, as mentioned, Problem $2'$ can be formulated for them as well.

Now let $f^2(x) = G(x)$. Thus, we have the functional equation

$$G(aX + bY) + G(bX - aY) = G(aX - bY) + G(bX + aY). \tag{12}$$

THEOREM. *Suppose that a function G: $\mathbb{N} \to \mathbb{C}$ satisfies* (12) *for certain coprime positive integers a and b, one of them being even. Then $G(n) = g(n) + An^2$, where A is a complex constant, and $g(n)$ is a periodic function with period depending only on a and b.*

The proof of this theorem is contained in the next three lemmas. This result is of independent interest, nevertheless, we will apply it to our needs, that is, to the following corollary.

COROLLARY. *If the quadratic form in Problem $2'$ is of the form*

$$q^2X^2 + (q^2 - 2p^2)XY + 2p^2Y^2,$$

where p and q are coprime integers, and q is odd, then the function f: $\mathbb{Z} \to \mathbb{C}$ satisfying (6)*, is of the form $f^2(n) = An^2 + g(n)$, where A is a complex constant, and g is a periodic function with period depending only on p and q. Therefore, $f^2(n)$ belongs to a finite-dimensional vector space over $\mathbb{C}$.*

Naturally, since condition (6) for $v \neq 0$ is not linear, we cannot claim that solutions form a vector space.

Proof. The proof of Corollary is nothing else but considerations in the beginning of this section.

LEMMA 1. *Suppose that a complex function G: $\mathbb{N} \to \mathbb{C}$ satisfies* (12) *with certain coprime positive integers a and b, not both equal to* 1. *Then the generating power series*

$$H(x) := \sum_{n=0}^{\infty} G(n)x^n$$

is a rational function $\frac{P(x)}{Q(x)}$, where $P(x) \in \mathbb{C}[x]$, and $Q(x)$ is an integer monic polynomial with free coefficient ± 1.

Proof. Take, in this identity, $Y = sa$ with some fixed s, $X = n + sbk$, and sum both expressions for $k = 1$ and $k = -1$. Thus, we obtain

$$\begin{aligned} &G(an + 2sab) + G(bn - sa^2 + sb^2) + G(bn - sa^2 - sb^2) \\ &\quad = G(an - 2sab) + G(bn + sa^2 + sb^2) + G(bn + sa^2 - sb^2). \end{aligned}$$

Now subtracting (12) with $X = n$ and $Y = 2sa$ from this expression, we obtain

$$\begin{aligned} &G(bn + 2sa^2) + G(bn - sa^2 + sb^2) + G(bn - sa^2 - sb^2) \\ &\quad = G(bn - 2sa^2) + G(bn + sa^2 + sb^2) + G(bn + sa^2 - sb^2). \end{aligned} \tag{13}$$

Naturally, we can also get a similar identity with a and b exchanged; hence, we can assume $b > a$ in the above. Then $a^2 + b^2 > 2a^2$, and it is coprime with b, hence, the product $s(a^2 + b^2)$ can have any residue modulo b. Therefore, we have proved that (12) implies the following recurrence relation which holds for any positive integers n and w:

$$G(bn + w) = \sum_{i=1}^{T} A_{i,w} G(bn + w - i); \tag{14}$$

here T is some fixed integer (depending only on a and b), and $A_{i,w}$ are some integers from the set $\{-1, 0, 1\}$ depending actually on i and w (mod b) only. From (13) we also see that the last nonzero term in (14) is $G(bn' - w)$ (this fact will later imply that $Q(x)$ is monic).

Finally, denote the formal power series

$$\sum_{n=0}^{\infty} G(bn+w)x^{bn+w} := H_w(x).$$

Hence, we are working in the field $\mathbb{C}((x))$. Take now, in (14), w any in the range $0, 1, \ldots, b-1$, multiply this equality by x^{bn+w} and sum over all nonnegative n such that $bn + w - T \geqslant 0$. Thus, we obtain the system of linear equations

$$H_w(x) + p_w(x) = \sum_{w'=0}^{b-1} P_{w,w'}(x) H_{w'}(x), \quad w = 0, 1, \ldots, b-1. \tag{15}$$

where $p_w \in \mathbb{C}[x]$ and $P_{w,w'} \in \mathbb{Z}[x]$. Further, for each w, one and only one of $P_{w,w'}$ has a maximal degree with leading coefficient $+1$, precisely, $P_{w,b-w}$. Moreover, in the matrix of this linear system only diagonal terms have free coefficients equal to -1.

Hence, if such a function $G(n)$ does exist, the corresponding power series necessarily satisfies the system of linear equations, hence, all H_w are, in fact, rational functions, whence

$$H(x) = \sum_{n=0}^{\infty} G(n)x^n = \sum_{w=0}^{b-1} H_w(x) = \frac{P(x)}{Q(x)}.$$

$Q(x)$ is a $\mathbb{Z}[x]$-factor of the determinant of the above system, and since, in each row, only $P_{w,b-w}$ has a maximal degree and is monic, the determinant and, hence, $Q(x)$ itself is monic. More importantly, by the remarks above, the free coefficient of $Q(x)$ is ± 1, which completes the proof of Lemma 1.

By a more thorough inspection of the proof of Lemma 1 it can be traced that the main part of this rational function is a polynomial with degree d less that $2b(a^2+b^2)$. Now separating this main part and expanding the proper rational function into simple fractions, we, therefore, obtain the finite sum

$$G(n) = \sum_{i,k} C_{i,k} n^i \xi_k^n \quad \text{for } n \geqslant d, \tag{16}$$

where ξ_k are reciprocals of the roots of $Q(x)$; hence, algebraic integers (moreover, units), and $C_{i,k} \neq 0$ are some complex constants.

LEMMA 2. *Let the function $G\colon \mathbb{N} \to \mathbb{C}$ defined by* (16) *satisfy* (12). *Then all ξ_k are roots of unity.*

Proof. Suppose that some of ξ_k have absolute value greater than 1. Choose all with maximal absolute value $r > 1$, and let ξ_k, $1 \leqslant k \leqslant T$, be all of them with maximal $i = I$. In (12), choose $X = k$ and $Y = l$ so that all

$$d_1 = ak + bl, \qquad d_2 = bk - al, \qquad d_3 = ak - bl, \quad \text{and} \quad d_4 = bk + al$$

are distinct and positive. For this, it is sufficient that

$$(k \pm l)a \neq (k \mp l)b \quad \text{and} \quad \frac{k}{l} > \max\left\{\frac{b}{a}, \frac{a}{b}\right\}.$$

Since a and b are coprime, the greatest of these d_i (say, $d_1 = L$) can attain any sufficiently large integral value (say, all values $L \geqslant S$). Substitute (16) into (12) with $X = kn$ and $Y = ln$. Consider the part of this sum

$$\sum_{k=1}^{T}(nL)^I C_{I,k} \cdot \xi_k^{Ln} := E_n.$$

Let $\arg(\xi_k) = \phi_k$. If $E_{n_0} \neq 0$ for some n_0 exceeding our bound, then arbitrarily choosing large n such that $nn_0\phi_k = n_0\phi_k + \varepsilon_{n,k} \pmod{2\pi}$, $\varepsilon_{n,k} \to 0$, we, thus, obtain $|E_{nn_0}| > \delta(n^I r^{nn_0})$, and since then E_{nn_0} is a dominant term, identity (12) cannot be satisfied (such a choice of n is always possible as one can see from the proof below). Thus, $E_n = 0$ for all n exceeding our bound:

$$\sum_{k=1}^{T} C_{I,k} \cdot \xi_k^{Ln} = 0.$$

It is easy to see that there exists $L \geqslant S$ such that all $L\phi_k$ as angles are arbitrarily close to 0. In fact, consider all T-tuples

$$\mathbf{a}_L = \left(\frac{L\phi_1}{2\pi}, \frac{L\phi_2}{2\pi}, \ldots, \frac{L\phi_T}{2\pi}\right) \pmod 1, \quad L \in \mathbb{N},\ L \geqslant S,$$

as points in the T-dimensional unit cube. Let $\mathcal{C}$ be the closure of this set. Hence, for every ε, there exists a finite integer N such that each $\mathbf{b} \in \mathcal{C}$ is at a distance at most ε from at least one $\mathbf{a}_{L'}$, $L' = S, S+1, S+N$. Hence, this is true for $\mathbf{b} = \mathbf{a}_L$. Taking $L \geqslant 2S + N$ and finding such L', we get that $L - L' \geqslant S$ and $\mathbf{a}_{L-L'}$ is close to some vertex of the unit cube. Therefore, $\mathbf{a}_{L-L'+1}$ is arbitrarily close to $\mathbf{a}_1$. Since, in our case, all ϕ_i are different, we can choose $L \geqslant S$ such that $\mathbf{a}_L$ will also have all different coordinates.

Now, in the above equality, take L such that all ξ_k^L are different, let n attain T consecutive sufficiently large values, and consider this as a system of linear equations for $C_{I,k}$, $1 \leqslant k \leqslant T$. The corresponding determinant will be a nonzero multiple of the Vandermonde determinant

$$\det\left(\xi_k^{Ln}\right)_{k,n=1}^{T},$$

hence, it is nonzero, and, therefore, all $C_{I,k}$ are zeros, a contradiction. Hence, all algebraic integers in (16) satisfy $|\xi_k| \leqslant 1$.

To finish, suppose that some ξ in (16) has a conjugate ξ' for which $|\xi'| > 1$. Let $\mathbf{L}$ be the normal closure of $\mathbb{Q}(\xi)$. Consider the automorphism of $\mathbf{L}$ which maps ξ to ξ'. Extend this automorphism to $\mathbb{C}$ and denote it by σ (such an extension is always possible; see [4], Chapter VIII). Applying σ to Eq. (12), we see that $G'(n) := \sigma G(n)$ satisfies the same relation, and applying σ to (16), we, therefore, obtain a similar expression for $G'(n)$, only with each $C_{i,k}$ replaced by $\sigma C_{i,k}$ and ξ_k by $\sigma\xi_k$. Here $|\sigma\xi| > 1$, which, as we have seen, cannot occur (here we use the trivial fact that σ maps nonzeros to nonzeros). Therefore, all algebraic integers in (16) have conjugates only on or inside the unit circle, and, therefore, Kronecker's theorem (see [1]) implies that they are roots of unity. Lemma 2 is proved.

Therefore, expression (16) can be simplified to

$$G(n) = \sum_{i=0}^{I} n^i g_i(n), \tag{17}$$

where g_i are periodic functions with finite periods.

LEMMA 3. *If a function* $G\colon \mathbb{N} \to \mathbb{C}$ *of the form* (17) *satisfies* (12) *with coprime positive integers a and b, one of these being even, then* $G(n) = g(n) + An^2$, *where* $g(n)$ *is a periodic function with finite period, and A is a complex constant.*

Proof. Suppose that the last nonzero periodic function in (17) is g_I, $I \geqslant 3$. Let the period of g_I be M. Putting (17) into (12), consider one part

$$\begin{aligned} W(X,Y) := {} & (aX+bY)^I g_I(aX+bY) + (bX-aY)^I g_I(bX-aY) \\ & - (aX-bY)^I g_I(aX-bY) - (bX+aY)^I g_I(bX+aY). \end{aligned}$$

When X and Y run through $X \equiv X_0 \pmod{M}$ and $Y \equiv Y_0 \pmod{M}$, the second multipliers in the expression of $W(X,Y)$ are constant, say h_1, h_2, h_3, and h_4. Then $W(X,Y)$ is a homogeneous polynomial of degree I, and, unless it is zero, it is a dominant term in the obtained expression, and we get a contradiction. Hence,

$$(aX+bY)^I h_1 + (bX-aY)^I h_2 - (aX-bY)^l h_3 - (bX+aY) h_4 \equiv 0.$$

This is valid for $X \equiv X_0 \pmod{M}$ and $Y \equiv Y_0 \pmod{M}$, but since it is a polynomial, all its coefficients must be zero.

Therefore, we have $I+1$ linear conditions for four unknowns h_i, $1 \leqslant i \leqslant 4$. Since $I \geqslant 3$, choose the first four of them. Then $\mathcal{A}z = \mathbf{o}$, where z is the column $(h_1,h_2,h_3,h_4)^T$, $\mathbf{o}$ is the column $(0,0,0,0)^T$, and $\mathcal{A}$ is the 4×4 matrix

$$\mathcal{A} = \begin{pmatrix} a^I & b^I & -a^I & -b^I \\ a^{I-1}b & -b^{I-1}a & a^{I-1}b & -b^{I-1}a \\ a^{I-2}b^2 & b^{I-2}a^2 & -a^{I-2}b^2 & -b^{I-2}a^2 \\ a^{I-3}b^3 & -b^{I-3}a^3 & a^{I-3}b^3 & b^{I-3}a^3 \end{pmatrix}.$$

The determinant is

$$4a^{2I-4}b^{2I-4}(a-b)^2(a+b)^2(a^2+b^2)^2 \neq 0,$$

hence, all $h_i = 0$.

In particular, $h_1 = g_I(aX+bY) = 0$, and since this argument can attain any residue modulo M, this implies $g_I(X) \equiv 0$, a contradiction, whence $I \leqslant 2$.

If $I = 2$, we obtain a similar system of three linear equations for h_i with the matrix consisting of the first three rows of $\mathcal{A}$ with $I = 2$. Since this matrix has rank 3, the space of solutions has rank 1, and solving we obtain

$$g_2(aX+bY) = g_2(bX-aY) = g_2(aX-bY) = g_2(bX+aY) \quad \text{for all } X, Y.$$

Let g_2 have a period M. Choose any residue w_0 modulo M, sufficiently large $w \equiv w_0 \pmod{M}$, and a', b' such that $ab' + ba' = w$. Let $X = b' + as$ and $Y = a' + bs$. From the first equality above we obtain

$$g_2\big(w + s(a^2+b^2)\big) = g_2(bb' - aa'), \quad s \in \mathbb{N},$$

hence, a^2+b^2 is a period. From the second equality we get in the same way that b^2-a^2 also is a period. Since, in our case, a and b are coprime and one of them is even, a^2+b^2 and b^2-a^2 are also coprime, whence we get that 1 also is a period, and, therefore, $g_2(n) \equiv A$.

Thus,

$$G(n) = g(n) + h(n)n + An^2.$$

Let M be the smallest period of $h(n)$.

Putting this again into (12), we see that the squares vanish, and similar considerations show that

$$\begin{cases} ah_1 + bh_2 - ah_3 - bh_4 = 0, \\ bh_1 - ah_2 + bh_3 - ah_4 = 0, \end{cases}$$

for

$$h_1 = h(aX+bY), \qquad h_2 = h(bX-aY), \qquad h_3 = h(aX-bY), \quad \text{and} \quad h_4 = h(bX+aY).$$

Suppose by symmetry that $a > b$. Now denote $M(M,b)^{-1}$ by M', where (M,b) stands, as usual, for the greatest common divisor. Let $Y = M's$ in the above equalities. Since $M'b$ is divisible by M and since M is a period, the first equality implies

$$h(bX - aM's) = h(bX + aM's).$$

The second equality gives

$$2bh(aX) = ah(bX - aM's) + ah(bX + aM's),$$

and, therefore,

$$bh(aX) = ah(bX + aM's).$$

Further, since b and aM' are coprime, the argument $bX + aM's$ can attain any residue modulo M for X, s varying. Choose w such that $T = |h(w)|$ is maximal, and let X and s satisfy $bX + aM's \equiv w \pmod{M}$. Then we get $bT \geqslant aT$, and since $a > b$, verily $T = 0$ and $h(n) \equiv 0$.

To finish the proof of Theorem, we need to prove the last statement on the period of this periodic function $g(n)$. But all roots of unity appearing in its Fourier expansion are roots of the determinant of the linear system (15), and the latter depends only on a and b.

It seems plausible that, in fact, $g(n)$ can be decomposed into three periodic functions

$$g(n) = g_{2ab}(n) + g_{a^2+b^2}(n) + g_{|a^2-b^2|}(n),$$

where g_i is periodic with period i (this is, of course, somehow stronger statement than that $g(n)$ has a period $2ab(a^2+b^2)|a^2-b^2|$). We do not give a proof of this here, since concrete examples will be studied in a continuation of this paper. Moreover, in the formulation of Theorem, the additional conditions $X, Y \geqslant n_0$, and the same condition for all arguments appearing there, e.g., $bX - aY \geqslant n_0$, will not make the proof more difficult. This is obvious from a more detailed inspection of the proof of all three lemmas. For example, when we are dealing with periodic functions, small arguments can be replaced by arbitrarily large.

4. OUTLINE FOR A GENERAL QUADRATIC FORM

In this section, we are dealing with quadratic forms and Problem 2′. Our aim is to derive, for a general quadratic form and a function f satisfying (6), a statement similar to Corollary of Theorem. Here we give a short outline for a possible solution and confine ourselves to norm forms in quadratic extensions.

Hence, let, for simplicity, $P \equiv 2 \pmod 4$ or $P \equiv 3 \pmod 4$, and let $\alpha = a + c\sqrt{P}$ and $\beta = b + d\sqrt{P}$ be a given integral basis of the field

$$\mathbf{K} = \mathbb{Q}(\sqrt{P}), \qquad ad - bc = 1.$$

Let $(\alpha', \beta') = (\alpha, \beta)A$; here and in the sequel, α' means the conjugate of α under the nontrivial automorphism of $\mathbf{K}$. Then

$$A = \begin{pmatrix} i & k \\ j & -i \end{pmatrix},$$

where $i = ad + bc$, $j = -2ac$, and $k = 2bd$. Further, let

$$\mathrm{Tr}\,\alpha^2 = e = 2a^2 + 2c^2P, \qquad \mathrm{Tr}(\alpha\beta) = f = 2ab + 2cdP, \quad \text{and} \quad \mathrm{Tr}\,\beta^2 = g = 2b^2 + 2d^2P.$$

Then $eg - f^2 = \mathrm{disc}(\mathbf{K})$ and also $\mathrm{Tr}\alpha = 2a$, $\mathrm{Tr}\beta = 2b$. Let

$$\mathcal{N}(X\alpha + Y\beta) = uX^2 + vXY + wY^2.$$

We will follow the pattern of the proof in Section 3. The first task is “eliminating” the middle terms by applying linear combinations of norm forms for certain values of X and Y. Hence, we need some parameterization of solutions of the following system of equations in $A, B, \ldots, H$:

$$\begin{cases} uA^2 + vAB + wB^2 = uC^2 + vCD + wD^2, \\ uD^2 + vCD + wC^2 = uE^2 + vEF + wF^2, \\ uF^2 + vEF + wE^2 = uG^2 + vGH + wH^2, \\ uH^2 + vGH + wG^2 = uB^2 + vAB + wA^2. \end{cases} \tag{18}$$

For $A\alpha + B\beta$ and $C\alpha + D\beta$ to have equal norms, it is sufficient that

$$A\alpha + B\beta = \pi_1\sigma_1 \quad \text{and} \quad C\alpha + D\beta = \pi_1\sigma_1'$$

for some algebraic integers $\pi_1, \sigma_1 \in \mathbf{K}$. (In view of Hilbert’s theorem 90 (see [4], p. 288), such a decomposition is also necessary at least with fractional π_1, σ_1.) Therefore, the existence of algebraic integers π_i, σ_i, $1 \leqslant i \leqslant 4$, such that

$$\begin{cases} A\alpha + B\beta = \pi_1\sigma_1, \ C\alpha + D\beta = \pi_1\sigma_1', \\ D\alpha + C\beta = \pi_2\sigma_2, \ E\alpha + F\beta = \pi_2\sigma_2', \\ F\alpha + E\beta = \pi_3\sigma_3, \ G\alpha + H\beta = \pi_3\sigma_3', \\ H\alpha + G\beta = \pi_4\sigma_4, \ B\alpha + A\beta = \pi_4\sigma_4', \end{cases} \tag{19}$$

is sufficient. Let us consider all $\pi_i = p_i\alpha + q_i\beta$ fixed and $\sigma_i = x_i\alpha + y_i\beta$ as unknown. Each equality above gives two linear conditions for $A, B, \ldots, H$ and x_i, y_i; therefore, we totally have 16 unknowns. To simplify, add, for example, first two, further first and conjugate of the second, and, finally, take the trace of the first. Therefore, we have three equations

$$\begin{cases} (A + C)\alpha + (B + D)\beta = \pi_1 \mathrm{Tr}\sigma_1, \\ (A + iC + kD)\alpha + (B + jC - iD)\beta = \sigma_1 \mathrm{Tr}\pi_1, \\ 2Aa + 2Bb = \mathrm{Tr}(\pi_1\sigma_1). \end{cases}$$

This gives five linear conditions instead of four but they are dependent. We will choose four of them, equivalent to the initial. In fact, since both a and b cannot be 0, without loss of generality, we can consider $\mathrm{Tr}(\beta) = 2b \neq 0$. Hence, if T is the matrix

$$T = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & i & k \\ 2a & 2b & 0 & 0 \end{pmatrix},$$

then

$$\det(T) = 2ak - 2bi + b = \mathrm{Tr}(\beta') + 2b = 4b \neq 0.$$

Therefore, the first two equalities of (19) are equivalent to the following system of linear equations:

$$\begin{cases} A + C - 2p_1ax_1 - 2p_1by_1 = 0, \\ B + D - 2q_1ax_1 - 2q_1by_1 = 0, \\ A + iC + kD - (2p_1a + 2q_1b)x_1 = 0, \\ 2Aa + 2Bb - (ep_1 + fq_1)x_1 - (fp_1 + gq_1)y_1 = 0. \end{cases}$$

In a similar way, each pair of equations in (19) gives four linear equations. Therefore, finally, we get

$$(A, B, \dots, H, x_1, y_1, \dots, x_4, y_4)\mathcal{R} = (0, 0, \dots, 0),$$

where $\mathcal{R}$ is a 16×16 square matrix. If we consider p's, q's, x's, and y's to be rational, then, except possible cases where some π_i is a rational multiple of α, we can always achieve all $q_i = 1$ (by replacing a pair π_i, σ_i in (19) by a pair $\sigma_i q_i$ and π_i / q_i). Hence, the determinant of $\mathcal{R}$ is a cyclic polynomial in p_1, p_2, p_3, and p_4 of degree at most 8, and degree at most 2 in each p_i. This polynomial depends only on a, b, c, d, and P. Suppose now that we are able to choose rational p's such that the matrix $\mathcal{R}$ has rank at most 14. Then, if a function $\mathbb{Z} \to \mathbb{C}$ satisfies (6), summing all equations corresponding to the equalities in (18), we obtain

$$(u - w)\big(f^2(A) + f^2(D) + f^2(F) + f^2(H) - f^2(B) - f^2(C) - f^2(E) - f^2(G)\big) = 0,$$

where $A, B, \dots, H$ are linear forms in two variables, and an analogue of Theorem would imply that, necessarily, $f^2(n) = An^2 + g(n)$, where A is a complex constant, and $g(n)$ is a periodic function. Hence, to implement this, we first need to choose suitable p's. In several special choices of a, b, c, and d, this can be done. Unfortunately, we are unable to give a more exhaustive treatment of this here, and the corresponding investigations will be presented in a continuation of this paper.

5. ONE CUBIC FIELD

As mentioned in Introduction, here we deal with Problem 1 for one normal cubic field. This method allows one to solve this problem for quadratic norm forms such as

$$X^2 + Y^2, \qquad X^2 + 5Y^2, \qquad X^2 - 6Y^2, \quad \text{and} \quad X^2 + XY + 2Y^2.$$

We skip this, since, in the first three cases or even in the case $X^2 + DY^2$, it can be solved using the result of [3], and the method is similar to that of the proof of Proposition 2. We also skip the last case, since the proof uses the same induction as in the cubic field case, which we will present now.

Consider the polynomial

$$h(X) = X^3 - 3X + 1.$$

It has the discriminant 81, and since it is the perfect square, the splitting field of $h(X)$ is cubic. Since $\mathrm{disc}(h) > 0$, all roots are real. Let α be one of them. Then the Galois group $\mathrm{Gal}(\mathbf{K}/\mathbb{Q})$ is cyclic of order 3, where $\mathbf{K} = \mathbb{Q}(\alpha)$. We will show that $\{1, \alpha, \alpha^2\}$ is an integral basis of the ring of integers $\mathcal{O}_{\mathbf{K}}$ in $\mathbf{K}$. Since

$$81 = \mathrm{disc}\big(h(X)\big) = D(1, \alpha, \alpha^2) = \mathrm{disc}(\mathcal{O}_{\mathbf{K}}/\mathbb{Z}) \cdot (\mathcal{O}_{\mathbf{K}}\colon\ \mathbb{Z}[\alpha])^2 \quad \text{and} \quad \mathrm{disc}(\mathcal{O}_{\mathbf{K}}/\mathbb{Z}) > 1,$$

we have only to verify that $(\mathcal{O}_{\mathbf{K}}\colon\ \mathbb{Z}[\alpha])$ is not equal to 3. Suppose that it is. Let ω_1, ω_2, and ω_3 be an integral basis of $\mathcal{O}_{\mathbf{K}}$. Then there exists an integer square matrix A of order 3 with determinant 3 such that $(\omega_1, \omega_2, \omega_3) \cdot A = (1, \alpha, \alpha^2)$. Changing the integral basis ω and matrix A, we can achieve it to be of the Hermite normal form (see [6], p. 35 for details). Hence, it has one of the three following forms:

$$\begin{pmatrix} 1 & 0 & \kappa \\ 0 & 1 & \eta \\ 0 & 0 & 3 \end{pmatrix}; \qquad \begin{pmatrix} 1 & \delta & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix}; \qquad \begin{pmatrix} 3 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix};$$

where η, κ, and δ are integers from the set $\{-2, -1, 0\}$. Rename the new integral basis again in $\{\omega_1, \omega_2, \omega_3\}$. Then, in the third case, we get that $3\omega_1 = 1$, hence, $\frac{1}{3}$ is an integer, a contradiction. In the first case, we get

$$\omega_1 = 1, \qquad \omega_2 = \alpha, \quad \text{and} \quad \alpha^2 = \kappa\omega_1 + \eta\omega_2 + 3\omega_3 = \kappa + \eta\alpha + 3\omega_3.$$

Therefore, $\frac{1}{3}(\alpha^2+\eta\alpha+\kappa)$ is an algebraic integer for certain κ and η, $0\leqslant\kappa,\eta\leqslant 2$, and we should only verify that it is not. Suppose that it is. Then

$$\mathcal{N}_{\mathbf{K}/\mathbb{Q}}(\alpha^2+\eta\alpha+\kappa)=1+3\eta+9\kappa+6\kappa^2+3\eta\kappa-3\eta^2\kappa-\eta^3+\kappa^3\equiv 0 \pmod{27}.$$

Now, a simple check shows that no pair (κ,η), $0\leqslant\kappa,\eta\leqslant 2$, satisfies this congruence.

In the second case, $\omega_1=1$ and $\alpha=\delta\omega_1+3\omega_2$, hence, $\frac{1}{3}(\alpha+\delta)$ is an algebraic integer for certain δ, $0\leqslant\delta\leqslant 2$. Therefore,

$$\mathcal{N}_{\mathbf{K}/\mathbb{Q}}(\alpha+\delta)=\delta^3-3\delta+1\equiv 0 \pmod{27}\quad\text{for some } \delta,\ 0\leqslant\delta\leqslant 2,$$

which is not satisfied. Hence, $\{1,\alpha,\alpha^2\}$ is an integral basis for $\mathcal{O}_{\mathbf{K}}$ and $\operatorname{disc}(\mathcal{O}_{\mathbf{K}}/\mathbb{Z})=81$. The polynomial $h(X)$ factors over $\mathbb{Q}(\alpha)$ as

$$(X-\alpha)\big(X-(\alpha^2-2)\big)\big(X-(-\alpha^2-\alpha+2)\big).$$

Let $\alpha'=\alpha^2-2$, $\alpha''=-\alpha^2-\alpha+2$. Therefore, $\{1,\alpha,\alpha'\}$ is also an integral basis, and, henceforth, we fix this one. The norm form in this basis is

$$\begin{aligned}T(a,b,c)&=\mathcal{N}(a+b\alpha+c\alpha')\\&=a^3-b^3-c^3-3ab^2-3ac^2+3abc+6b^2c-3bc^2.\end{aligned}\tag{20}$$

Thus, we have the functional equation for the function $f\colon\mathbb{Z}\to\mathbb{C}$

$$T\big(f(a),f(b),f(c)\big)=f\big(T(a,b,c)\big).\tag{21}$$

Thus, here we will prove the following statement, which solves Problem 1 for this cubic field.

PROPOSITION 3. *Let the form T be defined by* (20). *Then all functions $f\colon\mathbb{Z}\to\mathbb{C}$ satisfying* (21) *are the following*:

$$f(n)=n,\qquad f(n)=-n,\qquad f(n)\equiv 0,\qquad f(n)\equiv i,\quad\textit{or}\quad f(n)\equiv -i.$$

Proof. We have

$$\mathcal{N}(1+\alpha)=-3\quad\text{and}\quad\mathcal{N}(n+m\alpha)=n^3-3nm^2-m^3,$$

and also

$$\mathcal{N}\big((1+\alpha)(n+m\alpha)\big)=\mathcal{N}\big((1+\alpha')(n+m\alpha)\big)=\mathcal{N}\big((1+\alpha'')(n+m\alpha)\big).$$

This, in terms of T, gives the following identities:

$$T(n+2m,n+m,m)=T(n-m,n+m,m)=T(n-m,n-2m,-2m)$$

and, in the special case $m=1$,

$$T(n+2,n+1,1)=T(n-1,n+1,1)=T(n-1,n-2,-2).\tag{22}$$

Now, Eq. (21) with $a=b=c=0$ gives $f(0)=-f^3(0)$. That is, $f(0)=0$, $f(0)=i$, or $f(0)=-i$. The last two cases lead to the solutions $f(n)\equiv i$ and $f(n)\equiv -i$, respectively. We skip the proofs, since the method is similar to the following proof. Suppose that $f(0)=0$. Then $b=c=0$ gives $f(a^3)=f^3(a)$, and, for $a=1$, we derive $f(1)=0$ (which leads to the solution $f(n)\equiv 0$), $f(1)=1$, or $f(1)=-1$. Now, if f satisfies (21), then also $-f$ does, since T is a form of odd degree. Therefore, without loss of generality, we can assume that $f(1)=1$. Substitution $a=a$, $b=-a$, $c=0$ gives

$$f(-a^3)=f^3(a)-f^3(-a)-3f(a)f^2(-a);$$

since $f(-a^3)=f^3(-a)$, we obtain

$$f^3(a)-3f(a)f^2(-a)-2f^3(-a)=0.$$

This implies that, in the case $f(-a)=0$, we also have $f(a)=0$; in the case $f(-a)\neq 0$, the ratio $\frac{f(a)}{f(-a)}=Y$ satisfies the equation $Y^3-3Y-2=0$. Hence, it is equal to -1 or 2. The latter is impossible, since $\frac{f(-a)}{f(a)}=\frac{1}{2}$ cannot occur by the same reason. Therefore, $f(-a)=-f(a)$ in all cases.

Further, $a=b=1$ and $c=0$ gives $f(-3)=-3$, and then also $f(3)=3$. The first and third terms of identity (22) for $n=-1$ give

$$-3=T(1,0,1)=T(-2,-3,-2)=-T(2,3,2).$$

Therefore, $T(2,3,2)=3$ and

$$f\big(T(2,3,2)\big)=T\big(f(2),3,f(2)\big)=f(3)=3.$$

Let $f(2)=w$. Then the last equation yields $w^3-9w+10=0$. On the other hand,

$$T(2,1,0)=1\Rightarrow f\big(T(2,1,0)\big)=T\big(f(2),1,0\big)=f(1)=1.$$

This gives another cubic equation $w^3-3w-2=0$ for w. Since w must satisfy both equations, the only possibility is $w=2$. Additionally, $f(-2)=-2$.

Now we need only $f(4)$. Note that

$$T(4,2,0)=2^3T(2,1,0)=8$$

and, hence,

$$8=f^3(2)=f(8)=f\big(T(4,2,0)\big)=T\big(f(4),2,0\big),$$

and so $\kappa=f(4)$ satisfies $\kappa^3-12\kappa-16=0$. Hence, $f(4)=4$ or $f(4)=-2$. We will later show that, in fact, the last does not occur.

Thus, we finish the proof using induction. Suppose that we have proved that $f(n)=n$ for all $|n|\leqslant M$. The statement is true for $M=3$. Then the first equality of (22) with $n=M-1$ gives

$$\begin{aligned}T\big(f(M+1),M,1\big)&=T\big(f(M+1),f(M),f(1)\big)=f\big(T(M+1,M,1)\big)=f\big(T(M-2,M,1)\big)\\&=T\big(f(M-2),f(M),f(1)\big)=T(M-2,M,1)=-3M^3+9M^2-3.\end{aligned}$$

Let $f(M+1)=\Delta$. Then this gives the cubic equation for Δ

$$\Delta^3+\Delta(-3M^2+3M-3)+(2M^3-3M^2-3M+2)=0.$$

This factors as

$$\big(\Delta-(M+1)\big)\big(\Delta-(M-2)\big)\big(\Delta+(2M-1)\big)=0.$$

In particular, $f(4)=4$, 1, or -5 but we have already obtained that $f(4)=4$ or -2, hence, $f(4)=4$. We have proved the inductive step for $M=3$, and let $M\geqslant 4$.

Now, in the same way we will obtain the cubic equation for Δ from the second equality of (22) with $n=-M+1$. Then

$$T(M,M-2,-1)=-T(-M,-M+2,1)=-T(-M,-M-1,-2)=T(M,M+1,2).$$

Similarly, this gives

$$T(M,\Delta,2)=T\big(f(M),f(M+1),f(2)\big)=f\big(T(M,M+1,2)\big)=f\big(T(M,M-2,-1)\big)$$
$$=T(M,M-2,-1)=-3M^3+9M^2-9,$$

and, hence, this implies

$$\Delta^3+\Delta^2(3M-12)+\Delta(-6M+12)+(-4M^3+9M^2+12M-1)=0.$$

This expression factors as

$$\big(\Delta-(M+1)\big)\big(\Delta^2+\Delta(4M-11)+(4M^2-13M+1)\big)=0.$$

The discriminant of the second factor is equal to $-36M+117<0$ (for $M\geqslant 4$), and so it is irreducible.

Finally, Δ must satisfy both equations we have obtained, and, therefore, $\Delta=M+1$, i.e.,

$$f(M+1)=M+1 \quad\text{and}\quad f(-M-1)=-M-1.$$

The inductive step is proved.

Summarizing, for the field $\mathbb{Q}(\alpha)$ and a fixed integral basis $\{1,\alpha,\alpha'\}$, the only functions $f\colon \mathbb{Z}\to\mathbb{C}$ satisfying (21) are the following:

$$f(n)\equiv 0,\qquad f(n)\equiv i,\qquad f(n)\equiv -i,\qquad f(n)=n,\quad\text{and}\quad f(n)=-n,$$

which completes the proof of Proposition 3.

6. CONCLUSION

Before formulating the conjecture, we need one auxiliary lemma. It is not crucial for us, but it allows us to formulate the conjecture more clearly. Such a lemma might have appeared in the literature, but we could not find a relevant reference.

LEMMA 4. *Let* $\mathbf{K}$ *be a finite extension of* $\mathbb{Q}$ *of degree* $n\geqslant 2$. *Let* $\omega_1,\omega_2,\dots,\omega_n$ *be a basis of* $\mathbf{K}$ *as a vector space over* $\mathbb{Q}$. *Let*

$$\mathcal{N}(a_1\omega_1+a_2\omega_2+\dots+a_n\omega_n)=T(a_1,a_2,\dots,a_n)$$

be a norm form in this basis, where

$$\mathcal{N}=\mathcal{N}_{\mathbf{K}/\mathbb{Q}}.$$

If

$$T(a_1,a_2,\dots,a_n)=T'(a_1^s,a_2^s,\dots,a_n^s)$$

for some rational form T' *and natural* s, *then* $s=1$ *or* $s=2$.

Proof. We have that

$$\left\{1,\frac{\omega_2}{\omega_1},\frac{\omega_3}{\omega_1},\dots,\frac{\omega_n}{\omega_1}\right\}$$

is also a vector space basis. In fact, for any $\gamma\in\mathbf{K}$, the product $\gamma\omega_1$ can be uniquely expressed as

$$\gamma\omega_1=\sum_{i=1}^{n}r_i\omega_i,\qquad r_i\in\mathbb{Q}.$$

Therefore, there is a unique expression $\gamma=\sum_{i=1}^{n}r_i\frac{\omega_i}{\omega_1}$. Let $\gamma_i=\frac{\omega_i}{\omega_1}$. Thus, $\gamma_1=1$. Suppose that the assumption of Lemma is satisfied with some $s\geqslant 3$. Then also $n\geqslant 3$. In this case,

$$\mathcal{N}(a_1\omega_1+a_2\omega_2+a_3\omega_3)=T''(a_1^s,a_2^s,a_3^s)$$

for all rational a_1,a_2,a_3. Let $a_1=r$, and we fix $a_2=a$ and $a_3=b$, not both equal to 0. Let $\lambda=a\gamma_2+b\gamma_3$. Then

$$\begin{aligned}\mathcal{N}(r+\lambda)&=\mathcal{N}(r+a\gamma_2+b\gamma_3)\\&=\mathcal{N}(r\omega_1+a\omega_2+b\omega_3)\mathcal{N}(\omega_1)^{-1}\\&=CT''(r^s,a^s,b^s)\\&=H_\lambda(r^s),\end{aligned}$$

where $H_\lambda=H$ is a rational polynomial of one variable. Now let

$$T_\lambda(X)=T(X)\in\mathbb{Q}[X]$$

be the minimal monic polynomial of λ,

$$\big[\mathbb{Q}(\lambda)\colon\ \mathbb{Q}\big]=d_\lambda=d,\qquad \big[\mathbf{K}\colon\ \mathbb{Q}(\lambda)\big]=c_\lambda=c.$$

Then $dc=n$. Thus, in this notation,

$$\mathcal{N}(\lambda)=\big((-1)^dT(0)\big)^c=(-1)^nT^c(0).$$

The number $r+\lambda$ is a root of an irreducible monic polynomial $T(X-r)$; therefore,

$$\mathcal{N}(r+\lambda)=(-1)^nT^c(-r).$$

But we know that the latter is equal to $H(r^s)$. Since both are polynomials, and r is arbitrary rational number, they are equal to

$$(-1)^nT^c(-X)=H(X^s).$$

Clearly, $T(X)$ has a nonzero constant term. Then it is easy to see that $T(X)$ also is of the form $G(X^s)$. In fact, if it is not, let $q\in\mathbb{Q}$ be the constant term of $T(-X)$, and pX^t, $p\in\mathbb{Q}$, $p\neq 0$, be the term of the smallest degree, for which s does not divide t. Then $T^c(-X)$ contains the term $cq^{c-1}pX^t$, a contradiction. Therefore, provided that $s\geqslant 3$, we have proved the following:

For all $a,b\in\mathbb{Q}$, not both 0, the number $\lambda=a\gamma_2+b\gamma_3$ is a root of irreducible monic polynomial of the form $G_\lambda(X^s)$, where $G_\lambda(X)\in\mathbb{Q}[X]$.

Let $\sigma_1,\sigma_2,\dots,\sigma_n$ be different embeddings of $\mathbf{K}$ into $\overline{\mathbb{Q}}$, some algebraic closure of $\mathbb{Q}$. We will use the exponential notation $\sigma\colon\ \alpha\to\alpha^\sigma$. Then the polynomial

$$\prod_{l=1}^{n}\big(X-(a\gamma_2^{\sigma_l}+b\gamma_3^{\sigma_l})\big)$$

is a power of $G(X^s)$, therefore, it also is of the form $G'(X^s)$. In particular, since $s\geqslant 3$, the coefficients at X^{n-1} and X^{n-2} are 0, and we have

$$\sum_{l=1}^{n}(a\gamma_2^{\sigma_l}+b\gamma_3^{\sigma_l})=a\mathrm{Tr}(\gamma_2)+b\mathrm{Tr}(\gamma_3)=0,$$

where $\mathrm{Tr} = \mathrm{Tr}_{\mathbf{K}/\mathbb{Q}}$; we also have

$$\sum_{l \neq k}^{n} (a\gamma_2^{\sigma_l} + b\gamma_3^{\sigma_l}) \cdot (a\gamma_2^{\sigma_k} + b\gamma_3^{\sigma_k}) = a^2 \sum_{l \neq k} \gamma_2^{\sigma_l}\gamma_2^{\sigma_k} + 2ab \sum_{l \neq k} \gamma_2^{\sigma_l}\gamma_3^{\sigma_k} + b^2 \sum_{l \neq k} \gamma_3^{\sigma_l}\gamma_3^{\sigma_k} = 0.$$

Since a and b are arbitrary rational numbers (not both equal to 0), the two summands in the first equality and the three summands in the second one are all equal to 0. Hence,

$$\mathrm{Tr}(\gamma_2) = 0, \qquad \mathrm{Tr}(\gamma_3) = 0.$$

Additionally,

$$\mathrm{Tr}(\gamma_2^2) = \big(\mathrm{Tr}(\gamma_2)\big)^2 - \sum_{l \neq k} \gamma_2^{\sigma_l}\gamma_2^{\sigma_k} = 0, \qquad \mathrm{Tr}(\gamma_3^2) = 0;$$

we also have

$$\mathrm{Tr}(\gamma_2\gamma_3) = \mathrm{Tr}(\gamma_2)\mathrm{Tr}(\gamma_3) - \sum_{l \neq k} \gamma_2^{\sigma_l}\gamma_3^{\sigma_k} = 0.$$

Obviously, indices 2 and 3 can be replaced by any pair $\{i, j\}$, $2 \leqslant i, j \leqslant n$, $i \neq j$. The last equality also is true for indices 1 and $i \geqslant 2$, since $\gamma_1 = 1$.

Eventually, taking this into account, we obtain that the matrix

$$\big(\mathrm{Tr}(\gamma_i\gamma_j)\big)_{i,j=1}^{n}$$

has only one nonzero entry, that is, $\mathrm{Tr}(\gamma_1^2) = \mathrm{Tr}(1) = n$. Therefore, its determinant is 0, and since $\gamma_1, \gamma_2, \ldots, \gamma_n$ is a basis of $\mathbf{K}$ as a vector space over $\mathbb{Q}$, the latter contradicts to the fact that $\langle\delta_1, \delta_2\rangle := \mathrm{Tr}(\delta_1\delta_2)$ is a nondegenerate bilinear form in $\mathbf{K}$ (see [4], p. 286). For completeness, we give a short proof. Any $\delta \in \mathbf{K}$ is a $\mathbb{Q}$-linear combination of γ_i. Thus,

$$\mathrm{Tr}(\gamma_2\delta) = 0 \Rightarrow \mathrm{Tr}(\gamma_2\mathbf{K}) = 0 \Rightarrow \mathrm{Tr}(\mathbf{K}) = 0,$$

which contradicts to $\mathrm{Tr}(1) = n$. Thus, $s \leqslant 2$, and the lemma is proved.

Now we are ready to proceed with the following conjecture. As mentioned, this statement is true for quadratic norm forms $X^2 + DY^2$. The statement also is correct for the cubic form in Section 5. Also Proposition 2 of Section 2 corresponds to the second half of this conjecture in the case of the form $X^2 + Y^2$, and this can be extended without difficulty to the forms $X^2 + DY^2$, replacing the identity

$$(2n + r)^2 + (n - 2r)^2 = (2n - r)^2 + (n + 2r)^2$$

by

$$(n + D)^2 + D(n - 1)^2 = (n - D)^2 + D(n + 1)^2,$$

which immediately gives the desired linear recurrence relation. Naturally, the “if” part of the conjecture is trivial.

Conjecture. Let $f\colon \mathbb{Z} \to \mathbb{C}$ be any function. Let $\mathbf{K}$ be any proper finite extension of $\mathbb{Q}$ of degree n. Fix any integral basis of the ring of integers $\mathcal{O}_{\mathbf{K}}$: $\omega_1, \omega_2, \ldots, \omega_n$, and denote the norm form

$$\mathcal{N}(a_1\omega_1 + \cdots + a_n\omega_n) = T(a_1, \ldots, a_n).$$

Define $\Delta = T(1, 1, \ldots, 1)$ (which is, therefore, nonzero). Then relation (4) is satisfied if and only if $f(m) \equiv 0$, $f(m) \equiv \Delta^{-\frac{1}{n-1}}$ (any but fixed value of this radical, therefore, totally $n - 1$ values), or $f(m) = \zeta m$ for some fixed ζ, $\zeta^{n-1} = 1$, $m \in \mathbb{Z}$.

Moreover, the statement remains true if (4) is satisfied only for all $a_i \in \mathbb{Z}$, $|a_i| \geqslant N$ for all i, $1 \leqslant i \leqslant n$, and some fixed positive integer N.

Remark. In the case

$$T(a_1, a_2, \dots, a_n) = T'\big(a_1^2, a_2^2, \dots, a_n^2\big)$$

for some form T', we consider only "essentially different" solutions, which is defined in as follows. Two functions f are said to be "essentially equal," if they differ (probably) by the signs on the terms, which are not expressible as values of T with integer a_i. We needed Lemma 4 for such a purpose. In a case there exists a norm form $T'(a_1^s, a_2^s, \dots, a_n^s)$ for some $s \geqslant 3$, we would need to modify the notion of "essential equality" for every s. Fortunately, this cannot happen.

It is easy to explain why, empirically, this should be true. Examples with quadratic and cubic fields show that we can always expect to calculate some first values of $f(n)$ by *ad hoc* method. Moreover, for the extension of degree n (at least, in the Galois case), we could simply write the expression of type (22) with $n-1$ equalities. Generally, in the inductive step we have $(n-1)$ equations that are satisfied by the same complex number, and these are polynomials of degree n. And so it is hardly expectable that these weakly related polynomials have two common roots.

What concerns Question 1, we conclude with few remarks concerning our choice of norm forms. First, the norm form $T(a_1, a_2, \dots, a_s)$ is irreducible as a polynomial in $\mathbb{Z}[a_1, a_2, \dots, a_s]$, and, for reducible forms, the equivalent statement is false in general.

Example 1. Consider the reducible form $W(X,Y) = X^2 - Y^2$. Then the equation

$$f(X^2 - Y^2) = f^2(X) - f^2(Y)$$

is also satisfied by the primitive character modulo 4, that is,

$$f(X) = \begin{cases} 0 & \text{if } X \equiv 0 \pmod 2, \\ 1 & \text{if } X \equiv 1 \pmod 4, \\ -1 & \text{if } X \equiv 3 \pmod 4. \end{cases}$$

Second, if we consider irreducible polynomials that are not forms, this statement, in general, is also false.

Example 2. Let

$$W(a,b) = ab + a + b = (1+a)(1+b) - 1$$

(the simplest case of the formal group law). Then, for any nonnegative integer q and a function

$$f\colon\ \mathbb{Z} \to \mathbb{Z}, \qquad f(X) = (1+X)^q - 1,$$

we have

$$f\big(W(X,Y)\big) = f\big((1+X)(1+Y) - 1\big) = (1+X)^q(1+Y)^q - 1 = W\big(f(X), f(Y)\big).$$

More generally, let Γ: $\mathbb{Z} \to \mathbb{C}$ be any strongly multiplicative function. That is, given any complex number $\Gamma(p)$ for each prime

$$p \in \mathbb{N}, \qquad \Gamma(1) = 1, \qquad \Gamma(-1) = \pm 1, \qquad \Gamma(0) = 0,$$

we define

$$\Gamma(X) = \Gamma(\mathrm{sgn} X) \prod_{i=1}^{r} \Gamma^{s_i}(p_i) \quad \text{if } X = \pm \prod_{i=1}^{r} p^{s_i}$$

is a canonical expression of X. Then all complex-valued functions $f(X)$, $X \in \mathbb{Z}$, satisfying

$$f\bigl(W(X,Y)\bigr) = W\bigl(f(X), f(Y)\bigr) \quad \text{for all} \quad X, Y \in \mathbb{Z},$$

are given by $f(X) = \Gamma(X+1) - 1$.

Third, the key point in proving Conjecture in special cases is the presence of the relation of type (22), that is, integers in a number field form a linear algebraic group. This fails for certain forms that are not norm forms.

Example 3. Consider

$$W(X,Y) = X^3 + 2Y^3.$$

If there existed linear polynomials $g_1(X,Y)$, $g_2(X,Y)$, $g_3(X,Y)$, and $g_4(X,Y) \in \mathbb{Z}[X,Y]$ such that

$$g_1^3 + 2g_2^3 \equiv g_3^3 + 2g_4^3, \qquad g_1 \neq g_3, \qquad g_2 \neq g_4,$$

then the same would hold for some one variable linear functions, which can be verified to be false.

Fourth, the degree of the norm form is equal to the number of variables. Is it the "breaking point"? In other words, it is very likely that, for an irreducible form $L(a_1, a_2, \dots, a_s)$, which has the degree $n \geqslant 2$ less than the number of variables $(n < s)$, the equivalent statement remains correct. Then, on the other hand, it is natural to ask the following:

QUESTION 1. *Does there exist an irreducible integer form $M(a_1, a_2, \dots, a_s)$ of degree n greater than the number of variables $(n > s)$ such that*

$$f\bigl(M(a_1, a_2, \dots, a_s)\bigr) = M\bigl(f(a_1), f(a_2), \dots, f(a_s)\bigr)$$

for some function $f\colon \mathbb{Z} \to \mathbb{C}$ which is not a constant and not of the form $f(m) = \zeta m$?

Problem 2 seems to be more interesting. Here it is reasonable to ask the following:

QUESTION 2. *Is it true that relation* (6) *necessarily implies $f^2(n) = An^2 + g(n)$ with g being a periodic function?*

In the general case of Problem 2 and relation (5), we still do not have enough evidence that this necessarily yields $f^n(a) = Aa^n + g(a)$ with g being a periodic function.

Acknowledgments. I am obliged to Juozas Mačys for pointing out the problem. I would like also to thank Umberto Zannier for kind permission to use his unpublished manuscript, which also inspired for the investigations of Section 3.

REFERENCES

1. D. W. Boyd, Kronecker's theorem and Lehmer's problem for polynomials in several variables, *J. Number Theory*, **13**(1), 116–121 (1981).
2. S. Jakubec, Prime periods of periodical P-additive functions, *Ann. Math. Sil.*, **12**, 157–160 (1998).
3. I. Korec, Additive conditions on sums of squares, *Ann. Math. Sil.*, **12**, 35–51 (1998).
4. S. Lang, *Algebra*, 3rd ed., Addison-Wesley (1993).
5. J. Mačys, About one functional equation, *Alpha Plus Omega* [in Lithuanian], **2**, 85–96 (2004).
6. J. Milne, *Algebraic Number Theory*, Math676 (1998). www.jmilne.org.