ON AN IDENTITY OF RAMANUJAN OVER FINITELY GENERATED DOMAINS

GABRIELLA HAJDU AND LAJOS HAJDU

Abstract. In this paper we show that a well-known identity of Ramanujan admits only a bounded number of solutions over general finitely generated domains. The bound is explicit and uniform in the sense that it depends only on the dimensions of the domains involved. Our method is constructive, and opens up a possibility to determine the solutions in concrete instances. In some special cases all solutions are determined. Our results can also be considered as a continuation of some theorems of Z. Daróczy and G. Hajdu, obtained over $\mathbb{Z}$. We note that in case of Hosszú's equation, similar results were obtained by several authors.

1. Introduction

In the third volume of his famous Notebooks [1], Ramanujan states the following identity: if $ad = bc$, then

$$(a+b+c)^n + (b+c+d)^n + (a-d)^n = (a+b+d)^n + (a+c+d)^n + (b-c)^n$$

holds for $n = 2, 4$. Concerning this assertion, Z. Daróczy posed the following question: what functions satisfy the above identity? More precisely, one should determine all solutions f of the functional equation

$$f(a+b+c)+f(b+c+d)+f(a-d) = f(a+b+d)+f(a+c+d)+f(b-c) \quad (1)$$

which holds for any a, b, c, d with $ad = bc$. This problem has been solved by Z. Daróczy and G. Hajdu when for the unknown function we have $f: \mathbb{Z} \to \mathbb{R}$ or $f: F \to V$ where F is any field of characteristic zero and V is a linear space over some field of characteristic zero (see [3] and [2], respectively).

In the original identity of Ramanujan the domain where the parameters a, b, c, d come from is not specified. However, it is obvious that the commutativity of the multiplication is tacitly assumed. As we will work in general domains, we consider this identity under an assumption which is "more precise" than $ad = bc$. For the moment let R be a (not necessarily commutative) ring of characteristic zero, and let S be an appropriately chosen algebraic

2000 *Mathematics Subject Classification.* 39B52.

Key words and phrases. Ramanujan's identity, functional equations, finitely generated domains.

Research supported in part by the János Bolyai Research Fellowship of the Hungarian Academy of Sciences and by the OTKA grants T043080, T042985 and F034981.

structure, to be specified later. Let $f: R \to S$ be an arbitrary function, and suppose that the functional equation (1) holds for any $a, b, c, d \in R$ with

$$ad+da = bc+cb \text{ and } (uv+vu)^2-2(u^2v^2+v^2u^2) = (pq+qp)^2-2(p^2q^2+q^2p^2), \tag{2}$$

where $u = a+b+c$, $v = a-d$, $p = a+b+d$ and $q = b-c$. We mention that it is necessary to impose (2) in order to guarantee that the original solutions $f(x) = x^2, x^4$ of Ramanujan are also solutions in the non-commutative case (with $S = R$, say). Further, note that when the multiplication in R is commutative, then the second assertion is automatic, hence (2) reduces to $ad = bc$.

In this paper we give uniform finiteness results for the number of independent solutions of (1) with (2), when R and S are suitable finitely generated domains. The bound is explicit and uniform, that is it depends only on the dimensions of the domains involved. Our method is constructive in a sense, and provides an efficient tool to determine all solutions in concrete cases. Though there are some additional difficulties we have to deal with, following our approach we completely describe the set of solutions of (1) with (2) when R is the ring of integers of the number fields $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{2})$. There seems to be two natural methods for finding all solutions in concrete instances. To illustrate both of them, we give different arguments in case of the above structures.

Finally, we mention that similar investigations were performed by several authors concerning Hosszú's famous functional equation

$$f(x+y-xy) + f(xy) = f(x) + f(y),$$

see e.g. the papers of Davison [4] and Davison and Redlin [5], and the references given there.

2. Notation and results

To formulate our results, we need to introduce some notation which will be used throughout the paper without any further mentioning. From this point on, R will always denote a finitely generated $\mathbb{Z}$-algebra. That is, R is supposed to be a ring of characteristic zero, which is also a finitely generated $\mathbb{Z}$-module, of rank say n. Our assumptions imply that R has a basis $\vartheta_1, \dots, \vartheta_n$ over $\mathbb{Z}$, such that each $\alpha \in R$ can be expressed as

$$\alpha = a_1\vartheta_1 + \dots + a_n\vartheta_n,$$

where $a_1, \dots, a_n$ are uniquely determined integers. Note that R can be taken e.g. as the ring of integers of any algebraic number field, or as the ring of quadratic matrices of any size, having integer entries.

The range S of the function f in (1) does not play a vital role, the almost only important feature from our viewpoint is that it also should be finitely generated. So we can take S to be any finite dimensional linear space, over an arbitrary field F. For simplicity, we fix m to be the dimension of S over F.

The set of all solutions $f:\ R \to S$ to (1) with (2) will be denoted by $\mathcal{S}(R,S)$.

Now we can formulate our results. We start with a general statement.

Theorem 1. *Let R and S be as above. Then the functional equation* (1) *with* (2) *has at most $mC(n)$ independent solutions, where*

$$C(n) = 2^{n-1}\binom{10n+5}{n} + \sum_{i=0}^{n-1} 2^{i-1}\binom{10n+5}{i}\left(\binom{n-1}{i}+\binom{n}{i}\right).$$

More precisely, there exist solutions $f_1,\dots,f_k$ to (1) *with* (2) *where $k \le mC(n)$ such that for any $f \in \mathcal{S}(R,S)$ there are some $\lambda_1,\dots,\lambda_k \in F$ with*

$$f = \lambda_1 f_1 + \cdots + \lambda_k f_k.$$

The following theorems provide complete solutions to the functional equation (1) with (2), in case of two concrete algebras R. As in fact these domains are the rings of integers of certain algebraic number fields, for the sake of simplicity and convenience, we will set $S = \mathbb{C}$ in these statements. Write

$$\mathbb{G} = \mathbb{Z}[i] = \{a + bi\ :\ a, b \in \mathbb{Z}\}$$

for the set of the Gaussian integers and

$$\mathbb{A} = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2}\ :\ a, b \in \mathbb{Z}\}.$$

In what follows, for any $x \in \mathbb{G}$ (resp. $\mathbb{A}$) let $\overline{x}$ denote the algebraic conjugate of x, that is, for $x = a + bi \in \mathbb{G}$, $\overline{x} := a - bi$ and for $x = a + b\sqrt{2} \in \mathbb{A}$, $\overline{x} := a - b\sqrt{2}$. Finally, if $x, \gamma \in \mathbb{G}$ (resp. $\mathbb{A}$) and H is a full set of representatives of the remainder classes of γ in $\mathbb{G}$ (resp. in $\mathbb{A}$), then by $x \pmod{\gamma}\ H$ we mean the unique element h of H for which $x \equiv h \pmod{\gamma}$.

Theorem 2. *Let $R = \mathbb{G}$, and put $S = \mathbb{C}$. Then all solutions to the functional equation* (1) *with* (2) *are of the form $z_1 f_1 + \cdots + z_{11} f_{11}$ with $z_j \in \mathbb{C}$. Here the functions $f_j:\ \mathbb{G} \to \mathbb{C}$ $(j = 1,\dots,11)$ are given by*

$$f_1(x) = 1,\quad f_2(x) = x^2,\quad f_3(x) = x^4,\quad f_4(x) = \overline{x^2},\quad f_5(x) = \overline{x^4},$$

$$f_6(x) = \begin{cases} 1 & \text{if } x \equiv 0 \mod 2 \\ 0 & \text{otherwise,} \end{cases}$$

$$f_7(x) = x \pmod{1+i}\ \{0,1\},$$

$$f_8(x) = x^2 \pmod{2+i}\ H, \qquad f_9(x) = x^4 \pmod{2+i}\ H,$$

$$f_{10}(x) = x^2 \pmod{2-i}\ H, \qquad f_{11}(x) = x^4 \pmod{2-i}\ H,$$

where $H = \{0, 1, -1, i, -i\}$.

Theorem 3. *Let $R = \mathbb{A}$ and put $S = \mathbb{C}$. Then all solutions to the functional equation* (1) *with* (2) *are of the form $z_1 f_1 + \cdots + z_{11} f_{11}$ with $z_j \in \mathbb{C}$, where the functions f_j $(j = 1,\dots,11)$ are given by*

$$f_1(x) = 1,\quad f_2(x) = x^2,\quad f_3(x) = x^4,\quad f_4(x) = \overline{x^2},\quad f_5(x) = \overline{x^4},$$

$$f_6(x) = \begin{cases} 1 & \textit{if } \ x \equiv 0 \mod 2 \\ 0 & \textit{otherwise,} \end{cases}$$

$$f_7(x) = x \pmod{\sqrt{2}} \ \{0, 1\},$$

$$f_8(x) = x^2 \pmod{1 + 2\sqrt{2}} \ H_1, \qquad f_9(x) = x^4 \pmod{1 + 2\sqrt{2}} \ H_1,$$

$$f_{10}(x) = x^2 \pmod{1 - 2\sqrt{2}} \ H_2, \qquad f_{11}(x) = x^4 \pmod{1 - 2\sqrt{2}} \ H_2,$$

where

$$H_1 = \{0, 1, 2, -3, \sqrt{2}, 2\sqrt{2}, 2 + \sqrt{2}\}$$

and

$$H_2 = \{0, 1, 2, -3, 1 + \sqrt{2}, -\sqrt{2}, 2 + \sqrt{2}\}.$$

Interestingly, we obtained that both with $R = \mathbb{G}$ and $R = \mathbb{A}$, with $S = \mathbb{C}$, $\mathcal{S}(R, S)$ is generated by 11 independent functions. Moreover, the same number of independent solutions were obtained by Z. Daróczy and G. Hajdu in [3] over $\mathbb{Z}$. However, as the multiplicative structures of $\mathbb{Z}$, $\mathbb{G}$ and $\mathbb{A}$ are rather different, this phenomenon seems to be a strange coincidence only. This is also suggested by the following statement.

Proposition. *The dependence of the bound on n and m in Theorem 1 is necessary.*

3. Proofs

Before giving the proofs of the theorems of the previous section we note the following simple but useful fact. If f is a solution to (1) with (2) then f is even, i.e., $f(-x) = f(x)$ holds for all $x \in R$. This can easily be checked by interchanging the role of b and c in (1).

Proof of Theorem 1. First we show that there exists a "small" subset I of R such that the values taken by any solution $f \in \mathcal{S}(R, S)$ on I determine f completely. By this we mean that for any $x \in R$ there exist elements λ_u of F $(u \in I)$ which are independent of f such that

$$f(x) = \sum_{u \in I} \lambda_u f(u).$$

For this purpose, fix an arbitrary basis $\vartheta_1, \dots, \vartheta_n$ of R over $\mathbb{Z}$. If $\alpha \in R$ and

$$\alpha = a_1\vartheta_1 + \cdots + a_n\vartheta_n$$

with $a_1, \dots, a_n \in \mathbb{Z}$, then write

$$N(\alpha) = |a_1| + \cdots + |a_n|.$$

We call $a_1, \dots, a_n$ the coordinates and $N(\alpha)$ the norm of α. Let

$$T = \{b_1\vartheta_1 + \cdots + b_n\vartheta_n \ : \ b_i \in \mathbb{Z}, \ |b_i| \le 2\}$$

and write

$$I = \{x \in R \ : \ N(x) \le 10n + 5\}.$$

We show that f is determined by the values of f on I. We proceed by induction. Let x be an arbitrary element of R. If $N(x) \le 10n+5$, then our claim trivially holds. So we may assume that $N(x) > 10n+5$ and that for every $x' \in R$ with $N(x') < N(x)$ the assertion is valid. If one of the coordinates of x, say a_i is non-zero and divisible by 3, then put $t_1 = 3\vartheta_i$ or $t_1 = -3\vartheta_i$, according as a_i is positive or negative. Otherwise, let $t_1 = 0$. Moreover, choose a $t_2 \in T$ such that all coordinates of $x + t_2$ are divisible by 3, and that the sign of each non-zero coordinate of t_2 coincides with the sign of the corresponding coordinate of x. By the definition of T one can easily check that such a t_2 exists. Put $t = t_1 + t_2$. Define y to be the element in R obtained by dividing each coordinate of $x + t$ by 3. Observe that $N(t) \le 2n + 1$ and also that each coordinate of y has the same sign as the corresponding coordinate of x. Put

$$a = 2(y - t),\ b = y - t,\ c = 2t,\ d = t.$$

A simple calculation shows that for this choice of the parameters (2) is valid. Further, by the choice of t and our assumption $N(x) > 10n + 5$, using the information about the signs of the coordinates of x, t and y, a straightforward calculation shows that

$$N(a+b+c) > \max(N(a+b+d), N(a+c+d), N(b+c+d), N(a-d), N(b-c)).$$

Since $x = a + b + c$, this inductively proves that the value of f at x is determined by the values of f on I. As x was taken arbitrarily, our claim follows.

Clearly, we have

$$|I| = \#\{(b_1, \dots, b_n)\ :\ |b_1| + \cdots + |b_n| \le 10n + 5\}.$$

Thus by Lemma 2.3 of [6] we obtain $|I| = \sum\limits_{i=0}^{n} 2^i \binom{n}{i}\binom{10n+5}{i}$. Since for any $x \in R$ and $f \in \mathcal{S}(R, S)$ we have $f(x) = f(-x)$, we get that f is completely determined already by the values taken on the set

$$I' = \{x \in I\ :\ \text{the first coordinate of } x \text{ is non-negative}\}.$$

Using again Lemma 2.3 of [6], a simple calculation yields that $|I'| = C(n)$, where $C(n)$ is defined in the statement.

Observe that if for any $x \in R$ we have

$$f(x) = \sum_{u \in I'} \lambda_u^{(1)} f(u) = \sum_{u \in I'} \lambda_u^{(2)} f(u)$$

with some $\lambda_u^{(1)}, \lambda_u^{(2)} \in F$ $(u \in I')$ such that $\lambda_u^{(1)} \ne \lambda_u^{(2)}$ for some $u \in I'$, then it is possible to exclude an element of I' such that the remaining set still determines f on R. Hence we may reduce I' to a set $I_0 = \{u_1, \dots, u_l\}$ with $l \le C(n)$ such that the above expansion of $f(x)$ is unique for any $x \in R$. Fix an arbitrary basis $\beta_1, \dots, \beta_m$ of S over F. Define the functions f_{ij} $(1 \le i \le l,\ 1 \le j \le m)$ on I_0 by $f_{ij}(u_i) = \beta_j$ and $f_{ij}(u_r) = 0$ for $r \ne i$, and then extend this definition to the whole R in the unique way, to obtain solutions to (1) with (2). Then clearly every $f \in \mathcal{S}(R,S)$ is a linear combination of the functions f_{ij} over F. As the number of the f_{ij} is at most $mC(n)$, the theorem follows. $\square$

Proof of Theorem 2. The proof consists of two major parts. First we show that there exists a set I_0 such that any solution $f: \mathbb{G} \to \mathbb{C}$ to (1) with (2) is uniquely determined by the values it takes on I_0. For this purpose we use the same argument as in the proof of Theorem 1, with slight changes only. This way we can get a smaller bound for the diameter of the initial set I of "base points". In the second part we prove that the functions $f_1, \dots, f_{11}$ given in the theorem form a base of $\mathcal{S}(\mathbb{G},\mathbb{C})$ over $\mathbb{C}$.

For any $x = x_1 + x_2 i \in \mathbb{G}$ let

$$N(x) = |x| = \sqrt{x_1^2 + x_2^2},$$

the Euclidean norm (length) of x. The role of number 3 in the proof of Theorem 1 will be played by $1+i$. We put

$$T = \{z \in \mathbb{G} \ : \ |z| \le \sqrt{2}\} \quad \text{and} \quad I = \{x \in \mathbb{G} \ : \ |x| \le 7.64\}.$$

Assume $f: \mathbb{G} \to \mathbb{C}$ to be a solution to (1) with (2). We shall show that for any $x \in \mathbb{G}$, the value $f(x)$ can be obtained from the values $\{f(x') \ : \ x' \in I\}$. This trivially holds for any $x \in I$. Now let $x \in \mathbb{G}$, $|x| > 7.64$ and suppose that for any $x' \in \mathbb{G}$ with $|x'| < |x|$, $f(x')$ is determined by the values f takes on the set I. Choose an element $t \in T$ such that $x + t$ is divisible by $1 + i$ and the length of $x + (1-i)t$ is strictly less than the length of x. The definition of T guarantees the existence of such a t. Let $y = \dfrac{x+t}{1+i}$ and put

$$a = i(y-t), \ b = y - t, \ c = it, \ d = t.$$

Then $ad = bc$, that is, (2) is valid. Moreover, we have

$$a + b + c = x, \quad (1+i)(b+c+d) = x + it,$$
$$(1-i)(a-d) = x - t, \quad a + b + d = x + (1-i)t,$$
$$(1-i)(a+c+d) = x + (2-i)t, \quad (1+i)(b-c) = x + (1-2i)t.$$

Hence by $|x| > 7.64 > \frac{\sqrt{5}|t|}{\sqrt{2}-1}$, a simple calculation shows that

$$|a+b+c| > \max(|a+b+d|, |a-d|, |a+c+d|, |b+c+d|, |b-c|).$$

Our aim now is to reduce I and construct the smallest set I_0 with the same property, namely that any solution to (1) with (2) is determined by its values on I_0. To achieve this we eliminate as many elements from I as possible. Since for any $x \in \mathbb{G}$ we have $f(-x) = f(x)$, the elements of I having negative real parts can be omitted. Next, if taking an element x of I we can find suitable $a, b, c, d \in \mathbb{G}$ with the properties that

a) $ad = bc$ (i.e., (2) holds),
b) x equals one of the arguments of f in (1),
c) x is strictly longer than the other five arguments,

then we can cancel x from I, because $f(x)$ is determined by $\{f(x') : x' \in I,\ |x'| < |x|\}$. Moreover, in this case we can cancel $\overline{x}$ with $\overline{a}, \overline{b}, \overline{c}, \overline{d}$ and also $\pm i\overline{x}$ with $\pm i\overline{a}, \pm i\overline{b}, \pm i\overline{c}, \pm i\overline{d}$. In most cases we can choose d to be equal to either $-1-i$ or $-i$. For example, if $x = 5+i$ then we can take

$$a = -2+2i, \quad b = 2+2i, \quad c = 1, \quad d = -i.$$

Then in (1) we have

$$x = a+b+c = 5+i, \quad b+c+d = 3-3i, \quad a-d = 2+4i,$$

$$a+b+d = 3+i, \quad a+c+d = 1+i, \quad b-c = 2.$$

Similarly, for $x = 1+4i$ we may choose

$$a = -2+2i, \quad b = 2+2i, \quad c = 1, \quad d = -i$$

which yields

$$x = a+b+c = 1+4i, \quad b+c+d = 3+i, \quad a-d = -2+3i,$$

$$a+b+d = 3i, \quad a+c+d = -1+i, \quad b-c = 1+2i.$$

After the possible eliminations we obtain the set

$$\begin{aligned} I' = \{&0,\ 1,\ i,\ 2,\ 2i,\ 1+i,\ 1-i,\ 1-2i,\ 2-i,\ 3,\ 1-3i,\\ &3+i,\ 1+3i,\ 3-2i,\ 4i,\ 1-4i,\ 1+4i,\ 4+i,\ 2+3i,\\ &3+2i,\ 3i,\ 3-i,\ 2-2i,\ 2+2i,\ 1+2i,\ 2+i\}. \end{aligned}$$

We mention that I' could be further reduced by the above method, however, now it is worth changing the strategy. Namely, up to this point we used shorter arguments to eliminate the longest one, and now we abandon this restriction. In this way we can successively cancel the elements given in Table 1, in the column of x. In the table we give the appropriate choices of the parameters a, b, c, d as well, together with the other arguments occurring in (1) (recall that $f(-x) = f(x)$). Note that in each row of Table 1 we have $x = a+b+c$ except for $x = 4i$ when $x = a-d$.

After this elimination process we obtain the 11-element set

$$I_0 = \{0,\ 1,\ i,\ 2,\ 2i,\ 1+i,\ 1-i,\ 1-2i,\ 2-i,\ 3,\ 1-3i\}.$$

We show that I_0 is minimal, that is, every function solving (1) with (2) is uniquely determined by the values it takes on the set I_0. For this purpose we provide 11 linearly independent solutions which form a base of the linear space $\mathcal{S}(\mathbb{G}, \mathbb{C})$ over $\mathbb{C}$.

¿From Ramanujan's work we know the solutions

$$f_1(x) = 1, \quad f_2(x) = x^2, \quad f_3(x) = x^4.$$

Clearly, taking conjugates, we have two more solutions given by

$$f_4(x) = \overline{x^2}, \quad f_5(x) = \overline{x^4}.$$

Showing that the functions $f_6, \ldots, f_{11}$ are indeed solutions to (1) with (2) needs some calculation. We prove it only in one case, the other functions

x	a	b	c	d	the other arguments
$3+i$	$2i$	2	$1-i$	$-1-i$	$2-2i, 1+3i, 1+i, 0, 1+i$
$1+3i$	-1	$2+2i$	i	$2-2i$	$4+i, -3+2i, 3, 1-i, 2+i$
$3-2i$	$-1-2i$	$2+i$	$2-i$	$-1+2i$	$3+2i, 4i, i, -i, 2i$
$4i$	$5i$	$1-2i$	$-1-2i$	i	$i, -3i, 1+4i, -1+4i, 2$
$1-4i$	$2-i$	$-i$	$-1-2i$	-1	$-2-3i, 3-i, 1-2i, -3i, 1+i$
$1+4i$	$-1+2i$	$2+i$	i	1	$3+2i, -2+2i, 2+3i, 3i, 2$
$4+i$	$2-i$	$1+2i$	1	i	$2+3i, 2-2i, 3+2i, 3, 2i$
$2+3i$	$-1+i$	1	$2+2i$	$-2i$	$3, -1+3i, -i, 1+i, -1-2i$
$3+2i$	$1-i$	i	$2+2i$	-2	$3i, 3-i, -1, 1+i, -2-i$
$3i$	$1+i$	$-1+i$	i	-1	$-2+2i, 2+i, -1+2i, 2i, -1$
$3-i$	$-2i$	2	$1+i$	$-1+i$	$2+2i, 1-3i, 1-i, 0, 1-i$
$2-2i$	2	$1-i$	$-1-i$	-1	$-1-2i, 3, 2-i, -i, 2$
$2+2i$	2	$1+i$	$-1+i$	-1	$-1+2i, 3, 2+i, i, 2$
$1+2i$	$-1+i$	$1+i$	1	$-i$	$2, -1+2i, i, 0, i$
$2+i$	$1-i$	$1+i$	i	-1	$2i, 2-i, 1, 0, 1$

Table 1. The reduction of I'. We successively omit the elements in the column of x from I' to get I_0.

can be handled in a similar way. We show that f_9 solves (1) with (2), that is, $ad = bc$ implies

$$(a+b+c)^4+(b+c+d)^4+(a-d)^4 = (a+b+d)^4+(a+c+d)^4+(b-c)^4, \quad (3)$$

where raising to the fourth power is understood modulo $2+i$ (as in the statement of the theorem). Clearly, we may suppose that $a, b, c \in H = \{0, 1, -1, i, -i\}$. If $a = 0$ then we also have $bc = 0$, and (3) trivially holds. Hence we may assume that $a \neq 0$. Moreover, after multiplying (3) by the fourth power of the inverse of a modulo $2+i$, we may also suppose that $a = 1$. Hence by $ad = bc$, (3) reduces to

$$(1+b+c)^4+(b+c+bc)^4+(1-bc)^4 = (1+b+bc)^4+(1+c+bc)^4+(b-c)^4. \quad (4)$$

Observe that if one of b or c belongs to $\{-1, 0, 1\}$ then by $(-1)^4 = 1$, (4) is a formal identity. Using symmetry, it remains only to show that (4) holds in the following cases.

a) If $b = c = i$, then by

$$(1+2i)^4 \equiv 2^4 \equiv i^4 \equiv 1 \quad \text{and} \quad (-1+2i)^4 \equiv 0^4 \equiv 0 \pmod{2+i}$$

we get that

$$(1+2i)^4 + (-1+2i)^4 + 2^4 = i^4 + i^4 + 0^4,$$

that is, (4) holds.

b) If $b = i$ and $c = -i$, then using

$$1^4 \equiv (2-i)^4 \equiv (2i)^4 \equiv 1 \quad \text{and} \quad 0^4 \equiv (2+i)^4 \equiv 0 \pmod{2+i}$$

we obtain

$$1^4 + 1^4 + 0^4 = (2+i)^4 + (2-i)^4 + (2i)^4,$$

so (4) is valid again.

c) Finally, if $b = c = -i$, then

$$(-1-2i)^4 \equiv 2^4 \equiv (-i)^4 \equiv 1 \quad \text{and} \quad (1-2i)^4 \equiv 0^4 \equiv 0 \pmod{2+i}$$

give

$$(1-2i)^4 + (-1-2i)^4 + 2^4 = (-i)^4 + (-i)^4 + 0^4,$$

which shows that (4) is true also in this case.

This proves that f_9 is a solution to (1) with (2) indeed. In case of the other functions given in the statement, similar arguments are available to get the same conclusion.

To show that the functions $f_1, \dots f_{11}$ are linearly independent, we compose a matrix A from the values they take on the set I_0. So let A be the following matrix:

$$\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & -1 & 4 & -4 & 2i & -2i & -3-4i & 3-4i & 9 & -8-6i \\
0 & 1 & 1 & 16 & 16 & -4 & -4 & -7+24i & -7-24i & 81 & 28+96i \\
0 & 1 & -1 & 4 & -4 & -2i & 2i & -3+4i & 3+4i & 9 & -8+6i \\
0 & 1 & 1 & 16 & 16 & -4 & -4 & -7-24i & -7+24i & 81 & 28-96i \\
1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\
0 & 1 & -1 & -1 & 1 & 1 & -1 & 0 & 1 & -1 & -1 \\
0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\
0 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 0 & -1 & 0 \\
0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0
\end{pmatrix}$$

defined by $A_{jk} = f_j(x_k)$, where x_k $(k = 1, \dots, 11)$ are the elements of I_0 (in the given order). A simple calculation with Maple yields that the rank of A is 11, which shows that the solutions f_j $(j = 1, \dots, 11)$ are linearly independent over $\mathbb{C}$. This completes the proof of the theorem. □

Remark 1. In the proof of Theorem 2, after giving an initial bound for the size of I, we used reduction to construct I_0. That is, we eliminated as many elements from I as possible. However, there is another, "expansive" approach, when we gradually build up the set I_0 and then we check that every element in I can be obtained from this set. This is a more heuristic way of finding our set I_0, nevertheless this provides a quicker method. In the proof of Theorem 3 we show how it works. Of course, the argument in the proof of Theorem 2 could be applied here as well.

Proof of Theorem 3. During the proof we use the notation and formulas from the proof of Theorem 1. For any $x = a + b\sqrt{2} \in \mathbb{A}$ let $N(x) = |a| + |b|$ and put

$$I = \{x \in \mathbb{A} \ : \ N(x) \leq 25\}.$$

Suppose that $f : \mathbb{A} \to \mathbb{C}$ is a solution to (1) with (2). Then, as in the proof of Theorem 1, for any $x \in \mathbb{A}$ the value $f(x)$ can be obtained from the values $\{f(x') \ : \ x' \in I\}$.

To find I_0 (a minimal set of base points) we apply the following heuristics. We start with $I_0 = \{0\}$ and we expand this set gradually, until we obtain a set I_0 such that the values of any solution f of (1) with (2) are determined by the values of f taken on I_0. Note that for this purpose it is sufficient to check that for each $x \in I$, $f(x)$ is a linear combination of the values $f(u)$ $(u \in I_0)$ with complex coefficients (which are independent of f). We put

$H = I_0$. At each stage of the expansion, we do the following. We take all values a, b, c, d with $ad = bc$ from an appropriate (small) set and in each case we generate the arguments of f in (1). If only one of these arguments does not belong to the actual H and (1) is not an identity, then we add this argument to H. Then we repeat the process (with the new H). After a few rounds we stop and check whether the set H we obtained contains I. If it does, then we accept I_0 as a minimal set of base points, and we are done. In the opposite case, that is if there is an element x of I which is not in H (i.e. which we could not reach from I_0), then we add x to I_0 and start over the whole procedure. As the result of this method we obtained the following set of points:

$$I_0 = \{0,\ 1,\ 2,\ 3,\ \sqrt{2},\ 1+\sqrt{2},\ 2+\sqrt{2},\ 3+\sqrt{2},\ 2\sqrt{2},\ 3+2\sqrt{2},\ 1-2\sqrt{2}\}.$$

Though we used a heuristic procedure to get this I_0, we can prove that this set is a minimal set of base points indeed. On one hand, a simple calculation shows that for any solution f to (1) with (2), the values of f taken on I are uniquely determined by the values of f on I_0. (This is why we stopped the above procedure at this stage.) On the other hand, it is easy to check (in the same way as in the proof of Theorem 2) that the functions f_i $(i = 1, \dots, 11)$ are solutions to (1) with (2), moreover, they are linearly independent over $\mathbb{C}$. Hence the theorem follows. $\square$

Proof of the Proposition. Let n be an odd prime, and let α be a root of the polynomial $P(x) = \frac{x^n-1}{x-1}$. Note that P is irreducible over $\mathbb{Q}$, and put $R = \mathbb{Z}[\alpha]$. Then as is well-known, $1, \alpha, \dots, \alpha^{n-2}$ is a basis of the order R over $\mathbb{Z}$. Moreover, as $\alpha^{n-1} + \dots + \alpha + 1 = 0$, we have that $\alpha, \dots, \alpha^{n-1}$ is also a basis of R. Further, as α is a primitive n-th root of unity, the roots of P are given by $\alpha, \alpha^2, \dots, \alpha^{n-1}$. Let $c_j : \mathbb{Q}(\alpha) \to \mathbb{C}$ denote the isomorphism induced by the correspondence $\alpha \to \alpha^j$ for $j = 1, \dots, n-1$. Consider (1) and (2) with $S = \mathbb{C}$ and define the function $f_j : R \to \mathbb{C}$ by $f_j(x) = c_j(x^2)$ $(j = 1, \dots, n-1)$. As the c_j are isomorphisms, these functions are in $\mathcal{S}(R, S)$. We show that they are linearly independent over $\mathbb{C}$. For this purpose, observe that as α is an n-th root of unity, we have

$$\{\alpha^2, \dots, \alpha^{2(n-1)}\} = \{\alpha, \dots, \alpha^{n-1}\}.$$

Thus

$$\begin{vmatrix} c_1(\alpha^2) & \dots & c_1(\alpha^{2(n-1)}) \\ \vdots & \ddots & \vdots \\ c_{n-1}(\alpha^2) & \dots & c_{n-1}(\alpha^{2(n-1)}) \end{vmatrix}$$

is the square-root of the discriminant of the order R (up to sign), and hence it does not vanish. This shows that the functions f_j are linearly independent over $\mathbb{C}$. Hence (1) with (2) has at least $n-1$ independent solutions in this case, which shows that the dependence on n in our bound is necessary.

Let now $R = \mathbb{Z}$, $S = \mathbb{R}^m$, and suppose that $\vartheta_1, \dots, \vartheta_m$ is a basis of S over $F = \mathbb{R}$. Then the functions $g_j : R \to S$ $(j = 1, \dots, m)$ defined by

$g_j(x) = \vartheta_j$ $(x \in R)$, are in $\mathcal{S}(R,S)$, and are obviously linearly independent over F. Hence our claim follows. □

References

[1] S. Ramanujan, *Notebooks*, Tata Institute of Fundamental Research, Bombay, 1957.

[2] Z. Daróczy and G. Hajdu, *On the Ramanujan differences*, Publ. Math. Debrecen **53** (1998), no. 3-4, 281–291.

[3] Z. Daróczy and G. Hajdu, *On an identity of Ramanujan*, Acta Math. Hungar. **82** (1999), no. 1-2, 1–9.

[4] T. M. K. Davison, *On the Functional Equation* $f(m+n-mn)+f(mn) = f(m)+f(n)$, Aequationes Math. **10** (1974), 206–211

[5] T. M. K. Davison and L. Redlin *Hosszú's functional equation over rings generated by their units*, Aequationes Math. **21** (1980), 121–128

[6] P. Kirschenhofer, A. Pethő and R. F. Tichy *On analytical and diophantine properties of a family of counting polynomials*, Acta Sci. Math. (Szeged) **65** (1999), 47–59

Institute of Mathematics and Computer Science
Faculty of Mechanical Engineering
Szent István University
H-2103 Gödöllő, Páter K. u. 1.
Hungary
E-mail address: godenyne.hajdu.gabriella@gek.szie.hu

Institute of Mathematics
University of Debrecen
and the Number Theory Research Group
of the Hungarian Academy of Sciences
H-4010 Debrecen, P.O.B. 12
Hungary
E-mail address: hajdul@math.klte.hu