A CHARACTERIZATION OF FUNCTIONS USING LAGRANGE'S FOUR-SQUARE THEOREM

Imre Kátai and Bui Minh Phong
(Budapest, Hungary)

Communicated by Jean-Marie De Koninck

(Received May 17, 2020; accepted July 20, 2021)

Abstract. We give all solutions of the arithmetical functions $f, g, F, G :$ $: \mathbb{N}_0 \to \mathbb{C}$ which satisfy the relations

$$f\left(a^2+b^2+c^2+d^2\right) = g\left(a^2\right)+g\left(b^2\right)+g\left(c^2\right)+g\left(d^2\right)$$

and

$$F\left(a^2+b^2+c^2+d^2\right) = G\left(a^2+b^2\right)+G\left(c^2+d^2\right)$$

for every $a, b, c, d \in \mathbb{N}_0$, where $\mathbb{N}_0$ is the set of all non-negative integers.

1. Introduction

Let, as usual, $\mathbb{N}$, $\mathbb{N}_0$, $\mathbb{C}$ be the set of positive integers, non negative integers and complex numbers, respectively. Moreover, let $\mathcal{P}$ stand for the set of all primes.

By using the result of H. A. Helfgott [1] concerning the ternary Goldbach conjecture, in [2] we proved that if the functions f and g satisfy the condition

$$f\left(p_1+p_2+p_3\right) = g(p_1)+g(p_2)+g(p_3)$$

for every $p_1, p_2, p_3 \in \mathcal{P}$, then there exist constants $A, B \in \mathbb{C}$ such that

$$f(n) = An + 3B \quad \text{and} \quad g(p) = Ap + B$$

Key words and phrases: Arithmetical function, function equation.
2010 Mathematics Subject Classification: 11K65, 11N37, 11N64.
https://doi.org/10.71352/ac.52.177

hold for $n \in \mathbb{M}, p \in \mathcal{P}$, where

$$\mathbb{M} := \{p_1 + p_2 + p_3 \mid p_1, p_2, p_3 \in \mathcal{P}\}.$$

We also proved in [3] that if the sets

$$\mathcal{A} = \{a_1 < a_2 < \cdots\} \subseteq \mathbb{N}, \quad \mathcal{S} := \{m^2 \mid m \in \mathbb{N}\}$$

and the arithmetical functions $f : \mathcal{A}+\mathcal{S} \to \mathbb{C}$, $g : \mathcal{A} \to \mathbb{C}$ and $h : \mathcal{S} \to \mathbb{C}$ satisfy the equation

$$f\big(a + n^2\big) = g(a) + h\big(n^2\big) \text{ for every } \quad a \in \mathcal{A},\ n \in \mathbb{N},$$

then the assumption $8\mathbb{N} \subseteq \mathcal{A} - \mathcal{A}$ implies that there is a complex number A such that

$$g(a) = Aa+\overline{g}(a),\ \ h(n^2) = An^2+\overline{h}(n) \quad \text{and} \quad f(a+n^2) = A(a+n^2)+\overline{g}(a)+\overline{h}(n)$$

hold for all $a \in \mathcal{A}, n \in \mathbb{N}$, and also that

$$\overline{g}(a) = \overline{g}(b) \quad \text{if} \quad a \equiv b \pmod{120}, \quad (a, b \in \mathcal{A})$$

and

$$\overline{h}(n) = \overline{h}(m) \quad \text{if} \quad n \equiv m \pmod{60}, \quad (n, m \in \mathbb{N}).$$

By assuming the unknown hypothesis that every positive number of the form $8n$ is the difference of two primes, we determined all functions F, G, for which

$$F\big(p + n^2\big) = G(p) + H\big(n^2\big) \text{ for every } \quad p \in \mathcal{P}, n \in \mathbb{N}.$$

It was proved in [4] that if the functions $f, g, h : \mathbb{N} \to \mathbb{C}$ satisfy the following equation

$$f\big(p + n^3 + m^3\big) = g(p) + h\big(n^3\big) + h\big(m^3\big) \text{ for every } \ p \in \mathcal{P}, n, m \in \mathbb{N},$$

then there exist $A, B, C \in \mathbb{C}$ such that

$$h\big(n^3\big) = An^3 + B \quad \text{and} \quad g(p) = Ap + C \text{ for every } \ p \in \mathcal{P}, n \in \mathbb{N}.$$

In this note we prove the following results.

Theorem 1. *Assume that the arithmetical functions $f, g : \mathbb{N}_0 \to \mathbb{C}$ satisfy the relation*

$$f\big(a^2 + b^2 + c^2 + d^2\big) = g\big(a^2\big) + g\big(b^2\big) + g\big(c^2\big) + g\big(d^2\big) \tag{1.1}$$

for every $a, b, c, d \in \mathbb{N}_0$. Then there are numbers A and B such that

$$f(n) = An + 4B \quad \text{and} \quad g\big(m^2\big) = Am^2 + B \tag{1.2}$$

hold for every $n, m \in \mathbb{N}_0$.

Theorem 2. *Assume that the arithmetical functions $F, G : \mathbb{N}_0 \to \mathbb{C}$ satisfy the relation*

$$F\big(a^2 + b^2 + c^2 + d^2\big) = G\big(a^2 + b^2\big) + G\big(c^2 + d^2\big) \tag{1.3}$$

for every $a, b, c, d \in \mathbb{N}_0$. Then there are numbers C and D such that

$$F(n) = Cn + 2D \quad \text{and} \quad G\big(n^2 + m^2\big) = C\big(n^2 + m^2\big) + D \tag{1.4}$$

hold for every $n, m \in \mathbb{N}_0$.

We derive the following corollaries from Theorem 1 and Theorem 2.

Corollary 1. *Assume that the arithmetical function $f : \mathbb{N}_0 \to \mathbb{C}$ satisfies the relation*

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

for every $a, b, c, d \in \mathbb{N}_0$. Then $f(n) = f(1)n$ holds for every $n \in \mathbb{N}_0$.

Corollary 2. *Assume that the arithmetical function $F : \mathbb{N}_0 \to \mathbb{C}$ satisfies the relation*

$$F\big(a^2 + b^2 + c^2 + d^2\big) = F\big(a^2 + b^2\big) + F\big(c^2 + d^2\big)$$

for every $a, b, c, d \in \mathbb{N}_0$. Then $F(n) = F(1)n$ holds for every $n \in \mathbb{N}_0$.

2. Proof of Theorem 1

Lagrange's Four-Square Theorem states that every positive integer can be written as the sum of at most four squares. This theorem, also known as Bachet's conjecture, which Bachet inferred from a lack of a necessary condition being stated by Diophantus. Although the theorem was proved by Fermat using infinite descent, the proof was suppressed. The first published proof was given by Lagrange in 1770 and made use of the Euler four-square identity.

Lagrange also proved that, where 4 may be reduced to 3 except for numbers of the form $4^n(8k + 7)$, as proved by Legendre in 1798. We state these results as follows:

Lemma 1. (Lagrange's Four-Square Theorem.) *Every positive integer can be written as the sum of at most four squares.*

Lemma 2. (Lagrange.) *Every positive integer can be expressed as the sum of three squares if and only if it is not of the form $4^n(8k + 7)$ for non negative integers n and k.*

First we prove the following lemma.

Lemma 3. *Assume that (1.1) holds for every $a,b,c,d \in \mathbb{N}_0$. Then there are numbers A,B such that (1.2) is satisfied for $n,m \in \{0,1,2,3,4,5\}$.*

Proof. Let $A := g(1) - g(0)$ and $B := g(0)$. Since

$$f(0) = f\big(0^2+0^2+0^2+0^2\big) = 4g(0) = 4B$$

and

$$f(1) = f\big(1^2+0^2+0^2+0^2\big) = g(1) + 3g(0) = A + 4B,$$

consequently (1.2) is true for $n,m \in \{0,1\}$.

We infer from (1.2) that if

$$x^2+y^2+z^2+t^2 = a^2+b^2+c^2+d^2, \tag{2.1}$$

then

$$g\big(x^2\big)+g\big(y^2\big)+g\big(z^2\big)+g\big(t^2\big) = g\big(a^2\big)+g\big(b^2\big)+g\big(c^2\big)+g\big(d^2\big). \tag{2.2}$$

Since

$$\begin{aligned}(x,y,z,t,a,b,c,d) \in \big\{&(2,0,0,0,1,1,1,1),(3,0,0,0,2,2,1,0),\\ &(4,0,0,0,2,2,2,2),(5,0,0,0,4,3,0,0)\big\}\end{aligned}$$

satisfies (2.1), therefore we infer from (2.2) that

$$\begin{cases} g(4) = 4g(1) - 3g(0) = 4A + B,\\ g(9) = 2g(4) + g(1) - 2g(0) = 2(4g(1) - 3g(0)) + g(1) - 2g(0) =\\ \qquad = 9g(1) - 8g(0) = 9A + B,\\ g(16) = 4g(4) - 3g(0) = 4(4g(1) - 3g(0)) - 3g(0) = 16g(1) - 15g(0) =\\ \qquad = 16A + B,\\ g(25) = g(16) + g(9) - g(0) = (16g(1) - 15g(0)) + (9g(1) - 8g(0)) - g(0) =\\ \qquad = 25g(1) - 24g(0) = 25A + B. \end{cases}$$

Thus we have proved that $g(m^2) = Am^2 + B$ holds for $m \in \{0,1,2,3,4,5\}$. By using these relations, we get from (1.1) that

$$\begin{cases} f(1) = f\big(1^2+0^2+0^2+0^2\big) = g(1) + 3g(0) = A + 4B,\\ f(2) = f\big(1^2+1^2+0^2+0^2\big) = 2g(1) + 2g(0) = 2A + 4B,\\ f(3) = f\big(1^2+1^2+1^2+0^2\big) = 3g(1) + g(0) = 3A + 4B,\\ f(4) = f\big(1^2+1^2+1^2+1^2\big) = 4g(1) = 4A + 4B,\\ f(5) = f\big(2^2+1^2+0^2+0^2\big) = g(4) + g(1) + 2g(0) = 5g(1) - (5-4)g(0) =\\ \qquad = 5A + 4B, \end{cases}$$

which proves that $f(n) = An + 4B$ holds for $n \in \{0, 1, 2, 3, 4, 5\}$.

Lemma 3 is thus proved. ■

Lemma 4. *Assume that (1.1) holds for every $a, b, c, d \in \mathbb{N}_0$, then there are numbers A, B such that*

$$g\bigl(m^2\bigr) = Am^2 + B \quad \text{for every} \quad m \in \mathbb{N}_0. \tag{2.3}$$

Proof. By using Lemma 3, we assume that (2.3) holds for every $m < M$, where $M \in \mathbb{N}, M \geq 6$. If $M^2 - (M-1)^2 = 2M - 1 \neq 4^n(8k+7)$ for every $n, k \in \mathbb{N}_0$, then Lemma 2 implies that there are $x, y, z \in \mathbb{N}_0$ such that

$$M^2 - (M-1)^2 = 2M - 1 = x^2 + y^2 + z^2.$$

It is clear that $x, y, z < M$, and so by our assumptions, we have $g(x^2) = Ax^2 + B$, $g(y^2) = Ay^2 + B$ and $g(z^2) = Az^2 + B$. On the other hand, we have

$$\begin{aligned} f\bigl(M^2\bigr) &= f\bigl((M-1)^2 + x^2 + y^2 + z^2\bigr) = \\ &= g\bigl((M-1)^2\bigr) + g\bigl(x^2\bigr) + g\bigl(y^2\bigr) + g\bigl(z^2\bigr) = \\ &= \bigl(A(M-1)^2 + B\bigr) + \bigl(Ax^2 + B\bigr) + \bigl(Ay^2 + B\bigr) + \bigl(Az^2 + B\bigr) = \\ &= A\bigl((M-1)^2 + x^2 + y^2 + z^2\bigr) + 4B = AM^2 + 4B. \end{aligned}$$

But

$$AM^2 + 4B = f(M^2) = f(M^2 + 0^2 + 0^2 + 0^2) = g(M^2) + 3g(0) = g(M^2) + 3B,$$

which implies that

$$g(M^2) = AM^2 + B.$$

Consequently Lemma 2 is proved for the case $M^2 - (M-1)^2 = 2M - 1 \neq 4^n(8k+1)$ for every $n, k \in \mathbb{N}_0$.

Now assume that $M^2 - (M-1)^2 = 2M - 1 = 4^n(8k+7)$ for some $n, k \in \mathbb{N}_0$. This relation implies that $n = 0$ and $M = 4(k+1)$. Thus $\frac{M}{2} \in \mathbb{N}_0$ and so

$$\begin{aligned} f\bigl(M^2\bigr) &= f\Bigl(\Bigl(\frac{M}{2}\Bigr)^2 + \Bigl(\frac{M}{2}\Bigr)^2 + \Bigl(\frac{M}{2}\Bigr)^2 + \Bigl(\frac{M}{2}\Bigr)^2\Bigr) = 4g\Bigl(\Bigl(\frac{M}{2}\Bigr)^2\Bigr) = \\ &= 4\Bigl(A\Bigl(\frac{M}{2}\Bigr)^2 + B\Bigr) = AM^2 + 4B. \end{aligned}$$

Similarly as above, we have

$$AM^2 + 4B = f\bigl(M^2\bigr) = f\bigl(M^2 + 0^2 + 0^2 + 0^2\bigr) = g\bigl(M^2\bigr) + 3g(0) = g\bigl(M^2\bigr) + 3B,$$

which implies that

$$g\bigl(M^2\bigr) = AM^2 + B.$$

Hence, (2.3) holds for every $m \in \mathbb{N}_0$. Therefore, the proof of Lemma 4 is complete. ■

3. Proof of Theorem 1

Assume that function f, g satisfy (1.1). It follows from Lemma 1 that for every $n \in \mathbb{N}_0$ there exist $a, b, c, d \in \mathbb{N}_0$ such that

$$n = a^2 + b^2 + c^2 + d^2.$$

Then we infer from (1.1) and (2.3) that

$$\begin{aligned} f(n) &= f\big(a^2 + b^2 + c^2 + d^2\big) = g\big(a^2\big) + g\big(b^2\big) + g\big(c^2\big) + g\big(d^2\big) = \\ &= \big(Aa^2 + B\big) + \big(Ab^2 + B\big) + \big(Ac^2 + B\big) + \big(Ad^2 + B\big) = \\ &= A\big(a^2 + b^2 + c^2 + d^2\big) + 4B = An + 4B \end{aligned}$$

is satisfied for every $n \in \mathbb{N}_0$.

Theorem 1 is thus proved. ∎

4. Proof of Theorem 2

Assume that the arithmetical functions $F, G : \mathbb{N}_0 \to \mathbb{C}$ satisfy the relation (1.3). Now we prove the following lemmas.

Lemma 5. *Assume that the functions $F, G : \mathbb{N}_0 \to \mathbb{C}$ satisfy (1.3) for every $a, b, c, d \in \mathbb{N}_0$. Then*

$$G\big(n^2 + m^2\big) = C\big(n^2 + m^2\big) + D \quad \textit{for every} \quad n, m \in \mathbb{N}_0, \tag{4.1}$$

where $C = G(1) - G(0)$ and $D = G(0)$.

Proof. First we prove that (4.1) holds for $n^2 + m^2 \in \{0, 1, 2, 4, 5\}$. It follows from the definitions of C and D that (4.1) holds for the cases $n^2 + m^2 \in \{0, 1\}$.

We obtain from (1.3) that

$$F(2) = F\big(1^2 + 1^2 + 0^2 + 0^2\big) = G\big(1^2 + 1^2\big) + G\big(0^2 + 0^2\big) = G(2) + G(0)$$

and

$$F(2) = F\big(1^2 + 0^2 + 1^2 + 0^2\big) = G\big(1^2 + 0^2\big) + G\big(1^2 + 0^2\big) = 2G(1),$$

consequently $G(2) = 2G(1) - G(0) = 2C + D$. Thus, (4.1) is true for $n^2 + m^2 = 2$.

We also have

$$F(4) = F\big(2^2 + 0^2 + 0^2 + 0^2\big) = G\big(2^2 + 0^2\big) + G\big(0^2 + 0^2\big) = G(4) + G(0) = G(4) + D$$

and

$$F(4) = F\big(1^2+1^2+1^2+1^2\big) = G\big(1^2+1^2\big)+G\big(1^2+1^2\big) = 2G(2) = 2(2C+D),$$

which give $G(4) = 4C + D$, consequently (4.1) is true for $n^2 + m^2 = 4$.

Finally, using the two relations

$$F(5) = F\big(2^2+0^2+1^2+0^2\big) = G\big(2^2+0^2\big)+G\big(1^2+0^2\big) = G(4)+G(1) = 5C+2D$$

and

$$F(5) = F\big(2^2+1^2+0^2+0^2\big) = G\big(2^2+1^2\big)+G\big(0^2+0^2\big) = G(5)+G(0) = G(5)+D,$$

we obtain that $G(5) = 5C + D$. Thus, (4.1) is true for $n^2 + m^2 = 5$.

Now we assume that (4.1) is true for every $n^2 + m^2 < N^2 + M^2, N \le M$. As we have seen above, we have $N^2 + M^2 > 5$, and so $M \ge 2$.

(a) We consider the cases when $N = 0$. The proof of $G\big(M^2 + N^2\big) = C\big(M^2 + N^2\big) + D$ in this case is similar to the proof of Lemma 3. Indeed, if $M^2 - (M-1)^2 = 2M - 1 \ne 4^n(8k+7)$ for every $n, k \in \mathbb{N}_0$, then Lemma 2 implies that there are $x, y, z \in \mathbb{N}_0$ such that

$$M^2 - (M-1)^2 = 2M - 1 = x^2 + y^2 + z^2.$$

It is clear that $(M-1)^2+x^2, y^2+z^2 < N^2+M^2$, and so by our assumptions, we have $G\big((M-1)^2+x^2\big) = C\big((M-1)^2+x^2\big)+D$ and $G\big(y^2+z^2\big) = C\big(y^2+z^2\big)+D$. On the other hand, we have

$$\begin{aligned}F\big(M^2\big) &= F\big((M-1)^2 + x^2 + y^2 + z^2\big) = G\big((M-1)^2 + x^2\big) + G(y^2+z^2) = \\ &= \big(C((M-1)^2 + x^2) + D\big) + \big(C(y^2+z^2) + D\big) = \\ &= C\big((M-1)^2 + x^2 + y^2 + z^2\big) + 2D = CM^2 + 2D.\end{aligned}$$

But

$$\begin{aligned}CM^2 + 2D = F\big(M^2\big) &= F\big(M^2 + 0^2 + 0^2 + 0^2\big) = G\big(M^2 + 0^2\big) + G\big(0^2+0^2\big) = \\ &= G\big(M^2\big) + D,\end{aligned}$$

which implies that

$$G\big(M^2\big) = CM^2 + D.$$

Consequently Lemma 5 is proved for the case $M^2 - (M-1)^2 = 2M - 1 \ne 4^n(8k+1)$ for every $n, k \in \mathbb{N}_0$.

Now assume that $M^2 - (M-1)^2 = 2M - 1 = 4^n(8k+7)$ for some $n, k \in \mathbb{N}_0$. This relation implies that $n = 0$ and $M = 4(k+1)$. Thus $\frac{M}{2} \in \mathbb{N}_0$ and so

$$\begin{aligned}F(M^2) &= F\left(\left(\frac{M}{2}\right)^2 + \left(\frac{M}{2}\right)^2 + \left(\frac{M}{2}\right)^2 + \left(\frac{M}{2}\right)^2\right) = 2G\left(\left(\frac{M}{2}\right)^2 + \left(\frac{M}{2}\right)^2\right) = \\ &= 2\left(C\left(\left(\frac{M}{2}\right)^2 + \left(\frac{M}{2}\right)^2\right) + D\right) = CM^2 + 2D.\end{aligned}$$

Similarly as above, we have

$$CM^2 + 2D = F\big(M^2\big) = F\big(M^2 + 0^2 + 0^2 + 0^2\big) = G\big(M^2 + 0^2\big) + G\big(0^2 + 0^2\big) = \\ = G\big(M^2\big) + D,$$

which implies that

$$G\big(M^2\big) = CM^2 + D.$$

Thus, Lemma 5 is proved in the case $N = 0$.

(b) Assume that $N \geq 1$. Then $N^2 + 1^2 < N^2 + M^2$, $M^2 + 0^2 < N^2 + M^2$ and

$$G\big(N^2 + 1^2\big) = C\big(N^2 + 1\big) + D, \quad G\big(M^2\big) = CM^2 + D.$$

On the other hand, we have

$$F\big(N^2 + M^2 + 0^2 + 1^2\big) = G\big(N^2 + M^2\big) + G\big(0^2 + 1^2\big) = G\big(N^2 + M^2\big) + G(1)$$

and

$$\begin{aligned} F\big(N^2 + M^2 + 0^2 + 1^2\big) &= G\big(N^2 + 1^2\big) + G\big(M^2 + 0^2\big) = \\ &= \big(C\big(N^2 + 1\big) + D\big) + \big(CM^2 + D\big) = \\ &= C\big(N^2 + M^2\big) + C + 2D = \\ &= C\big(N^2 + M^2\big) + D + G(1). \end{aligned}$$

These imply that

$$G\big(N^2 + M^2\big) = C\big(N^2 + M^2\big) + D,$$

which completes the proof of Lemma 5. ∎

Proof of Theorem 2. Assume that function F, G satisfy (1.3). It follows from Lemma 2 that for every $n \in \mathbb{N}_0$ there exist $a, b, c, d \in \mathbb{N}_0$ such that

$$n = a^2 + b^2 + c^2 + d^2.$$

Then we infer from (1.3) and (4.1) that

$$\begin{aligned} F(n) = F\big(a^2 + b^2 + c^2 + d^2\big) &= G\big(a^2 + b^2\big) + G\big(c^2 + d^2\big) = \\ &= \big(C\big(a^2 + b^2\big) + D\big) + \big(C\big(c^2 + d^2\big) + D\big) = \\ &= C\big(a^2 + b^2 + c^2 + d^2\big) + 2D = Cn + 2D \end{aligned}$$

is satisfied for every $n \in \mathbb{N}_0$.

Theorem 2 is thus proved. ∎

5. Proofs of the corollaries

Assume that the arithmetical function $f : \mathbb{N}_0 \to \mathbb{C}$ satisfies the relation

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

for every $a, b, c, d \in \mathbb{N}_0$. Then Theorem 1 implies that $f(n) = An + 4B$ and $f\big(m^2\big) = Am^2 + 2B$ for every $n, m \in \mathbb{N}$, consequently $B = 0$ and $f(n) = An$ for every $n \in \mathbb{N}$. Corollary 1 is thus proved. ■

If the arithmetical function $F : \mathbb{N}_0 \to \mathbb{C}$ satisfies the relation

$$F\big(a^2 + b^2 + c^2 + d^2\big) = F\big(a^2 + b^2\big) + F\big(c^2 + d^2\big)$$

for every $a, b, c, d \in \mathbb{N}_0$, then Theorem 2 implies that $f(n) = Cn + 2D$ and $f(m^2) = Cm^2 + D$ for every $n, m \in \mathbb{N}$. Consequently $D = 0$ and $f(n) = Cn$ for every $n \in \mathbb{N}$. Corollary 2 is thus proved. ■

References

[1] **Helfgott, H.A.,** The ternary Goldbach conjecture is true, in: *Proceedings of the International Congress of Mathematicians—Seoul*, 2014. Vol. II, 391—418, Kyung Moon Sa, Seoul, 2014.

[2] **Kátai, I. and B.M. Phong,** A consequence of the ternary Goldbach theorem, *Publ.Math.Debrecen*, **86** (2015), 465–471.

[3] **Kátai, I. and B.M. Phong,** The functional equation $f(\mathcal{A}+\mathcal{B}) = g(\mathcal{A}) + h(\mathcal{B})$, *Annales Univ. Sci. Budapest., Sect. Comp.*, **43** (2014), 287–301.

[4] **Khanh, B.M.M.,** Characterization of arithmetical function with functional equation, *Annales Univ. Sci. Budapest., Sect. Comp.*, **45** (2016), 223—237.

I. Kátai and B. M. Phong
Department of Computer Algebra
Faculty of Informatics
Eötvös Loránd University
H-1117 Budapest, Pázmány Péter sétány 1/C
Hungary
katai@inf.elte.hu
bui@inf.elte.hu