Bull. Korean Math. Soc. **60** (2023), No. 1, pp. 75–81
https://doi.org/10.4134/BKMS.b210915
pISSN: 1015-8634 / eISSN: 2234-3016

MULTIPLICATIVE FUNCTIONS COMMUTABLE WITH BINARY QUADRATIC FORMS $x^2 \pm xy + y^2$

Poo-Sung Park

Abstract. If a multiplicative function f is commutable with a quadratic form $x^2 + xy + y^2$, i.e.,

$$f(x^2 + xy + y^2) = f(x)^2 + f(x)\,f(y) + f(y)^2,$$

then f is the identity function. In other hand, if f is commutable with a quadratic form $x^2 - xy + y^2$, then f is one of three kinds of functions: the identity function, the constant function, and an indicator function for $\mathbb{N} \setminus p\mathbb{N}$ with a prime p.

1. Introduction

In 2014, Bašić [1] classified arithmetic functions f satisfying

$$f(m^2 + n^2) = f(m)^2 + f(n)^2$$

for all positive integers m and n. His result was a variation of Chung's work [2], which was inspired from Claudia Spiro's study about *additive uniqueness sets* [6]. It is naturally generalized to studying arithmetic functions f satisfying

$$f\big(Q(x_1, x_2, \dots, x_k)\big) = Q\big(f(x_1), f(x_2), \dots, f(x_k)\big)$$

for various quadratic forms Q. After Bašić's work for $Q(x, y) = x^2 + y^2$, You et al. [7] and Khanh [4] studied about $Q(x, y) = x^2 + ky^2$.

The author extended Bašić's work to multiplicative functions commutable with sums of more than 2 squares. That is, if a multiplicative function f satisfies

$$f(x_1^2 + x_2^2 + \cdots + x_k^2) = f(x_1)^2 + f(x_2)^2 + \cdots + f(x_k)^2$$

for $k \geq 3$, then f is uniquely determined to be the identity function [5].

Let $Q(x, y) = ax^2 + bxy + cy^2$ be a positive definite binary quadratic form with $a, b, c \in \mathbb{Z}$. The value $b^2 - 4ac$ is called *discriminant* of Q. The discriminant

Received December 21, 2021; Revised March 16, 2022; Accepted April 22, 2022.
2020 *Mathematics Subject Classification.* Primary 11A25, 11E20.
Key words and phrases. Additive uniqueness, multiplicative function, functional equation, quadratic form.
This work was supported by Kyungnam University Foundation Grant, 2019.

of the smallest absolute value is -3 for $x^2 \pm xy + y^2$. So, it is a natural question to ask which multiplicative function f satisfies the condition

$$f(x^2 \pm xy + y^2) = f(x)^2 \pm f(x)\, f(y) + f(y)^2.$$

In this article, we classify such multiplicative functions.

2. Results

Theorem 2.1. *If a multiplicative function $f : \mathbb{N} \to \mathbb{C}$ satisfies*

$$f(x^2 + xy + y^2) = f(x)^2 + f(x)\, f(y) + f(y)^2,$$

then f is the identity function.

Proof. We will show that $f(n) = n$ for $1 \le n \le 28$ and use induction.

Note that $f(1) = 1$ and $f(3) = 3$ with $x = y = 1$. Since f is multiplicative, the values of f at powers of primes determine f.

If n is not divisible by 3, then $f(n^2) = f(n)^2$ from

$$\begin{aligned} f(3n^2) &= f(3)\, f(n^2) = 3f(n^2) \\ &= f(n^2 + n \cdot n + n^2) = 3f(n)^2. \end{aligned}$$

Thus, $f(4) = f(2)^2$, $f(16) = f(4)^2$, and $f(25) = f(5)^2$.

Since

$$\begin{aligned} f(7) &= f(1^2 + 1 \cdot 2 + 2^2) = 1 + f(2) + f(2)^2, \\ f(13) &= f(1)^2 + f(1)\, f(3) + f(3)^2 = 13, \\ f(21) &= f(3)\, f(7) = 3f(7) \\ &= f(1)^2 + f(1)\, f(4) + f(4)^2 = 1 + f(2)^2 + f(2)^4, \\ f(39) &= f(3)\, f(13) = 39 \\ &= f(2)^2 + f(2)\, f(5) + f(5)^2, \\ f(91) &= f(7)\, f(13) = 13\, f(7) \\ &= f(5)^2 + f(5)\, f(6) + f(6)^2 = f(5)^2 + 3f(2)f(5) + 9f(2)^2, \end{aligned}$$

we can conclude that $f(n) = n$ for $n = 2, 4, 16, 5, 7, 13$.

Since

$$\begin{aligned} f(84) &= f(4)\, f(3)\, f(7) = 4 \cdot 3 \cdot 7 = 84 \\ &= f(2)^2 + f(2)\, f(8) + f(8)^2 = 4 + 2f(8) + f(8)^2, \\ f(43) &= f(1)^2 + f(1)\, f(6) + f(6)^2 = 43, \\ f(129) &= f(3)\, f(43) = 3 \cdot 43 = 129 \\ &= f(5)^2 + f(5)\, f(8) + f(8)^2 = 25 + 5f(8) + f(8)^2, \end{aligned}$$

we can find $f(8) = 8$.

Since $f(7) = 7$ and

$$f\big(3^2 + 3\cdot(2\cdot 3) + (2\cdot 3)^2\big) = f(3)^2 + f(3)\,f(2\cdot 3) + f(2\cdot 3)^2 = 7f(3)^2$$
$$= f(7\cdot 3^2) = f(7)\,f(9),$$

we obtain that $f(9) = 9$.

The next prime is 11. But we need to find $f(19)$ to determine $f(11)$. Note that $f(19) = f(2)^2 + f(2)\,f(3) + f(3)^2 = 19$. Now, since

$$\begin{aligned} f(133) &= f(7)\,f(19) = 7\cdot 19 = 133\\ &= f(1)^2 + f(1)\,f(11) + f(11)^2 = 1 + f(11) + f(11)^2,\\ f(247) &= f(13)\,f(19) = 13\cdot 19 = 247\\ &= f(7)^2 + f(7)\,f(11) + f(11)^2 = 49 + 7f(11) + f(11)^2, \end{aligned}$$

we can find $f(11) = 11$.

Note that

$$\begin{aligned} f(399) &= f(3)\,f(7)\,f(19) = 3\cdot 7\cdot 19 = 399\\ &= f(5)^2 + f(5)\,f(17) + f(17)^2 = 25 + 5f(17) + f(17)^2,\\ f(427) &= f(3)^2 + f(3)\,f(19) + f(19)^2 = 427\\ &= f(6)^2 + f(6)\,f(17) + f(17)^2 = 36 + 6f(17) + f(17)^2. \end{aligned}$$

Thus, $f(17) = 17$.

We have $f(23) = 23$ from

$$\begin{aligned} f(553) &= f(7)\,f(79) = 7\left(f(3)^2 + f(3)\,f(7) + f(7)^2\right) = 7\cdot 79 = 553\\ &= f(1)^2 + f(1)\,f(23) + f(23)^2 = 1 + f(23) + f(23)^2,\\ f(579) &= f(3)\,f(193) = 3\left(f(7)^2 + f(7)\,f(9) + f(9)^2\right) = 3\cdot 193 = 579\\ &= f(2)^2 + f(2)\,f(23) + f(23)^2 = 4 + 2f(23) + f(23)^2. \end{aligned}$$

Note that

$$f(27) = f(3)^2 + f(3)\,f(3) + f(3)^2 = 27.$$

From the above results, it appears that $f(n) = n$ for $1 \le n \le 28$.

Now, consider $f(n)$ for $n \ge 29$. We divide two cases: $n = 2k+1$ and $n = 2k$.

Note that

$$\begin{aligned} &(2k+1)^2 + (2k+1)(k-3) + (k-3)^2\\ &= (2k-3)^2 + (2k-3)(k+2) + (k+2)^2 \end{aligned}$$

when $k > 3$. Thus, if we assume that $f(m) = m$ for all $m < n = 2k+1$, we can write a functional equation

$$\begin{aligned} &f(2k+1)^2 + f(2k+1)(k-3) + (k-3)^2\\ &= (2k-3)^2 + (2k-3)(k+2) + (k+2)^2 \end{aligned}$$

for $f(2k+1)$ by induction hypothesis and we obtain

$$f(2k+1) = 2k+1 \quad \text{or} \quad f(2k+1) = -3k+2.$$

In other hand, since

$$\begin{aligned} &f\left((2k+1)^2 + (2k+1)(k-10) + (k-10)^2\right) \\ =\ &f\left((2k-11)^2 + (2k-11)(k+5) + (k+5)^2\right) \end{aligned}$$

when $k > 10$, we obtain

$$f(2k+1) = 2k+1 \quad \text{or} \quad f(2k+1) = -3k+9.$$

Therefore, the solution satisfying both equalities simultaneously is that $f(n) = f(2k+1) = 2k+1$.

Similarly, from

$$\begin{aligned} &(2k)^2 + (2k)(k-7) + (k-7)^2 \\ =\ &(2k-8)^2 + (2k-8)(k+3) + (k+3)^2 \end{aligned}$$

with $k > 7$ we obtain that

$$f(2k) = 2k \quad \text{or} \quad f(2k) = -3k+7$$

if we assume that $f(m) = m$ for $m < n = 2k$. Also, from

$$\begin{aligned} &(2k)^2 + (2k)(k-14) + (k-14)^2 \\ =\ &(2k-16)^2 + (2k-16)(k+6) + (k+6)^2 \end{aligned}$$

with $k > 14$ we obtain that

$$f(2k) = 2k \quad \text{or} \quad f(2k) = -3k+14.$$

Therefore, we conclude that $f(n) = f(2k) = 2k$. □

Theorem 2.2. *A multiplicative function $f : \mathbb{N} \to \mathbb{C}$ satisfies*

$$f(x^2 - xy + y^2) = f(x)^2 - f(x)\,f(y) + f(y)^2$$

if and only if f is one of the following:

(1) *the identity function $f(n) = n$;*
(2) *the constant function $f(n) = 1$;*
(3) *the function f_p defined by*

$$f_p(n) = \begin{cases} 0, & p \mid n \\ 1, & p \nmid n \end{cases}$$

for some prime $p \equiv 2 \pmod 3$.

Proof. It is trivial that the identity function and the constant function satisfy the functional equation. Let us consider the third case f_p.

It is known that $p \equiv 2 \pmod 3$ if and only if p cannot be represented as $x^2 - xy + y^2$ [3]. Assume that $n = x^2 - xy + y^2$. Then $n = (x + \omega y)(x + \overline{\omega} y)$ with $\omega = (-1 + \sqrt{-3})/2$ is the factorization in $\mathbb{Z}[\omega]$ a PID. If n is divisible by

p, both x and y are divisible by p, since p is an inert prime in $\mathbb{Z}[\omega]$. Thus, the function f_p works well.

Now let us prove "only if" part. Note that

$$f(n^2) = f(n^2 - n \cdot n + n^2) = f(n)^2 - f(n)\,f(n) + f(n)^2 = f(n)^2.$$

We have that $f(1) = 1$. From the equalities

$$\begin{aligned} f(3) &= f(1)^2 - f(1)\,f(2) + f(2)^2 = 1 - f(2) + f(2)^2, \\ f(7) &= f(1)^2 - f(1)\,f(3) + f(3)^2 = 1 - f(3) + f(3)^2 \\ &= f(2)^2 - f(2)\,f(3) + f(3)^2 = f(2)^2 - f(2)\,f(3) + f(3)^2, \end{aligned}$$

there are three cases:

$$\begin{array}{llllll} f(1) = 1, & f(2) = 0, & f(3) = 1, & f(4) = 0, & f(6) = 0, & f(7) = 1; \\ f(1) = 1, & f(2) = 1, & f(3) = 1, & f(4) = 1, & f(6) = 1, & f(7) = 1; \\ f(1) = 1, & f(2) = 2, & f(3) = 3, & f(4) = 4, & f(6) = 6, & f(7) = 7. \end{array}$$

Since

$$\begin{aligned} f(1 - n + n^2) &= f(1^2 - 1 \cdot n + n^2) \\ &= 1 - f(n) + f(n)^2 \end{aligned}$$

and

$$\begin{aligned} f(1 - n + n^2) &= f\big((n-1)^2 - (n-1)n + n^2\big) \\ &= f(n-1)^2 - f(n-1)\,f(n) + f(n)^2, \end{aligned}$$

we have that

$$f(n-1)^2 - f(n-1)\,f(n) = 1 - f(n)$$

or

$$\big(f(n-1) - f(n) + 1\big)\big(f(n-1) - 1\big) = 0.$$

Thus, it yields a condition

$$(*) \qquad f(n-1) = 1 \quad \text{or} \quad f(n) = f(n-1) + 1.$$

So, if $f(2) = 2$, then $f(3) = 3$ and thus $f(4) = 4$, and so forth. We obtain the identity function $f(n) = n$ when $f(2) = 2$.

If $f(2) = 0$, then we have $f(3) = f(5) = f(7) = 1$ and $f(4) = f(6) = 0$. From

$$\begin{aligned} f\big(2^2 - 2 \cdot (2k) + (2k)^2\big) &= f(2)^2 - f(2)\,f(2k) + f(2k)^2 = f(2k)^2 \\ &= f(4 - 4k + 4k^2) = f(4)\,f(1 - k + k^2) = 0 \end{aligned}$$

we deduce that $f(2k) = 0$ for $k \geq 1$. Since $f(2k+1) = 1$ by condition $(*)$, $f(2) = 0$ yields a sequence alternating 1 and 0. That is, $f = f_2$.

Now, the condition $f(1) = f(2) = f(3) = f(4) = f(6) = f(7) = 1$ remains. If $f(n) = a$ for some $a \in \mathbb{C} \setminus \{1, 0, -1, -2, \dots\}$, then $f(m) \neq 1$ for all $m > n$. But, since $1 = f(2) = f(2^2) = f(2^4) = \cdots = f(2^{2^N})$ for sufficiently large N, it is a contradiction. So, we can deduce that $f(n)$ can have only integers ≤ 1.

Suppose that s is the smallest integer such that $f(s) = 0$. If there exists no such s, then f is a constant function $f(n) = 1$.

Since f is multiplicative and $f(n^2) = f(n)^2$, we can say that $s = p^{2k-1}$ with prime p and positive integer k. Note that

$$\begin{aligned} & f\left((p^{2k})^2 - p^{2k}p^{2k-1} + (p^{2k-1})^2\right) \\ &= f(p^{2k})^2 - f(p^{2k})\, f(p^{2k-1}) + f(p^{2k-1})^2 = f(p^{2k})^2 \\ &= f\left((p^{2k-1})^2(p^2 - p + 1)\right) = f(p^{2k-1})^2 f(p^2 - p + 1) = 0. \end{aligned}$$

Thus, $f(p^{2k}) = f(p^k)^2 = 0$. By the minimality of $s = p^{2k-1}$, we can deduce that $k = 1$. That is, s is the prime p itself.

Then, we obtain $f(p\ell) = 0$ for any positive integer ℓ, since

$$\begin{aligned} & f\left(p^2 - p(p\ell) + (p\ell)^2\right) \\ &= f(p)^2 - f(p)\, f(p\ell) + f(p\ell)^2 = f(p\ell)^2 \\ &= f\left(p^2(1 - \ell + \ell^2)\right) = f(p)^2 f(1 - \ell + \ell^2) = 0. \end{aligned}$$

That is, we can conclude that

$$f(n) = f_p(n) = 0 \text{ when } n \text{ is a multiple of } p$$

and $f(p\ell + 1) = 1$ by condition $(*)$.

Now, let n be a positive integer with $p \nmid n$. Then, there exists an integer m such that $nm \equiv 1 \pmod{p}$ and $(n, m) = 1$. Letting $nm = p\ell + 1$, we obtain

$$1 = f(p\ell + 1) = f(nm) = f(n)\, f(m).$$

Since f can have only integers ≤ 1, we can conclude that

$$(**) \qquad f(n) = \pm 1 \quad \text{if} \quad p \nmid n.$$

Now let us characterize the prime p. If p can be represented as $x^2 - xy + y^2$, then $0 = f(p) = f(x)^2 - f(x)\, f(y) + f(y)^2$. But, this never happen since $f(x)$ and $f(y)$ are ± 1. Hence, $p \equiv 2 \pmod{3}$.

If $f(n) = -1$ for $n \leq p - 2$, then $f(n + 1) = 0$ with $n + 1 \leq p - 1$ by $(*)$. But, this is impossible by $(**)$. Thus, if $f(n) = -1$ for $n \leq p - 1$, then $n = p - 1$. In this case, $f(d) = -1$ for a proper divisor d of $p - 1$ unless p is a Fermat prime. Thus, it is a contradiction. If $p = 2^{2^r} + 1$, then $-1 = f(p - 1) = f(2^{2^r}) = f(2^{2^{r-1}})^2$, which is impossible for $f(2^{2^{r-1}}) = \pm 1$. So, we can conclude that

$$f(1) = f(2) = f(3) = \cdots = f(p - 1) = 1 \text{ and } f(p) = 0.$$

Similarly, suppose that $f(n) = -1$ for some n. If $p(\ell - 1) + 1 \leq n \leq p\ell - 2$ with $\ell \geq 2$, then $f(n + 1) = 0$ with $p(\ell - 1) + 2 \leq n + 1 \leq p\ell - 1$ by $(*)$. But, this is a contradiction by $(**)$ since $n + 1$ is not a multiple of p. Hence, if $f(n) = -1$ with $p(\ell - 1) + 1 \leq n \leq p\ell - 1$, then $n = p\ell - 1$. Then, since $n - 1$

and n are relatively prime and $(n-1)n = (p\ell - 2)(p\ell - 1) \equiv 2 \not\equiv -1 \pmod{p}$, we can deduce a contradictory equality

$$\begin{aligned} f\big((n-1)n\big) &= f(n-1)f(n) = -1 \\ &= f\big((p\ell-2)(p\ell-1)\big) = 1. \end{aligned}$$

Therefore, we can conclude that $f(n) = f_p(n) = 1$ when n is not divisible by p. □

References

[1] B. Bašić, *Characterization of arithmetic functions that preserve the sum-of-squares operation*, Acta Math. Sin. (Engl. Ser.) **30** (2014), no. 4, 689–695. https://doi.org/10.1007/s10114-014-3112-9

[2] P. V. Chung, *Multiplicative functions satisfying the equation* $f(m^2+n^2) = f(m^2)+f(n^2)$, Math. Slovaca **46** (1996), no. 2-3, 165–171.

[3] D. A. Cox, *Primes of the form* $x^2 + ny^2$, A Wiley-Interscience Publication, John Wiley & Sons, Inc., New York, 1989.

[4] B. M. M. Khanh, *On conjecture concerning the functional equation*, Ann. Univ. Sci. Budapest. Sect. Comput. **46** (2017), 123–135.

[5] P.-S. Park, *On k-additive uniqueness of the set of squares for multiplicative functions*, Aequationes Math. **92** (2018), no. 3, 487–495. https://doi.org/10.1007/s00010-017-0517-4

[6] C. A. Spiro, *Additive uniqueness sets for arithmetic functions*, J. Number Theory **42** (1992), no. 2, 232–246. https://doi.org/10.1016/0022-314X(92)90022-H

[7] L. You, Y. Chen, P. Yuan, and J. Shen, *A characterization of arithmetic functions satisfying* $f(u^2 + kv^2) = f^2(u) + kf^2(v)$, arXiv:1606.05039 [math.NT].

Poo-Sung Park
Department of Mathematics Education
Kyungnam University
Changwon 51767, Korea
Email address: pspark@kyungnam.ac.kr