Annales Mathematicae Silesianae 12 (1998), 35–51

Prace Naukowe Uniwersytetu Śląskiego nr 1751, Katowice

ADDITIVE CONDITIONS ON SUMS OF SQUARES

IVAN KOREC

Abstract. Functions $F : \mathbb{N} \to \mathbb{R}$ which satisfy the condition $\forall x, y, z, w$
$(ax^2 + cy^2 = au^2 + cv^2 \implies a \cdot F(x) + c \cdot F(y) = a \cdot F(u) + c \cdot F(v))$
are considered. For some small positive integers a, c they are completely characterized. E.g., for $a = c = 1$ they form a 6-dimensional real vector space with a base consisting of $F_0(x) = x^2$ and five periodical functions with periods 1, ... , 5. Further, functions $F : \mathbb{N} \to \mathbb{R}$ which satisfy the condition
$$\forall x, y, z\,(x^2 = y^2 + z^2 \implies F(x) = F(y) + F(z))$$
are studied; 17 linearly independent examples of such functions are presented, including periodical ones with the periods 16, 9, 25, 13.

1. Introduction

Let $\mathbb{N}$ be the set of nonnegative integers and let $\mathbb{R}$ be the set of reals. We shall usually consider the functions $F : \mathbb{N} \to \mathbb{R}$, unless other domain and range are explicitly mentioned.

The square-additive functions (defined below by (2.1)) arose by investigation of elementary definability of addition from the quadratic form $x^2 + y^2$. Now this definability problem is solved. The square-additive functions are not explicitly used in the solution, but they help to refuse some attempts for defining formulas. However, the notion seems to be interesting in itself.

Conditions like (2.1) can be considered as natural generalizations of functional equations. It can also be rewritten in the form

$$F\left(\sqrt{x^2 + y^2 - u^2}\right) = F(x) + F(y) - F(u).$$

Received on August 11, 1998.

1991 *Mathematics Subject Classification.* Primary 11A25. Secondary 11Y99.

Key words and phrases: Square-additive functions.

This work is supported by Grant 5123 of Slovak Academy of Sciences.

However, considering this equation we have to assume that the left side is defined. Therefore the considered domain is very essential. Notice that Cauchy's functional equation (3.1) and the functional equation of the logarithm can be rewritten in a form similar to (2.1):

$$z = x + y \implies g(z) = g(x) + g(y), \qquad z = xy \implies g(z) = g(x) + g(y).$$

For positive integers a, c we shall define (a, c)-square-additive functions by (4.1). They are similarly related to the definability of addition from the quadratic forms $ax^2 + cy^2$. (This problem is now solved only for some pairs (a, c).) The vector space of (a, c)-square-additive functions has finite dimension; below it will be determined in some cases.

Finally, Pythagorean-additive functions (defined by (5.1)) are considered. The condition (5.1) is simpler and essentially weaker than (2.1). (Strictly speaking (5.1) is not a consequence of (2.1); it will be if we assume additionally $F(0) = 0$.) It will be shown that the set of Pythagorean-additive function is much richer (and more complex) than the set of square-additive functions. They form a vector space consisting of dimension at least 17 (and, maybe, infinite), while the square-additive functions form a vector space of dimension 6.

2. Square-additive functions

DEFINITION 2.1. A function $F : \mathbb{N} \to \mathbb{R}$ will be called square-additive if for all $x, y, u, v \in \mathbb{N}$

$$x^2 + y^2 = u^2 + v^2 \implies F(x) + F(y) = F(u) + F(v). \tag{2.1}$$

LEMMA 2.2. *For every integer $x > 6$ (and also for $x = 5$) there are nonnegative integers $y, u, v < x$ such that $x^2 + y^2 = u^2 + v^2$.*

PROOF. We can easily check that for all integers w, z

$$(5w + z)^2 + |2z|^2 = (3w - z)^2 + (4w + 2z)^2. \tag{2.2}$$

Further, if $w > |z|$ we have

$$|2z| < 5w + z, \qquad 0 \leqslant 3w - z < 5w + z, \qquad 0 \leqslant 4w + 2z < 5w + z.$$

Every integer x can be (uniquely) expressed as $5w + z$ for suitable integers w and $|z| \leqslant 2$. For $x \geqslant 13$ we have $w \geqslant 3 > |z|$, and the requested y, u, v can be obtained from (2.2). The same holds also for $x \in \{5, 9, 10, 11\}$ because

also for these x we have $w > |z|$. For the remaining three cases we can use the equalities

$$7^2+1^2=5^2+5^2, \qquad 8^2+1^2=7^2+4^2, \qquad 12^2+1^2=8^2+9^2. \qquad \square$$

COROLLARY 2.3. *A square-additive function is uniquely determined by its values for* $x \in \{0,1,2,3,4,6\}$.

The square-additive functions obviously form a vector space over $\mathbb{R}$; its basis is given in the following theorem, where the symbol $a \operatorname{MOD}(n)$ denotes the smallest nonnegative residue of a mod n.

THEOREM 2.4. *There are six linearly independent square-additive functions:*

$$F_0(x)=x^2, \qquad F_2(x)=x^2 \operatorname{MOD} 2, \qquad F_4(x)=\tfrac{x^3-x}{2} \operatorname{MOD} 2,$$
$$F_1(x)=1, \qquad F_3(x)=x^2 \operatorname{MOD} 3, \qquad F_5(x)=(x^2+1) \operatorname{MOD} 5,$$

and every square-additive function is a linear combination of these functions.

PROOF. To prove the first assertion let us consider at first the function F_5 and assume that $x^2+y^2=u^2+v^2$. Let $X = x^2 \operatorname{MOD} 5$, and define analogously Y, U, V. Notice that $F_5(x)$ is uniquely determined by X (and the same applies for the other letters). We have

$$X+Y \equiv U+V \pmod 5 \qquad \text{and} \qquad X,Y,U,V \in \{0,1,4\},$$

and we may assume $X \leqslant Y$, $U \leqslant V$, $X \leqslant U$. If $\{X,Y\}=\{U,V\}$ then obviously $F(x)+F(y)=F(u)+F(v)$. Otherwise we can see that $X=0$, $Y=0$, $U=1$, $V=4$, and therefore $F(x)+F(y)=2=F(u)+F(v)$.

The proofs for F_2, F_3, and F_4 are similar (but easier) and the proofs for F_0 and F_1 are trivial.

To prove that these functions are linearly independent, let us form the matrix consisting of the values $F_i(x)$ for $x \in \{0,1,2,3,4,6\}$.

(2.3)
$$\begin{array}{c} \\ x=0 \\ x=1 \\ x=2 \\ x=3 \\ x=4 \\ x=6 \end{array} \begin{array}{c} \begin{array}{cccccc} F_0 & F_1 & F_2 & F_3 & F_4 & F_5 \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 2 \\ 4 & 1 & 0 & 1 & 1 & 0 \\ 9 & 1 & 1 & 0 & 0 & 0 \\ 16 & 1 & 0 & 1 & 0 & 2 \\ 36 & 1 & 0 & 0 & 0 & 2 \end{pmatrix} \end{array}.$$

Its determinant is non-zero (it is equal to -120), and hence the columns of the matrix are linearly independent.

Now consider any square additive function F. Corollary 2.3 shows that the transposed vector $[F(i)]_{i=0,1,2,3,4,6}$ can be expressed as a linear combination of the columns of the matrix (2.3) and this implies our assertion. □

NOTATION. The symbols F_i will be always used below in the sense introduced in Theorem 2.4. (Sometimes a new domain will be specified; e.g., F_0 and F_1 can be considered on $\mathbb{R}$.)

COROLLARY 2.5. (i) *Every bounded square-additive function is periodical and its period is a divisor of* 60. *Conversely, every divisor of* 60 *is such a period.*

(ii) *For every square-additive function* $F : \mathbb{N} \to \mathbb{N}$ *there exists* $k \in \mathbb{N}$ *such that* $\lim_{x\to\infty} \frac{F(x)}{x^2} = \frac{k}{120}$. *Conversely, for every* $k \in \mathbb{N}$ *such* F *exists.*

PROOF. To prove (i) observe first that for $i = 1, \dots, 5$ the function F_i is of period i. The number 60 is the smallest common multiple of these periods. Further, if f, g have relatively prime periods p, q then $f + g$ has the period pq. So we can obtain all divisors of 60 as the periods of sums of at most three functions F_i, $1 \leqslant i \leqslant 5$.

For the first part of (ii) let us consider any square-additive function $F : \mathbb{N} \to \mathbb{N}$. It can be (uniquely) expressed as a linear combination of the functions F_i. Its coefficients are determined by the system of linear equations $A\mathbf{x} = \mathbf{a}$ with the matrix A given by (2.3) and $\mathbf{a}$ being the transposed vector $[F(0), F(1), F(2), F(3), F(4), F(6)]$. Since the determinant of A equals 120 and the limit $\lim_{x\to\infty} F(x)x^{-2}$ equals the coefficient of F_0, which obviously cannot be negative, we arrive at the first assertion of (ii).

For the second part of (ii) it suffices to construct F only for $k = 1$; the functions for the other k can be obtained as its multiples. Let us consider the square-additive function g defined by $g(x) = 0$ for $0 \leqslant x \leqslant 4$ and $g(6) = 1$. (Now we know that all its values are integers; the nonnegativity will be verified later.) Solving the system of linear equation described above we obtain the formula

$$g(x) = \tfrac{1}{120}F_0(x) - \tfrac{1}{5}F_1(x) + \tfrac{1}{8}F_2(x) - \tfrac{1}{3}F_3(x) + \tfrac{1}{2}F_4(x) + \tfrac{1}{5}F_5(x).$$

Since the coefficient of F_0 is positive almost all values of g are nonnegative; if we add a suitable multiple of F_1 then all values of the new functions will be nonnegative. (However, no addition is necessary. Indeed, we can verify that $F(7) = 0$, and for $x \geqslant 8$ the first member is greater than the sum of absolute values of both negative members.) Further, obviously $\lim_{x\to\infty} \frac{g(x)}{x^2} = \frac{1}{120}$. □

THEOREM 2.6. (i) *Every square-additive function F satisfies the linear recurrence*

$$F(x+12) = F(x+9) + F(x+8) + F(x+7) - \\ - F(x+5) - F(x+4) - F(x+3) + F(x). \tag{2.4}$$

(ii) *No linear recurrence of degree less than* 12 *is satisfied by all square-additive functions.*

PROOF. (i) It is not difficult to verify that the functions $F_0, \dots, F_5$ satisfy the given linear recurrence.

(ii) Let us consider the following 12 functions:

$$g_1(x) = F_0(x), \quad g_2(x) = 2x+1 = F_0(x+1) - F_0(x), \quad g_3(x) = 1 = F_1(x),$$
$$g_4(x) = 2F_3(x) - 3F_1(x), \quad g_5(x) = g_4(x+1),$$
$$g_6(x) = 3F_4(x) - F_1(x), \quad g_7(x) = g_6(x+1), \quad g_8(x) = g_6(x+2),$$
$$g_9(x) = F_5(x) - F_1(x), \quad g_{9+i}(x) = g_9(x+i) \text{ for } i = 1,2,3.$$

Since they arise from F_i $(i = 0, \dots, 5)$ by shifts and linear combinations they satisfy every linear recurrence which is satisfied by all square-additive functions. Now it suffices to show that the functions g_i $(i = 1, \dots, 12)$ are linearly independent. Let

$$\sum_{i=1}^{12} a_i g_i(x) = 0 \tag{2.4}$$

for all $x \in \mathbb{N}$. By growth considerations we can see that $a_1 = a_2 = 0$. The functions $g_4, \dots, g_{12}$ are periodical with the average value 0, and hence $a_3 = 0$. Since the remaining functions have periods 3, 4, 5 (and average value 0) we have

$$0 = \sum_{y=x}^{x+39} \sum_{i=4}^{12} a_i g_i(y) = \sum_{i=4}^{12} \sum_{y=x}^{x+39} a_i g_i(y) = \sum_{i=4}^{5} a_i g_i(x).$$

Analogously (by summation of (2.4) for 45 or 36 consecutive values of x) we can separate the functions g_i from the last two rows. It remains to prove the linear independence for every row separately, and that is easy (e.g., by computing three determinants of degrees 2, 3, 4). □

3. Generalization to other domains

The notion of square-additive functions can be modified to functions with other domains in the obvious way. If the domain of a square-additive function F contains both x and $-x$ then necessarily $F(-x) = F(x)$. We can obtain that from (2.1) by the substitution $y = -x$, $u = x$, $v = x$. So it is not too essential in the following theorems whether we consider also negative numbers or not. (The theorems could be easily reformulated for the nonnegative reals or nonnegative rational numbers.)

Remember that Cauchy's functional equation is

$$g(x+y) = g(x) + g(y), \tag{3.1}$$

and it is usually considered on the domain $\mathbb{R}$ (and with the quantifiers $(\forall x, y \in \mathbb{R})$). Its continuous solutions are linear functions $g(x) = kx$, $k \in \mathbb{R}$. However, there are also $2^{\mathfrak{c}}$ discontinuous solutions, where $\mathfrak{c}$ denotes the cardinality of continuum, which can be obtained through Hamel's basis using axiom of choice. Notice that every solution g of (3.1) is an odd function (i.e., $g(-x) = g(x)$ for all x), and that for odd functions it suffices to consider nonnegative x, y in (3.1).

THEOREM 3.1. (i) *A function $F : \mathbb{R} \to \mathbb{R}$ is square-additive if and only if there is a real a and a solution g of Cauchy's functional equation such that for all x*

$$F(x) = a + g(x^2). \tag{3.2}$$

(ii) *There are $2^{\mathfrak{c}}$ square-additive functions on $\mathbb{R}$.*

PROOF. (i) Let $a \in \mathbb{R}$, let g be a solution of (3.1), and let F be defined by (3.2) and let x, y, u, v satisfy $x^2 + y^2 = u^2 + v^2$. Then

$$\begin{aligned} F(x) + F(y) &= a + g(x^2) + a + g(y^2) = 2a + g(x^2 + y^2) = \\ &= 2a + g(u^2 + v^2) = a + g(u^2) + a + g(v^2) = F(u) + F(v). \end{aligned}$$

Conversely, let F be a square-additive function on $\mathbb{R}$ and let $g : \mathbb{R} \to \mathbb{R}$ be defined by

$$g(x) = \begin{cases} F\left(\sqrt{|x|}\right) - F(0) & \text{if } x \geqslant 0 \\ F(0) - F\left(\sqrt{|x|}\right) & \text{if } x < 0. \end{cases} \tag{3.3}$$

We can easily verify that g is a solution of Cauchy's equation. Indeed, g is an odd function and for nonnegative x, y we have

$$g(x+y) = F\left(\sqrt{x+y}\right) - F(0) = F\left(\sqrt{x+y}\right) + F(0) - 2F(0) =$$
$$= F\left(\sqrt{x}\right) + F\left(\sqrt{y}\right) - 2F(0) = g(x) + g(y).$$

(It was essential here that $\sqrt{x}$, $\sqrt{y}$, $\sqrt{x+y}$ exist; similar computation does not hold for the domains $\mathbb{N}$, $\mathbb{Z}$ or $\mathbb{Q}$.)

The formulas (3.2) and (3.3) give (mutually inverse) bijections between the set of square additive functions and the cartesian product of $\mathbb{R}$ with the set of solutions of Cauchy's equation and we obtain that (3.2) holds with $a = F(0)$. Finally, the assertion (ii) is an easy consequence of (i) and the existence of 2^c solutions of Cauchy's functional equation (3.2). □

THEOREM 3.2. *A function $F : \mathbb{Q} \to \mathbb{R}$ is square-additive if and only if F is a linear combination of $F_0(x) = x^2$ and $F_1(x) = 1$.*

PROOF. The sufficiency of the condition is obvious. To prove its necessity let us consider the restriction of F to the set $\mathbb{N}$. By adding a suitable multiple of F_0 we can assume that this restriction is bounded. If suffices to show that the modified function is constant, i.e., a multiple of F_1.

Let us take an arbitrary positive rational number $\frac{p}{q}$, put $y = \frac{1}{60q}$, and consider the restriction G of the function F to the set $M_y = \{ky \mid k \in \mathbb{N}\}$. The properties of square-additive functions on M_y are quite analogous to their properties on $\mathbb{N}$. In particular, G can be expressed as a linear combination of the functions G_i defined by

$$G_i(x) = F_i(60qx) \text{ for all } x \in M_y,\ i = 0, 1, \ldots, 5.$$

Since G is bounded on $\mathbb{N}$ the function G_0 is used with the coefficient 0, and hence G is periodical with the period $60y$ (it need not be the smallest one). Hence

$$F\left(\tfrac{p}{q}\right) = G\left(\tfrac{p}{q}\right) = G(60py) = G(0) = F(0),$$

i.e., (the modified) F is a constant function. □

4. (a, c)-square-additive functions

Now we shall consider the following generalization of square-additivity. (We again consider the functions on $\mathbb{N}$, and variables usually range over $\mathbb{N}$.)

DEFINITION 4.1. A function $F : \mathbb{N} \to \mathbb{R}$ will be called (a, c)-*square-additive* if for all $x, y, u, v \in \mathbb{N}$

$$(4.1)\quad ax^2 + cy^2 = au^2 + cv^2 \implies a \cdot F(x) + c \cdot F(y) = a \cdot F(u) + c \cdot F(v).$$

Without loss of generality we may assume that a, c are relatively prime and $a \geqslant c$. (Otherwise we can interchange a, c or divide a, c by its greatest common divisor.) The original notion is obviously obtained by the choice $a = c = 1$ but this case is usually not included in the statements below.

LEMMA 4.2. (i) *For all integers (and even all reals) r, s we have*

$$a \cdot \left(\tfrac{a+c}{2} r + s\right)^2 + cs^2 = a \cdot \left(\tfrac{a-c}{2} r + s\right)^2 + c \cdot \left(ar + s\right)^2. \tag{4.2}$$

(ii) *For every (a, c)-square-additive functions F it holds*

$$a \cdot F\left(\left|\tfrac{a+c}{2} r + s\right|\right) + c \cdot F(|s|) = a \cdot F\left(\left|\tfrac{a-c}{2} r + s\right|\right) + c \cdot F\left(|ar + s|\right). \tag{4.3}$$

provided all terms are defined (i.e., the arguments of F belong to $\mathbb{N}$).

PROOF. The formula (4.2) can be directly verified, and then (4.3) is a consequence of (4.1). □

LEMMA 4.3. *For every two integers $a > c > 0$ there is a positive integer x_0 such that*

$$\begin{aligned}(\forall x > x_0)(\exists y, u, v < x)\, &\left(ax^2 + cy^2 = au^2 + cv^2 \vee\right. \\ &\left. \vee\ ay^2 + cx^2 = au^2 + cv^2\right).\end{aligned} \tag{4.4}$$

Moreover, we can take $x_0 = \lfloor \frac{a}{2} \rfloor$ if $a + c$ is even and $x_0 = a$ if $a + c$ is odd.

PROOF. (Remember once more that y, u, v range over $\mathbb{N}$.) If $a + c$ is even we can substitute $r = -1$, $s = x$ into (4.2), and we obtain

$$a \cdot \left(x - \tfrac{a+c}{2}\right)^2 + cx^2 = a \cdot \left(x - \tfrac{a-c}{2}\right)^2 + c \cdot (x - a)^2.$$

For $x > \frac{a}{2}$ we have

$$\left|x - \tfrac{a+c}{2}\right| < x, \qquad \left|x - \tfrac{a-c}{2}\right| < x, \qquad |x - a| < x,$$

and the expressions on the left are integers.

If $a + c$ is odd we can similarly substitute $r = -2$, $s = x$, and we obtain

$$a \cdot (x - a - c)^2 + cx^2 = a \cdot (x + c - a)^2 + c \cdot (x - 2a)^2.$$

We can verify that for $x > a$ one has

$$|x - a - c| < x, \qquad |x + c - a| < x, \qquad |x - 2a| < x. \qquad \square$$

a \ c	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
1	6				:					:					:					:					:				
2	2	.			:					:					:					:					:				
3	1	3	.		:					:					:					:					:				
4	3	.	3	.	:					:					:					:					:				
5	2	5	2	5	.					:					:					:					:				
6	6	.	.	.	5	.				:					:					:					:				
7	3	7	3	7	3	7	.			:					:					:					:				
8	4	.	4	.	6	.	6	.		:					:					:					:				
9	4	8	.	8	4	.	3	8	.	:					:					:					:				
10	10	.	10	.	.	.	10	.	9	.					:					:					:				
11	5	11	5	11	5	11	5	9	5	11	.				:					:					:				
12	9	.	.	.	9	.	9	.	.	.	11	.			:					:					:				
13	6	13	6	13	6	13	6	12	6	13	6	13	.		:					:					:				
14	14	.	14	.	14	.	.	.	14	.	11	.	13	.	:					:					:				
15	6	15	.	6	.	.	6	6	.	.	7	.	6	12	.					:					:				
16	6	.	6	.	6	.	6	.	6	.	14	.	10	.	11	.				:					:				
17	8	17	8	17	8	17	8	8	8	17	8	17	8	17	8	14	.			:					:				
18	16	.	.	.	14	.	16	.	.	.	16	.	17	.	.	.	17	.		:					:				
19	9	19	9	19	9	19	9	18	9	19	9	19	9	19	9	18	9	19	.	:					:				
20	15	.	15	.	.	.	7	.	11	.	15	.	13	.	.	.	17	.	19	.					:				
21	9	21	.	9	9	.	.	9	.	18	10	.	10	.	.	9	8	.	9	9	.				:				
22	22	.	22	.	22	.	20	.	22	.	.	.	22	.	22	.	17	.	19	.	21	.			:				
23	11	23	11	23	11	23	11	21	11	23	11	23	11	23	11	11	11	23	11	23	11	23	.		:				
24	12	.	.	.	12	.	12	.	.	.	10	.	12	.	.	.	16	.	18	.	.	.	22	.	:				
25	12	24	12	24	.	24	12	24	12	.	11	12	12	24	.	22	12	24	12	.	9	22	11	24	.				
26	26	.	26	.	24	.	26	.	26	.	26	.	.	.	26	.	26	.	26	.	20	.	23	.	24	.				
27	13	26	.	13	11	.	13	13	.	26	13	.	13	26	.	11	13	.	13	13	.	22	11	.	11	26	.			
28	21	.	21	.	21	.	.	.	17	.	21	.	17	.	21	.	21	.	19	.	.	.	23	.	21	.	13	.		
29	14	29	14	29	14	29	14	14	14	29	14	29	14	29	14	26	14	29	14	29	14	29	14	26	14	29	14	29	.
30	30	.	.	.	.	.	30	.	.	.	30	.	30	.	.	.	30	.	30	.	.	.	23	.	.	.	.	.	29	

Table 1. Minimal values of x_0 in (4.4) for relatively prime $a \geqslant c \geqslant 1$.

The smallest possible values of x_0 for some values $a \geqslant c > 0$ are given in Table 1. Only the values for relatively prime a, c are given (because of reason explained above). We can see that the last part of Lemma 4.3 often, but not always, gives the optimal values of x_0.

LEMMA 4.4. *Let $a > c$ be relatively prime positive integers. Then*

(i) *The set of (a,c)-square-additive functions forms a finitely dimensional vector space over $\mathbb{R}$.*

(ii) *Every (a,c)-square-additive function F satisfies the linear recurrence*

$$F(x+2a) = \tfrac{a}{c} \cdot F(x+a+c) - \tfrac{a}{c} \cdot F(x+a-c) + F(x).$$

(iii) *The functions* $F_0(x) = x^2$ *and* $F_1(x) = 1$ *are* (a, c)*-square-additive.*
(iv) *If, moreover,* $ac \equiv 2 \pmod 4$ *then the function* $F_2(x) = x^2 \operatorname{MOD} 2$ *is* (a, c)*-square-additive, too.*

PROOF. (i) is a consequence of Lemma 4.3. The number x_0+1 is the upper bound for the dimension because every (a, c)-square-additive functions F is uniquely determined by its values for $x \leqslant x_0$. (The estimation of dimension is very rough; it will be diminished below.)

(ii) We can substitute $r = 2$, $s = x$ into (4.3) and then perform an elementary manipulation. (Often there are further linear recurrences for (a, c)-square-additive functions.)

(iii) is almost obvious.

(iv) The condition means that one of a, c is odd and the other is even. Four possible values of $(ax^2 + cy^2) \operatorname{MOD} 4$ correspond to the four possible combinations of the parities of x, y. If we know $ax^2 + cy^2$ then we can uniquely determine these parities, and then also $a \cdot F_2(x) + c \cdot F_2(y)$. □

THEOREM 4.5. *Let* $0 < c < a < 20$ *and let* a, c *be relatively prime. Then:*

(i) *If* $ac \equiv 2 \pmod 4$ *then a function* $F : \mathbb{N} \to \mathbb{R}$ *is* (a, c)*-square additive if and only if* F *is a linear combination of the functions*

$$F_0(x) = x^2, \quad F_1(x) = 1, \quad \text{and} \quad F_2(x) = x^2 \operatorname{MOD} 2.$$

(ii) *If* $ac \not\equiv 2 \pmod 4$ *then a function* $F : \mathbb{N} \to \mathbb{R}$ *is* (a, c)*-square additive if and only if* F *is a linear combination of the functions* F_0 *and* F_1.

PROOF. The assertions were proved by computer computation. Any (a, c)-square additive function F is uniquely by its values

$$F(0),\ F(1), \ldots,\ F(x_0); \tag{4.5}$$

where x_0 is the constant from Lemma 4.3. Further values can be determined by suitable application of (4.1). However, the values (4.5) cannot be chosen arbitrarily. Let us consider (4.5) as indeterminates. For $x > x_0$ we can express $F(x)$ as a linear combination of (4.5) (by repeated application of (4.1)). If we obtain two different expressions for the same $F(x)$ then we can use them to construct a linear equation for (4.5). Of course, it may happen that an equation dependent on the previously constructed ones is obtained. But

every substantially new equation diminish the number k of independent members of (4.5). The computation can be finished when $k = 3$ (in the case (i)) or $k = 2$ (in the case (ii)). In all considered these values were reached. □

PROBLEM 4.6. *Does Theorem 4.5 hold for all relatively prime positive integers a, c (i.e., without the upper bound 20)?*

5. Pythagorean-additive functions

DEFINITION 5.1. A function $F : \mathbb{N} \to \mathbb{R}$ will be called Pythagorean-additive (shortly: P-additive) if for all $x, y, z \in \mathbb{N}$

$$x^2 = y^2 + z^2 \implies F(x) = F(y) + F(z). \tag{5.1}$$

As for the notions above, the set of P-additive functions forms a vector space over $\mathbb{R}$. We can see that a square-additive function F is P-additive if and only if $F(0) = 0$. Hence the functions F_0, F_2, F_3, F_4, and $F_5 - F_1$ are P-additive (and linearly independent); the functions F_1, F_5 are not.

LEMMA 5.2. *Let F be a periodical P-additive function with the period m. Then:*

(i) *For all $x \leqslant m$ we have $F(m - x) = F(x)$.*
(ii) *$F(0) = 0$ and if $8|m$ then $F(\frac{m}{2}) = 0$.*
(iii) *If $m > 1$ is a product of primes of the form $4k + 1$ then the set $\{1, 2, \ldots, \frac{m-1}{2}\}$ can be partitioned into $\frac{m-1}{4}$ two-element sets $\{y_i, z_i\}$ such that $F(y_i) + F(z_i) = 0$ for all $i = 1, \ldots, \frac{m-1}{4}$.*
(iv) *If $m > 1$ is a power of a prime greater than 3 then $\sum_{x=0}^{m-1} F(x) = 0$.*

PROOF. For (i) we can apply (5.1) to the equality

$$(mx + x)^2 = (mx - x)^2 + (2mx)^2.$$

Then for (ii) we can use the equalities

$$0^2 = 0^2 + 0^2 \quad \text{and} \quad \left(\frac{3m}{8}\right)^2 + \left(\frac{m}{2}\right)^2 = \left(\frac{5m}{8}\right)^2.$$

(Notice that $F(0) = 0$ is proved without the assumption of periodicity.)

To prove (iii) we shall use the fact that there are relatively prime integers s, t such that $s^2 + t^2 = m^2$. From now on we shall work with arithmetic modulo m (we shall use $\equiv$ but we shall omit $\pmod m$). Let $r \equiv st^{-1}$; such

r is defined, ant it holds $r^2 \equiv -1$ because $s^2 + t^2 \equiv 0$. We shall also consider F as defined on the residue classes modulo m. Now let $M = \{1, 2, \ldots, \frac{m-1}{2}\}$. We shall define a mapping $\alpha : M \to M$ by $\alpha(x) \equiv \pm rx$; the sign is uniquely determined by the condition $\alpha(x) \in M$.

For every $x \in M$ we have $\alpha(x) \neq x$. Indeed, otherwise we have $rx \equiv \pm x$, $sx \equiv \pm tx$, and hence $s \equiv \pm t \pmod{p}$ and $s^2 \equiv t^2 \pmod{p}$ for a prime divisor p of m. Since also $s^2 + t^2 \equiv 0 \pmod{p}$ (and $p > 2$) we have $p|r$, $p|s$, which is a contradiction. Further, for every $x \in M$ we have

$$\alpha(\alpha(x)) = \pm(r \cdot (\pm rx)) = \pm r^2 x = \pm x = x,$$

where the signs are always chosen so that elements of M are obtained. Hence the orbits of α are two-elements subsets of M. The set $\{y_i, z_i\}$ will be these orbits, i.e., the set of the form $\{x, \alpha(x)\}$, $x \in M$.

It remains to prove $F(x) + F(\alpha(x)) = 0$. Now let $y \equiv s^{-1}$ be fixed. We have $(xsy)^2 + (xty)^2 = (xmy)^2$, and hence $F(xsy) + F(xty) = 0$. However,

$$x \equiv xsy \quad \text{and} \quad \alpha(x) \equiv \pm xr \equiv \pm xty.$$

Therefore by periodicity of F and the property (1) from Lemma 5.2 we have

$$F(x) + F(\alpha(x)) = F(xsy) + F(xty) = 0.$$

Now we shall prove (iv). If m is not a power of 5 we shall use that $(3x)^2 + (4x)^2 = (5x)^2$ and hence

$$\sum_{x=0}^{m-1} F(3x) + \sum_{x=0}^{m-1} F(4x) = \sum_{x=0}^{m-1} F(5x).$$

The integer m is relatively prime with 3, 4, and 5. Therefore all three sums and the sum in the lemma contain the same summands (in different orders), and hence they are equal. Then they must be equal to 0.

If m is a power of 5 a Pythagorean triple (u, v, m) with u, v relatively prime to 5 can be similarly used instead of $(3, 4, 5)$ (the integers u, v can be obtained from a suitable power of $3 + 4i$). However, we can also apply (iii). □

THEOREM 5.3. *There are at least 17 linearly independent P-additive functions.*

PROOF. The list of functions can consist of

(1) Fourteen periodical functions: four with the period $2^4 = 16$, three with the period $3^2 = 9$, five with the period $5^2 = 25$, and two with the period 13.
(2) Two functions with the unique nonzero value (at 1 and at 2).
(3) The function $F_0(x) = x^2$.

They are presented in Table 2; for the periodical function the repeated part is always written only once. The periodical functions were found by computer computation, (We could find another system in which some periods would be smaller.) The computation was simplified and accelerated by using the properties from Lemma 5.2, and also by a result of A. Schinzel [Sch]. Notice that there are no further linearly independent P-additive functions with periods up to 100.

n	p	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	16	0	1	0	0	0	0	0	1	0	1	0	0	0	0	0	1									
2	16	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0									
3	16	0	0	0	1	0	1	0	0	0	0	0	1	0	1	0	0									
4	16	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0									
5	9	0	1	0	0	0	0	0	0	1																
6	9	0	0	1	0	0	0	0	1	0																
7	9	0	0	0	0	1	1	0	0	0																
8	25	0	1	0	0	0	0	0	-1	0	0	0	0	0	0	0	0	0	0	-1	0	0	0	0	0	1
9	25	0	0	1	0	0	0	0	0	0	0	0	-1	0	0	-1	0	0	0	0	0	0	0	0	1	0
10	25	0	0	0	1	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	1	0	0
11	25	0	0	0	0	0	0	1	0	-1	0	0	0	0	0	0	0	0	-1	0	1	0	0	0	0	0
12	25	0	0	0	0	0	0	0	0	0	1	0	0	-1	-1	0	0	1	0	0	0	0	0	0	0	0
13	13	0	1	0	0	-1	-1	1	1	-1	-1	0	0	1												
14	13	0	0	1	-1	1	0	-1	-1	0	1	-1	1	0												
15	-	0	1	0	0	0	0	0	0	0	0	...														
16	-	0	0	1	0	0	0	0	0	0	0	...														
17	-	0	1	4	9	16	25	36	49	64	81	...														

Table 2. Linearly independent P-additive functions.

The statement about F_0 is almost obvious. The last item follows from the fact that no Pythagorean triangle with side 1 or 2 exists. Hence the values at these points can be chosen arbitrarily.

It remains to prove that the presented 17 functions are linearly independent. A simple way is to compute the rank of the 17×25 matrix consisting of the values of these functions for $x = 0, 1, \ldots 24$. It also suffices to consider

its minor corresponding to

$$x \in \{1,2,3,4,6,7,8,9,11,12,14,15,16,17,18,21,23\}.$$

Some computation can be avoided if we pay attention to the rate of growth, the periods, and the mean values. (E.g., if we form the sums of 13 consecutive values then the functions with the period 13 vanish.) Then we can divide the whole set of functions into several subsets which can be further considered separately. □

From the above functions we can construct P-additive functions with periods m for all $m > 1$, $m|39600 = 16 \cdot 9 \cdot 25 \cdot 13$. It is not clear whether all P-additive functions satisfy any linear recurrence. However, the above presented functions satisfy the linear recurrence whose characteristic polynomial is the least common multiple of

$$\chi^{16} - 1, \quad \chi^9 - 1, \quad \chi^{25} - 1, \quad \chi^{13} - 1, \quad \chi^3, \quad (\chi - 1)^3.$$

Now we shall find a necessary condition for the periods of periodic P-additive functions. We shall need the following two lemmas for that. For the first one remember that a *circulant matrix* is a square matrix in which the next row is always obtained from the previous one by the cyclic shift one element to the right.

LEMMA 5.4. *The determinant of the circulant $n \times n$ matrix with the first row $(a_0, a_1, \ldots, a_{n-1})$ is equal to*

$$\prod_{j=0}^{n-1} \left(a_0 + a_1\xi^j + a_2\xi^{2j} + \cdots + a_{n-1}\xi^{(n-1)j}\right), \tag{5.2}$$

where

$$\xi = \cos\frac{2\pi}{n} + \mathrm{i}\sin\frac{2\pi}{n}. \tag{5.3}$$

The proof can be found in [Dav].

LEMMA 5.5. *If A, B, C are complex numbers of absolute value 1, then one has $A + B = C$ if and only if the ratios A/C and B/C are distinct primitive sixth roots of unity.*

PROOF. Trivial. □

THEOREM 5.6. *Let $m > 5$ be a prime and let there exist a (non-constant) periodical P-additive function with the period m. Then*

(i) *It holds $m \equiv 1 \pmod 6$.*

(ii) *For every triple of positive integers p, q, s such that m does not divide pqs and $p^2 + q^2 = s^2$ there is $j \in \{1, 2, \ldots, m-1\}$ such that $p^j \not\equiv q^j \pmod m$ and*

$$(pq)^j \equiv s^{2j} \pmod m, \qquad p^{3j} + s^{3j} \equiv 0 \pmod m. \tag{5.4}$$

(iii) *Under the assumptions of* (ii), *the elements ps^{-1} and qs^{-1} have orders divisible by 6 in the multiplicative group modulo m.*

PROOF. Notice that p, q, r do not explicitely occur in the statement (i). Nevertheless, they are used in the proof of (i); we obviously may choose, e.g., $(p, q, r) = (3, 4, 5)$ if necessary.

Let F be a function with the mentioned properties. We shall construct a system of $m-1$ homogeneous linear equations for the values $F(x)$, $x = 1, 2, \ldots m-1$, and we shall consider its matrix M. Since this system has a nontrivial solution the determinant of M must be zero; this fact will be used to prove (i)–(iii).

Let r be the least primitive root modulo m. The columns of M will correspond to the values r^j, $j = 0, 1, \ldots, m-2$ and the rows of M will correspond to the triples (pr^k, qr^k, sr^k), where $j, k \in \{0, 1, \ldots, m-2\}$. By (5.1) and periodicity of F we have

$$F(pr^k \operatorname{MOD} m) + F(qr^k \operatorname{MOD} m) = F(sr^k \operatorname{MOD} m).$$

This equation will be used to construct the k-th row of M (the enumeration starts with 0). Two elements of the row will be 1, one will be equal to -1 and the other elements will be 0. Notice that the matrix M is circulant. (An example for $m = 13$ and $(p, q, s) = (3, 4, 5)$ is given in Table 3. The condition (ii) is fulfilled for $j = 2$ and $j = 10$.)

We shall apply Lemma 5.4 (with $n = m-1$) to the matrix M. If

$$p \equiv r^u \pmod m, \qquad q \equiv r^v \pmod m, \qquad s \equiv r^w \pmod m,$$

then we have $a_u = a_v = 1$, $a_w = -1$ and $a_k = 0$ for $k \notin \{u, v, w\}$. Therefore

$$|M| = \prod_{j=1}^{n-1} \left(\xi^{uj} + \xi^{vj} - \xi^{wj}\right).$$

$r^e \equiv$	1	2	4	8	3	6	12	11	9	5	10	7
$2^0 \equiv 1$	0	0	1	0	1	0	0	0	0	−1	0	0
$2^1 \equiv 2$	0	0	0	1	0	1	0	0	0	0	−1	0
$2^2 \equiv 4$	0	0	0	0	1	0	1	0	0	0	0	−1
$2^3 \equiv 8$	−1	0	0	0	0	1	0	1	0	0	0	0
$2^4 \equiv 3$	0	−1	0	0	0	0	1	0	1	0	0	0
$2^5 \equiv 6$	0	0	−1	0	0	0	0	1	0	1	0	0
$2^6 \equiv 12$	0	0	0	−1	0	0	0	0	1	0	1	0
$2^7 \equiv 11$	0	0	0	0	−1	0	0	0	0	1	0	1
$2^8 \equiv 9$	1	0	0	0	0	−1	0	0	0	0	1	0
$2^9 \equiv 5$	0	1	0	0	0	0	−1	0	0	0	0	1
$2^{10} \equiv 10$	1	0	1	0	0	0	0	−1	0	0	0	0
$2^{11} \equiv 7$	0	1	0	1	0	0	0	0	−1	0	0	0

Table 3. The matrix M for $m = 13$ and $(p, q, s) = (3, 4, 5)$

Hence $|M| = 0$ if for some j it holds $\xi^{uj} + \xi^{vj} - \xi^{wj} = 0$; let us consider such j. Lemma 5.4 implies now

$$\xi^{uj} \neq \xi^{vj}, \quad \xi^{uj}\xi^{vj} = \xi^{2wj} \quad \text{and} \quad \xi^{3uj} = (-1) \cdot \xi^{3wj}.$$

However, the multiplicative group of nonzero residue classes modulo m is isomorphic with the multiplicative group of complex n-th roots of 1. By this isomorphism r corresponds to ξ, and hence ξ^u, ξ^v, ξ^w correspond to (the residue classes modulo m represented by) p, q, s, respectively. (Moreover the complex number -1 correspond to the residue class contining -1.) So we obtain $p^j \not\equiv q^j \pmod m$ and (5.4).

The second congruence of (5.4) implies $(ps^{-1})^{3j} \equiv -1$ (as before, all congruences are taken mod m) and therefore $(ps^{-1})^{6j} \equiv 1$. To prove (iii) we must show $(ps^{-1})^{2j} \not\equiv 1$. (We need not consider the element qs^{-1} because of symmetry of the assumptions.) If $(ps^{-1})^{2j} \equiv 1$ then $p^{2j} \equiv s^{2j}$, and by the first congruence (5.4) $p^j \equiv q^j$, what is a cotradiction.

For (i) we can use that if $m \not\equiv 1 \pmod 6$ then the multiplicative group modulo m contains no elements of order 6. □

PROBLEM 5.7. *Are there infinitely many linearly independent P-additive functions $F : \mathbb{N} \to \mathbb{R}$?*

It would be true, e.g., if the answer to the following problem is "infinitely many":

PROBLEM 5.8. *Determine the number of connected components of the graph G whose vertices are odd positive integers and every two distinct*

vertices x, y are connected by an edge if and only if $|x^2 - y^2|$ is a square.

The graph G has at least three components because the vertex 1 is isolated and 3, 7 belong to distinct components. It may happen that every path between two relatively small odd integers contains rather large members. For example, consider the path

$$47,\ 1105,\ 169,\ 65,\ 25,\ 7.$$

The number 1105 cannot be avoided in any path connecting 47 and 7. (Notice that the answer "finitely many", or even the answer "3", does not immediately imply negative answer to Problem 5.7.)

References

[Dav] P. J. Davis, *Circulant matrices*, J. Wiley, New York (1979).

[Kor] I. Korec, *Definability of arithmetical operations from binary quadratic forms*, Preprint 5/1998 of Math. Institute SAV Bratislava, 10.

[Sch] A. Schinzel, *On Pythagorean triangles*, Ann. Math. Silesianae **12** (1998), 31.

Mathematical Institute
Slovak Academy of Sciences
Štefánikova 49
SK–814 73 Bratislava
Slovakia