A SET OF UNIQUENESS FOR COMPLETELY ADDITIVE ARITHMETIC FUNCTIONS

J. Fehér (Pécs, Hungary)
K.-H. Indlekofer (Paderborn, Germany)
N.M. Timofeev (Vladimir, Russia)

Dedicated to Prof. Árpád Varecza on his 60th birthday

Abstract. By definition, the set $A \subset \mathbb{N}$ is called a set of *uniqueness* (mod 1) if the implication $f(A) \subset \mathbb{Z} \Rightarrow f(\mathbb{N}) \subset \mathbb{Z}$ holds for all completely additive functions $f : \mathbb{N} \to \mathbb{R}$. The paper is dealing with the question whether the sets of forms $A := \{x^2 + hy^2 + a : x, y \in \mathbb{N}\}$ are sets of *uniqueness* (mod 1), where h, a are positive integers.

1. Introduction

The function $f : \mathbb{N} \to \mathbb{R}$ is completely additive if

$$f(nm) = f(n) + f(m) \quad (\forall n, m \in \mathbb{N}).$$

Let us denote by $\mathcal{A}_{\mathbb{R}}$ the set of completely additive functions.

The set $A = \{a_1, a_2, \ldots\} \subset \mathbb{N}$ is a set of *uniqueness*, if

$$f(A) = \{0\} \Rightarrow f = 0 \quad (\forall f \in \mathcal{A}_{\mathbb{R}}),$$

and A is called a set of *uniqueness* (mod 1) (see [5]), if

$$f(A) \subset \mathbb{Z} \Rightarrow f(\mathbb{N}) \subset \mathbb{Z} \quad (\forall f \in \mathcal{A}_{\mathbb{R}}).$$

Some famous examples of sets of *uniqueness*:

(a) $A = \{p+1 \mid p \text{ prime}\}$ ([1], [5]),

(b) $A = \{x^2+y^2 \mid x,y \in \mathbb{N}\}$ ([6]).

Elliot [1], Indlekofer [3], Kátai [6] showed examples of sets of *uniqueness* (mod 1) as well. Wolke [7] and, with a different proof, Indlekofer ([4], Theorem 1) showed that for a set of A *uniqueness* every $n \in \mathbb{N}$ must be expressible as a finite product of rational powers of elements of A. Indlekofer ([4], Theorem 2) and Hoffmann [2] proved that the sets A of *uniqueness* (mod 1) can be characterized by the property that every $n \in \mathbb{N}$ can be expressed as a finite product of integer powers of elements of A. In this paper we show some more examples of sets of *uniqueness* (mod 1).

For any set $A = \{a_1, \ldots\} \subset \mathbb{N}$ denote

$$\langle A \rangle := \left\{ \prod_{i=1}^{s} a_i^{e_i} : e_i \in \mathbb{Z},\ s \geq 1 \right\}.$$

It is clear that A is a set of *uniqueness* (mod 1) if and only if $\langle A \rangle = \mathbb{Q}_+$.

For a fixed $A \in \mathbb{N}_0$ denote

$$E_A := \{x^2+y^2+A : x,y \in \mathbb{N}\},$$
$$E_0^* := \{x^2+y^2 > 0 : x,y \in \mathbb{N}_0\},$$
$$F_A := \{x^2+2y^2+A : x,y \in \mathbb{N}\},$$
$$F_0^* := \{x^2+2y^2 > 0 : x,y \in \mathbb{N}_0\}.$$

We prove the theorems as follows.

Theorem 1.1. *If $A \in E_0^*$, then E_A is a set of uniqueness* (mod 1).

Theorem 1.2. *If $A \in F_0^*$, then F_A is a set of uniqueness* (mod 1).

Theorem 1.3. *If $A \in \mathbb{N}$, then $\{n = 2^\alpha \prod p_i^{\alpha_i} : \alpha \geq 0, p_i \equiv 1 \pmod 4\} \subset \subset \langle E_A \rangle$.*

Theorem 1.4. *If $A = MT$, $M \in F_0^*$, $T \equiv -1 \pmod 4$, then $\{n = = \prod q_i^{\alpha_i} : q_i \equiv 1, 3 \pmod 8$ prime $\} \subset \langle F_A \rangle$.*

2. Lemmas

Lemma 2.1. *Let $c \in \mathbb{N}$ and let $q > 5$ be prime where $q \not| c$. Further, let the Dirichlet character $\chi \pmod q$ defined by $\chi(a) = \left(\frac{a}{q}\right)$ $(q \not| a)$, where $\left(\frac{a}{q}\right)$*

denotes the Legendre symbol. Then, for all pairs $(i,j)\in\{-1,1\}\times\{-1,1\}$ *there exists* $a\in\mathbb{N}$ *with* $q\nmid a$ *such that*

$$(\chi(a),\chi(a-c))=(i,j). \tag{2.2}$$

Proof. Obviously (2.2) is equivalent to each of the following assertions:
(i) $\exists b\in\mathbb{N}$ such that $(\chi(cb),\chi(cb-c))=(i,j)$,
(ii) $\exists b\in\mathbb{N}$ such that $(\chi(b),\chi(b-1))=(i,j)$.
Put $S(i,j)=|\{b=2,\dots,q-1:\chi(b)=i,\chi(b-1)=j\}|$. Then

$$\begin{aligned} S(i,j)&=\frac{1}{4}\left|\sum_{b=2}^{q-1}(i+\chi(b))(j+\chi(b-1))\right|=\\ &=\frac{1}{4}\left|ij(q-2)-i\chi(-1)-j+\sum_{b=2}^{q-1}\chi(b)\chi(b-1)\right|. \end{aligned} \tag{2.3}$$

Let $\chi(kq):=0$, and $T(h):=\sum_{b=1}^{q-1}\chi(b)\chi(b+h)\quad(\forall h\in\mathbb{Z})$. In this case, if $q\mid h$ then $T(h)=q-1$. Assume that $q\nmid h$ and $ah\equiv b \pmod q$. So we have

$$T(h)=\sum_{a=1}^{q-1}\chi(ah)\chi(ah+h)=\chi^2(h)\sum_{a=1}^{q-1}\chi(a)\chi(a+1)=T(1),$$

$$\sum_{h=0}^{q-1}T(h)=q-1+(q-1)T(1). \tag{2.4}$$

On the other hand

$$\sum_{h=0}^{q-1}T(h)=\sum_{h=0}^{q-1}\sum_{b=1}^{q-1}\chi(b)\chi(b+h)=\sum_{b=1}^{q-1}\chi(b)\sum_{h=0}^{q-1}\chi(b+h)=0,$$

and from (2.4) we deduce that $T(1)=-1$. Using this, (2.3) implies that

$$S(i,j)=\frac{1}{4}\left|ij(q-2)-i(-1)^{\frac{q-1}{2}}-j-1\right|$$

holds for all odd primes q. This shows that

$$S(i,j)\geq\frac{1}{4}(q-5)>0\ \text{ for }\ q>5.$$

This ends the proof of Lemma 2.1.

Lemma 2.5. *Let $q > 5$ be a prime, $A, B, C \in \mathbb{Z}$ and $q \nmid ABC$. Then the congruence*

$$Ax^2 + By^2 + C \equiv 0 \pmod{q} \tag{2.6}$$

has got a nontrivial ($q \nmid xy$) solution.

Proof. By Lemma 2.1. there is $q \nmid \alpha \in \mathbb{Z}$ s.t.

$$\left(\left(\frac{\alpha}{q} \right), \left(\frac{\alpha - C}{q} \right) \right) = \left(\left(\frac{-A}{q} \right), \left(\frac{B}{q} \right) \right).$$

Hence there are $y_0 \in \mathbb{N}$ s.t. $By_0^2 + C \equiv \alpha \pmod{q}$ and $x_0 \in \mathbb{N}$ s.t. $Ax_0^2 + \alpha \equiv 0 \pmod{q}$. The properties $q \nmid \alpha - C$ and $q \nmid \alpha$ imply that x_0, y_0 are a nontrivial solution of (2.6).

Lemma 2.7. *Let $k^2 \neq q \in \mathbb{N}$ and $A = 2^\alpha B \in \mathbb{N}$ with odd $B > 1$. If the Pell equation*

$$x^2 - qy^2 = -1 \tag{2.8}$$

has got a solution, then there are $Q_1, Q_2 \in E_0$ s.t.

$$q(Q_1 + A) = Q_2 + A. \tag{2.9}$$

Proof. (a) Firstly, we show that the statement is true for $\alpha = 0$. There are elements in $\mathbb{Q}(\sqrt{q})$ having norms (-1) and $1 - q$ respectively, which implies that there is an element in $\mathbb{Q}(\sqrt{q})$ s.t. its norm equals $q - 1$. Consequently there are $x_0, u_0 \in \mathbb{N}$ s.t.

$$x_0^2 - qu_0^2 = q - 1.$$

Let $y_0 = v_0 = 1$ and

$$x_1 = x_0 \frac{B+1}{2},\ u_1 = u_0 \frac{B+1}{2},\ y_1 = y_0 \frac{B-1}{2},\ v_1 = v_0 \frac{B-1}{2}.$$

It is easy to check that $Q_1 = u_1^2 + v_1^2$, $Q_2 = x_1^2 + y_1^2 \in E_0$ also solve the equation (2.9).

(b) Let $A = 2^\alpha B$ ($B > 1$ odd) and $Q_1 = u_1^2 + v_1^2$, $Q_2 = x_1^2 + y_1^2$ (as above). Then

$$q(Q_1 2^\alpha + 2^\alpha B) = Q_2 2^\alpha + 2^\alpha B.$$

If $u_1 = v_1$ then $\left(\frac{B+1}{2}, \frac{B-1}{2}\right) = 1$ implies $\frac{B+1}{2}\Big| 1 = v_0$, hence $B = 1$. This implies $Q_1 \neq 2T^2$, $Q_2 \neq 2L^2$, consequently $Q_1 2^\alpha = Q_1'$, $Q_2 2^\alpha = Q_2' \in E_0$ and $q(Q_1' + A) = q(Q_2' + A)$.

Lemma 2.10. *Let* $A = MT$, *where* $M \in F_0^*$, $T \equiv -1 \pmod 4$ *and* $k^2 \neq q \in \mathbb{N}$. *Now, if the equation*

$$x^2 - qy^2 = -2 \tag{2.11}$$

is solvable, then there are $Q_1, Q_2 \in F_0$ *s.t.*

$$q(Q_1 + A) = Q_2 + A. \tag{2.12}$$

Proof. (a) First we show that the statement of the lemma is true when $A \equiv -1 \pmod 4$. (2.11) has a solution, hence there are $y_0, v_0 \in \mathbb{N}$ s.t.

$$y_0^2 - qv_0^2 = -2(1 - q).$$

Let $x_0 = u_0 = 1$ and

$$x_1 = x_0 \frac{A-1}{2},\ u_1 = u_0 \frac{A-1}{2},\ y_1 = y_0 \frac{A+1}{4},\ v_1 = v_0 \frac{A+1}{4}.$$

It is easy to check that $Q_1 = u_1^2 + 2v_1^2$, $Q_2 = x_1^2 + 2y_1^2 \in F_0$ also solve the equation (2.12).

(b) Let $A = MT$, $M \in F_0^*, T \equiv -1 \pmod 4$. Then (2.12) true with $A := T$, i.e. $q(Q_1 + T) = Q_2 + T$. Multiplying by M we get $q(Q_1 M + TM) = Q_2 M + TM$. After that, denoting $Q_1' := Q_1 M$, $Q_2' := Q_2 M \in F_0$, we get

$$q(Q_1' + A) = Q_2' + A.$$

Remark 2.13. The proof of Lemma 2.10. does not work for some $A - s$, e.g. for $A := 7.23$.

3. Proof of Theorem 1.1

First, let us note that for $\alpha \in E_0^*$ and $\beta \in E_0$ the condition $\alpha\beta \notin E_0$ may hold only in the case $\alpha = 2h^2$, $\beta = 2k^2$.

(a) First we show that $A \in E_0^*$ implies $2, 3, 5, A \in \langle E_A \rangle$.

It is clear that the following implications hold.

$$5A \in E_0 \Rightarrow 6A \in \langle E_A \rangle, \quad 13A \in E_0 \Rightarrow 14A \in \langle E_A \rangle,$$
$$17A \in E_0 \Rightarrow 18A \in \langle E_A \rangle, \quad 20A \in E_0 \Rightarrow 21A \in \langle E_A \rangle,$$
$$34A \in E_0 \Rightarrow 35A \in \langle E_A \rangle.$$

Consequently,

$$2 = (14A)(21A)^{-1}(18A)(6A)^{-1} \in \langle E_A \rangle,$$
$$3 = (18A)(6A)^{-1} \in \langle E_A \rangle, \quad 5 = (35A)(14A)^{-1} \cdot 2 \in \langle E_A \rangle,$$
$$A = (6A)3^{-1} \cdot 2^{-1} \in \langle E_A \rangle.$$

(b) If $q > 5$ is a prime, then there are $x_0, y_0 \in \mathbb{N}$ s.t. $x_0^2 + y_0^2 + 1 = Dq$, $D < q$, $Dq - 1 \neq h^2$. By Lemma 2.2. there are $x_0, y_0 \in \mathbb{N}$, $x_0, y_0 < \frac{q}{2}$ s.t. $x_0^2 + y_0^2 + 1 = qD_0$. Assume that $qD_0 - 1 = 2h^2$. Then $h < \frac{q}{2}$. Put $x_1 := q - h$, $y_1 := h$. For such x_1, y_1 we have $x_1^2 + y_1^2 + 1 = (q-h)^2 + h^2 + 1 = q(q - 2h + D_0) = qD_1$. If $D_1 \geq q$, then $D_0 q \geq 2hq > 4h^2$ that is impossible. So $D_1 < q$ and $qD_1 - 1$ is odd.

(c) Now, let $q > 5$ be prime and assume that $D < q$ implies $D \in \langle E_A \rangle$. Let $x_0, y_0 \in \mathbb{N}$ s.t. $x_0^2 + y_0^2 + 1 = qD$, $D < q$, $Dq - 1 \neq 2h^2$. In this case $(Dq - 1)A \in E_0 \Rightarrow DqA \in \langle E_A \rangle$, hence $q = (DqA)D^{-1}A^{-1} \in \langle E_A \rangle$. This completes the proof of Theorem 1.1.

4. Proof of Theorem 1.2

First, let us note that the conditions $\alpha \in F_0^*$ and $\beta \in F_0$ imply $\alpha\beta \in F_0$.

(a) First we show that F_1 is a set of *uniqueness* (mod 1).

$$5 = (1^2 + 2 \cdot 1^2 + 1)^{-1}(1^2 + 2 \cdot 3^2 + 1) \in \langle F_1 \rangle,$$
$$3 = (3^2 + 2 \cdot 1^2 + 1)(1^2 + 2 \cdot 2^2 + 1)^2(1^2 + 2 \cdot 3^2 + 1)^{-2} \in \langle F_1 \rangle,$$
$$2 = (1^2 + 2 \cdot 2^2 + 1) \cdot 5^{-1} \in \langle F_1 \rangle.$$

Let $q > 5$ be a prime and assume that $D < q$ implies $D \in \langle F_1 \rangle$. By the Lemma 2.2 there are $x_0, y_0 < \frac{q}{2}$ s.t.

$$x_0^2 + 2y_0^2 + 1 = qD \in \langle F_1 \rangle. \tag{4.1}$$

The condition (4.1) implies that $D < \dfrac{q}{4} + 2\dfrac{q}{4} + \dfrac{1}{q} < q$, hence by the assumption $D \in \langle F_1 \rangle$, so $q = (Dq)D^{-1} \in \langle F_A \rangle$.

(b) We show that the condition $A \in F_0^*$ implies $A \in \langle F_A \rangle$.

$$(1^2 + 2 \cdot 1^2)A \in F_0 \Rightarrow 4A \in \langle F_A \rangle,$$
$$(1^2 + 2 \cdot 2^2)A \in F_0 \Rightarrow 10A \in \langle F_A \rangle,$$
$$(1^2 + 2 \cdot 3^2)A \in F_0 \Rightarrow 20A \in \langle F_A \rangle.$$

Consequently,
$$A = (4A)(20A)^{-2}(10A)^2 \in \langle F_A \rangle.$$

(c) Finally, assume $A \in F_0^*$ and $n \in \mathbb{N}$. Because F_1 is a set of *uniqueness* (mod 1), we have

$$n = \prod_{j=1}^{s} (x_j^2 + 2y_j^2 + 1)^{\ell_j} \Rightarrow n \cdot A^{\sum \ell_j} \prod_{j=1}^{s} ((x_j^2 + 2y_j^2)A + A)^{\ell_j} =$$
$$= \prod_{j=1}^{s} (X^2 + 2Y^2 + A)^{\ell_j} \in \langle F_A \rangle.$$

Further, $A^{\sum \ell_j} \in \langle F_A \rangle \Rightarrow n = \left(nA^{\sum \ell_j}\right)\left(A^{\sum \ell_j}\right)^{-1} \in \langle F_A \rangle$. This proves the theorem.

5. Proof of Theorem 1.3

Let $A = 2^\alpha B$, B odd.

(a) If $B = 1$ then $A = 2^\alpha \in E_0^*$ and the statement is true by Theorem 1.1.

(b) Assume $A = 2^\alpha B$, $B > 1$ odd. It is enough to prove that if q is prime s.t. either $q = 2$ or $q \equiv 1 \pmod 4$, then $q \in \langle E_A \rangle$. In the case $q = 2$, the Pell equation (2.8) is solvable, hence by Lemma 2.4. we see that there are $Q_1, Q_2 \in E_0$ s.t.

$$2(Q_1 + A) = Q_2 + A \Rightarrow 2 = (Q_2 + A)(Q_1 + A)^{-1} \in \langle E_A \rangle.$$

Let $q \equiv 1 \pmod 4$ and assume that for $q' = 2$, or $q' \equiv 1 \pmod 4$, $q' < q$ we have $q' \in \langle E_A \rangle$. Let $x_0^2 + 1 = qD$, $x_0 < \dfrac{q}{2}$. Then $D < q$ and $p|D \Rightarrow$

either $p = 2$ or $p \equiv 1 \pmod 4$, hence $D \in \langle E_A \rangle$. On the other hand, $qD \neq k^2$ and $x_0^2 - (qD)1^2 = -1$, hence by Lemma 2.7. there are

$$Q_1, Q_2 \in E_0 \text{ s.t. } (qD)(Q_1 + A) = Q_2 + A \Rightarrow$$
$$\Rightarrow qD = (Q_2 + A)(Q_1 + A)^{-1} \in \langle E_A \rangle,$$

and therefore $q = (Dq)D^{-1} \in \langle E_A \rangle$. This proves Theorem 1.3.

6. Proof of Theorem 1.4

It is enough to prove that $q \equiv 1, 3 \pmod 8$ implies $q \in \langle F_A \rangle$. For $q = 3$ the equation (2.11) is solvable, so by Lemma 2.10 there are $Q_1, Q_2 \in F_0$ s.t. $3(Q_1 + A) = Q_2 + A \Rightarrow 3 \in \langle F_A \rangle$. Let $q > 3$, prime $q \equiv 1, 3 \pmod 8$ and assume $q' < q, q' \equiv 1, 3 \pmod 8$ implies $q' \in \langle F_A \rangle$. The condition $\left(\frac{-2}{q}\right) = 1$ implies that there is $x_0 < \frac{q}{2}$ s.t. $x_0^2 + 2 = qD$. As $D < q$ and $p \mid D$ implies $p \equiv 1, 3 \pmod 8$, we see that $D \in \langle F_A \rangle$. On the other hand, $qD \neq k^2$ and $x_0^2 - (qD)1^2 = -2$, by Lemma 2.10. there are $Q_1, Q_2 \in F_0$ s.t.

$$(qD)(Q_1 + A) = Q_2 + A \Rightarrow (qD) = (Q_2 + A)(Q_1 + A)^{-1} \in \langle F_A \rangle,$$

and therefore $q = (qD)D^{-1} \in \langle F_A \rangle$. This proves the theorem.

7. Remarks, further developments

In this section we show some results that are useful for investigations around structures of $\langle E_A \rangle$ and $\langle F_A \rangle$, respectively, for some of those A-s which are not treated in the previous sections.

Let $H \in \mathbb{N}$ and $A \in \mathbb{N}_0$ and denote

$$H_A := \{x^2 + Hy^2 + A | x, y \in \mathbb{N}\}.$$

Lemma 7.1. *If H is squarefree, $A \notin H_0$ and $H(A - 1) > 1$, then $A \in$ $\in \langle H_A \rangle$.*

Proof. Put $A = 1+T$. Then necessarily $T \neq Ha^2$, because in the contrary case $A = 1^2+Ha^2 \in H_0$. As H is squarefree, $HT \neq b^2$, hence the Pell equation

$$(HT)u^2 + 1 = v^2$$

has a nontrivial solution $u_0, v_0 \in \mathbb{N}$. For these u_0, v_0 we have $Hu_0^2A + 1 = = Hu_0^2 + HTu_0^2 + 1 = Hu_0^2 + v_0^2 \in H_0 \Rightarrow (Hu_0^2+1)A+1 \in \langle H_A \rangle$. On the other hand,

$$Hu_0^2 + 1^2 \in H_0 \Rightarrow (Hu_0^2+1)A^2 \in H_0 \Rightarrow (Hu_0^2+1)A^2 + A \in \langle H_A \rangle,$$

hence

$$A = ((Hu_0^2+1)A^2 + A)((Hu_0^2+1)A+1)^{-1} \in \langle H_A \rangle.$$

Denote by $P(A)$ the set of prime divisors of A.

Lemma 7.2. *If $P(A) \subset \langle E_A \rangle$ and for primes $q \leq \max\{5, \sqrt{2A}\}$ we have $q \in \langle E_A \rangle$, then E_A is a set of uniqueness* (mod 1).

Proof. Let q be a prime s.t. $P(A) \not\ni q > \max\{5, \sqrt{2A}\}$ and assume that $p < q$ implies $p \in \langle E_A \rangle$. By Lemma 2.2 there are $x_0, y_0 \in \mathbb{N}$ s.t. $x_0^2 + y_0^2 + +A = qD$, $x_0, y_0 < \frac{q}{2}$. If $D \geq q$, then $\frac{q^2}{2} + A \geq q^2 \Rightarrow q \leq \sqrt{2A}$, that is impossible, hence $D < q \Rightarrow D \in \langle E_A \rangle$. On the other hand, $qD \in E_A$, hence $q = (qD)D^{-1} \in \langle E_A \rangle$.

The following lemma can be proved analogously.

Lemma 7.3. *If $P(A) \subset \langle F_A \rangle$ and for primes $q \leq \max\{5, 2\sqrt{A}\}$ we have $q \in \langle F_A \rangle$, then F_A is a set of uniqueness* (mod 1).

Remark 7.4. *An example of a set of uniqueness* (mod 1) *which does not follows from Theorem 1.1, but from Theorem 1.3 and the Lemmas of this sections is: E_{371}.*

Proof. $371 = 7 \cdot 53$. This implies that $7 \cdot 53 \in \langle E_{371} \rangle$ (see Lemma 7.1). But $53 \in \langle E_{371} \rangle$ (see Theorem 1.3), hence $7 = 371 \cdot 53^{-1} \in \langle E_{371} \rangle$. After that (taking into occount Lemma 7.2 and Theorem 1.3) it is enough to show, that $q = 3, 11, 19, 23 \in \langle E_{371} \rangle$.

$$3(5+371) = 754 + 371, \qquad 5, 754 \in E_0 \Rightarrow 3 \in \langle E_{371} \rangle,$$

$$11(13+371) = 3853 + 371, \qquad 13, 3853 \in E_0 \Rightarrow 11 \in \langle E_{371} \rangle,$$

$$19(5+371) = 6773 + 371, \qquad 5, 6773 \in E_0 \Rightarrow 19 \in \langle E_{371} \rangle,$$

$$23(2+371) = 8208 + 371, \qquad 2, 8208 \in E_0 \Rightarrow 23 \in \langle E_{371} \rangle.$$

Above we have utilized several times the following simple fact: if there are $Q_1, Q_2 \in H_0$ s.t. $Q_1 + A = q(Q_2 + A)$, then $q = (Q_1 + A)(Q_2 + A)^{-1} \in \langle H_A \rangle$.

The following lemma is quite useful for our "experimental" computations.

Lemma 7.5. *If there are $Q_1, Q_2 \in H_0$ s.t. $Q_1 + A = qQ_2$, then there are $Q_1', Q_2' \in H_0$ s.t. $Q_1' + A = q(Q_2' + A)$.*

Proof. Let $x^2 + Hy^2 + A = q(u^2 + Hv^2)$. This shows $-A = x^2 - qu^2 + H(y^2 - qv^2)$. Multiplying by $(1 - q)$, we have $A(q-1) = (x^2 - qu^2)(1^2 - q1^2) + H(y^2 - qv^2)(1^2 - q1^2) = X^2 - qU^2 + H(Y^2 - qV^2)$. From this we have $X^2 + HY^2 + A = q(U^2 + HV^2 + A)$.

Remark 7.6. *The set F_{161} is a set of uniqueness* (mod 1).

Proof. $161 = 7 \cdot 23 \notin F_0$. The Lemma 7.3. shows that it is enough to show that for primes $q \le 23$ we have $q \in \langle F_{161} \rangle$.

$$3^2 + 2 \cdot 2^2 + 161 = 2 \cdot 89, \quad 89 \in F_0 \Rightarrow 2 \in \langle F_{161} \rangle,$$
$$1^2 + 2 \cdot 3^2 + 161 = 5 \cdot 36, \quad 36 \in F_0 \Rightarrow 5 \in \langle F_{161} \rangle,$$
$$5^2 + 2 \cdot 3^2 + 161 = 3 \cdot 68, \quad 68 \in F_0 \Rightarrow 3 \in \langle F_{161} \rangle,$$
$$4^2 + 2 \cdot 3^2 + 161 = 13 \cdot 5 \cdot 3 \in \langle F_{161} \rangle \Rightarrow 13 = (13 \cdot 5 \cdot 3)5^{-1}3^{-1} \in \langle F_{161} \rangle,$$
$$6^2 + 2 \cdot 5^2 + 161 = 19 \cdot 13 \in \langle F_{161} \rangle \Rightarrow 19 = (19 \cdot 13)13^{-1} \in \langle F_{161} \rangle,$$
$$4^2 + 2 \cdot 4^2 + 161 = 11 \cdot 19 \in \langle F_{161} \rangle \Rightarrow 11 = (11 \cdot 19) \cdot 19^{-1} \in \langle F_{161} \rangle,$$
$$5^2 + 2 \cdot 3^2 + 161 = 17 \cdot 12, \quad 12 \in F_0 \Rightarrow 17 \in \langle F_{161} \rangle.$$
$$7^2 + 2 \cdot 7^2 + 161 = 7 \cdot 4 \cdot 11 \in \langle F_{161} \rangle \Rightarrow 7 = (7 \cdot 4 \cdot 11) \cdot 2^{-2} \cdot 11^{-1} \in \langle F_{161} \rangle.$$

Finally $161 = 7 \cdot 23 \in \langle F_{161} \rangle$ (by Lemma 7.1) $\Rightarrow 23 = 161 \cdot 7^{-1} \in \langle F_{161} \rangle$, and by Lemma 7.3 the F_{161} is a set of *uniqueness* (mod 1).

Finally, let us mention, that our concrete examples above suggest the following.

Conjecture 7.7. *Let $H \in \mathbb{N}$ squarefree, $A \in \mathbb{N}$, $q \not| AH$ and $\left(\frac{H}{q}\right) = -1$ prime. Then the following three relations are true*

(a) $H_0 + A \cap q(H_0 + A) \ne \emptyset$,

(b) $H_0 + A \cap q \cdot H_0 \ne \emptyset$,

(c) $H_0 - A \cap q \cdot H_0 \ne \emptyset$.

Remark 7.8. By Lemma 7.5 (b) implies (a). It is easy to see that if (c) is true, then the condition $A_1 := Aq$ implies (b).

References

[1] **Elliot P.D.T.A.,** A conjecture of Kátai, *Acta Arith.,* **26** (1974), 11-20.

[2] **Hoffmann P.,** Note on a problem of Kátai, *Acta Math. Hung.,* **45** (1985), 261-262.

[3] **Indlekofer K.-H.,** On sets characterizing additive aritmetical functions, *Math. Z.,* **146** (1976), 285-290.

[4] **Indlekofer K.-H.,** On sets characterizing additive and multiplicative arithmetical functions, *Ill. J. Math.,* **25** (1981), 251-257.

[5] **Kátai I.,** On sets characterizing number-theoretical functions, *Acta Arith.,* **13** (1968), 315-320.

[6] **Kátai I.,** On sets characterizing number-theoretical functions II., *Acta Arith.,* **16** (1968), 1-4.

[7] **Wolke D.,** Bemerkungen ber Eindeutigkeitsmengen additiver Funktionen, *Elem. Math.,* **33** (1978), 14-16.

(Received April 6, 2001)

J. Fehér
Dept. of Mathematics
Janus Pannonius University
Ifjúság u. 6
H-7624 Pécs, Hungary

K.-H. Indlekofer
Fachbereich Math.-Inf.
Universität Paderborn
Warburger Str. 100
D-33100 Paderborn, Germany

N.M. Timofeev
Vladimir State Ped. Univ.
pr. Stroitelei 11
600024 Vladimir, Russia