Annales Univ. Sci. Budapest., Sect. Comp. 27 (2007) 57-63

SOME REMARKS ON SETS OF UNIQUENESS FOR ADDITIVE AND MULTIPLICATIVE FUNCTIONS

J. Fehér (Pécs, Hungary)
I. Kátai (Budapest, Hungary)

Dedicated to the memory of Professor M.V. Subbarao

Abstract. The multiplicative group generated by $\{\varphi(n) \mid n \in \mathbb{N}\}$ is investigated, where φ is a quadratic polynomial.

1. This paper is a continuation of our paper [1]. Let Q_x be the multiplicative group of positive rationals. If A is a subset in Q_x, then let $\langle A\rangle$ be the smallest subgroup of Q_x which contains the elements of A, i.e. $\langle A\rangle$ is the set of the elements $\alpha = a_1^{\varepsilon_1}\dots a_r^{\varepsilon_r}$, where a_j run over the elements of A, and $\varepsilon_1, \varepsilon_2, \dots \varepsilon_r \in \{-1, 1\}$.

Let $\mathcal{B}$ be a set of positive integers, let us write its elements b_i in growing order: $b_1 < b_2 < \dots$. Let $\mathcal{P}(\mathcal{B})$ be the set of the prime divisors of $\mathcal{B}$, i.e. a prime p belongs to $\mathcal{P}(\mathcal{B})$ if $p|b_j$ holds for at least one j.

The following assertion is clear: $\langle B\rangle$ is a subgroup in $\langle\mathcal{P}(\mathcal{B})\rangle$.

Let $\mathcal{B}$ be the whole set of the primes. For some $p \in \mathcal{P}(\mathcal{B})$ let $\nu(p)$ be the smallest k for which $p \mid b_k$.

Lemma 1. *Assume that $b_{\nu(p)} < p^2$ holds for every $p \in \mathcal{P}(\mathcal{B})$, $p \geq Y$. Then every $r \in \langle\mathcal{P}(\mathcal{B})\rangle$ can be written in the form $r = \rho\cdot\eta$, where $\eta \in \langle\mathcal{B}\rangle$, and*

The research was supported by the Hungarian National Foundation for Scientific Research under grants OTKA T043657 and T46993.

all the prime factors of the nominator and denominator of ρ are less than Y (and they clearly belong to $\mathcal{P}(\mathcal{B})$).

The assertion is quite obvious, it is used several places (see Elliott [2], or [1]).

Let

$$\varphi(x) = ax^2 + bx + c \in \mathbb{Z}[x], \qquad a > 0. \tag{1.1}$$

We can write

$$4a\varphi(x) = (2ax + b)^2 - \mathcal{D}, \qquad \mathcal{D} = b^2 - 4ac.$$

Assume that $\mathcal{D} \neq 0$. Let

$$\Phi := \{\varphi(n) \mid n \in \mathbb{N}\} \setminus \{0\}, \tag{1.2}$$

$$\mathcal{E}_1 := \left\{p \mid p \in \mathcal{P}, \left(\frac{\mathcal{D}}{p}\right) = 1\right\}, \quad \mathcal{E}_2 = \{p \mid p \in \mathcal{P},\ p \mid \mathcal{D}\}. \tag{1.3}$$

Let $K = \max\{2, a, |\mathcal{D}|\}$.

Theorem 1. *Let $a = 1, 2, 3, 4$. Then $\langle\Phi\rangle$ is a subgroup in $\langle\mathcal{E}_2\rangle \otimes \langle\rho_2\rangle$ and the factor group $\langle\mathcal{E}_1\rangle \otimes \langle\mathcal{E}_2\rangle \mid \langle\Phi\rangle$ is finite.*

Proof. Let $p > K$, $\left(\frac{\mathcal{D}}{p}\right) = 1$. Then the congruence $y^2 \equiv \mathcal{D} \pmod{p}$ is solvable, for its smallest positive solution y_0 we have: $0 < y_0 \leq \dfrac{p-1}{2}$, $y_0 \geq$ $\geq \sqrt{|\mathcal{D}|}$. Among the numbers $y_t = y_0 + tp$ $(t = -a, \dots, a-1)$ there exists such one for which $y_t \equiv b \pmod{2a}$, furthermore

$$-ap + \sqrt{|\mathcal{D}|} \leq y_t \leq (a-1)p + \frac{p-1}{2}.$$

Let n_0 be defined as $n_0 = \dfrac{y_t - b}{2a}$. Let us observe that

$$4apH := 4a\varphi(n_0) = y_t^2 - \mathcal{D} \tag{1.4}$$

(H is an integer defined by (1.4)). Then

$$(0 <)\ 4apH \leq (ap - \sqrt{|\mathcal{D}|})^2 - \mathcal{D} = a^2p^2 - 2a\sqrt{|\mathcal{D}|}p + (|\mathcal{D}| - \mathcal{D}).$$

Since $4a\varphi(n_0)$ is a multiple of p $(> 2|\mathcal{D}|)$, therefore

$$4apH \le a^2p^2 - 2a\sqrt{|\mathcal{D}|}p + (|\mathcal{D}| - \mathcal{D}). \tag{1.5}$$

Hence $0 < H < p$ follows, if $\mathcal{D} > 0$, $\ a = 1, 2, 3, 4$. Let $\mathcal{D} = |\mathcal{D}|$. From (1.5) we get

$$H \le \frac{ap}{4} - \frac{\sqrt{\mathcal{D}}}{2} + \frac{2\mathcal{D}}{4ap}. \tag{1.6}$$

The right hand side of (1.6) is less that p. This is clear, if $a \le 3$. In the case $a = 4$ we use the assumption $p > K$, whence $\dfrac{2\mathcal{D}}{4ap} - \dfrac{\sqrt{\mathcal{D}}}{2} < 0$ follows. Now the theorem directly follows from Lemma 1.

2. We hope that Theorem 1 remains valid for $a \ge 5$ as well. We can prove the following partial result.

Theorem 2. *Let* $\Phi = \{\varphi(n) := 5n^2 + 1, \quad n \in \mathbb{N}\}$. *Then* $\mathcal{P}(\Phi) =$ *set of 2 and all those odd primes* q *for which* $\left(\frac{-5}{q}\right) = 1$. *Furthermore, every* $r \in \langle \mathcal{P}(\Phi) \rangle$ *can be written as*

$$r = \rho\eta, \tag{2.1}$$

where $\eta \in \langle \Phi \rangle$ *and* $\rho = 1$ *or* 2. *Finally,* $2 \notin \langle \Phi \rangle$.

Proof. First we prove that $2 \notin \langle \Phi \rangle$. Let us assume indirectly that $\varphi(n_1) \dots \varphi(n_s) = 2\varphi(m_1) \dots \varphi(m_h)$. Since $\varphi(m_j), \varphi(n_e)$ are $\equiv 1 \pmod 5$, this is obvious.

We have $\varphi(1) = 6$, $\varphi(2) = 3 \cdot 7$, $\varphi(8) = 3 \cdot 107$, $\varphi(12) = 7 \cdot 107$, we have $\varphi(2)\dfrac{\varphi(8)}{\varphi(12)} = 3^2 \in \langle \Phi \rangle$, $\quad \dfrac{\varphi(1)^2}{3^2} = 2^2 \in \langle \Phi \rangle$.

Let $p \in \mathcal{P}(\Phi)$, $p > 6$, and assume that every prime $q \in \mathcal{P}(\Phi)$, $q < p$ can be written as $\rho\eta$, where $\rho = 1$ or 2, $\eta \in \langle \Phi \rangle$.

We have to prove that the same is true for p as well.

Let n_p be the smallest positive integer for which $5n_p^2 + 1 \equiv 0 \pmod p$. Then $n_p \le \dfrac{p-1}{2}$. Let $5n_p^2 + 1 = A_p \cdot p$. If A_p is not prime, then all its prime divisors are less than p, consequently we can use the inductional hypothesis. We may assume that $A_p =$ prime $= Q \ge p$. In this case $6 \mid n_p$. Let us consider $\varphi(p - n_p)$. Since $(p - n_p, 6) = 1$, therefore $6 \mid \varphi(p - n_p) = 6Rp$. Then $6Rp \le 5p^2$, and so $R < p$, the prime factors of R can be written in the form (2.1), consequently

p can be written in the form (2.1) as well. Hence our theorem immediately follows.

3. We have

3.1. Theorem 3. *Let* $\Phi = \{\varphi(n) = 4n^2 + 1, \quad n \in \mathbb{N}\}$. *Then*

$$\mathcal{P}(\Phi) = \{p \in \mathcal{P} \mid p \equiv 1 \pmod 4\} \quad \textit{and} \quad \langle \mathcal{P}(\Phi)\rangle = \langle \Phi \rangle.$$

Proof. It is well-known that $p \in \mathcal{P}(\Phi)$ if and only if $p \neq 2$ and $\left(\frac{-1}{p}\right) = 1$, i.e. if $p \equiv 1 \pmod 4$. We have $\varphi(1) = 5 \in \langle\Phi\rangle$. Let $p \equiv 1 \pmod 4$, $p > 5$, and assume that every $q \in \mathcal{P}$, $q \equiv 1 \pmod 4$, $q < p$ belongs to $\langle\Phi\rangle$. Let y_0 be the smallest positive solution of $y^2 + 1 \equiv 0 \pmod p$. Then $y_0 \in \left[1, \dfrac{p-1}{2}\right]$, which is either even, or odd, and in the last case $p - y_0$ is even. Let $2n = y_0$ or $p - y_0$. Then $1 \leq 2n \leq p - 1$, $pH = \varphi(n) \leq p^2 - 2p + 2$, whence $H < p$, and so $H \in \langle\Phi\rangle$, i.e. $p = \dfrac{\varphi(n)}{H} \in \langle\Phi\rangle$. By using induction the proof is completed.

3.2. Theorem 4. *Let* $\Phi = \{\varphi(n) = 3n^2 + 1, \quad n \in \mathbb{N}\}$. *Then* $\mathcal{P}(\Phi) = \{2\} \cup \mathcal{P}_1$, *where* $\mathcal{P}_1 = \{p \mid p \equiv 1 \pmod 3\}$. *Then* $2 \notin \langle\Phi\rangle$, *and*

$$\langle\Phi\rangle = \langle\{2^2\} \cup \mathcal{P}_1\rangle.$$

Proof. If $2 \mid \varphi(n)$, then $2^2 \| \varphi(n)$. If $\gamma \in Q_x$ and

$$\gamma = \frac{\varphi(n_1)\ldots\varphi(n_k)}{\varphi(r_1)\ldots\varphi(r_s)},$$

then $2^\mu \| \gamma$ implies that μ is even, and so $2 \notin \langle\Phi\rangle$. Furthermore, $\varphi(1) = 2^2 \in \langle\Phi\rangle$. Since $\varphi(2) = 13$, $\varphi(3) = 28$, $\varphi(4) = 49$, $\varphi(5) = 4\cdot 19$, we obtain that $7, 13, 19 \in \langle\Phi\rangle$. Let $p \equiv 1 \pmod 3$, $p > 20$, and assume that $q \in \langle\Phi\rangle$ if $q < p$, $q \in \mathcal{P}$, $q \equiv 1 \pmod 3$.

Let $\kappa(y) := y^2 + 3$. Then $3\varphi(n) = (3n)^2 + 3 = \kappa(3n)$. Let y_0 be the smallest positive integer for which $\kappa(y) \equiv 0 \pmod p$ holds. We define n_0 as follows.

If $3 | y_0$, then $n_0 := \dfrac{y_0}{3}$. If $y_0 \equiv 1 \pmod 3$, then let $n_0 = \dfrac{p - y_0}{3}$, if $y_0 \equiv -1 \pmod 3$, then $n_0 = \dfrac{y_0 + p}{3}$. In the first and second case $3n_0 \in [1, p-1]$, in the last case $3n_0 \in \left[1, \dfrac{3}{2}p - \dfrac{1}{2}\right]$. Thus $1 \leq 3\varphi(n_0) = \kappa(3n_0) < \left(\dfrac{3}{2}p - \dfrac{1}{2}\right)^2 + 3$. Let us write $\varphi(n_0)$ as pH. Then

$$H = \frac{3\varphi(n_0)}{3p} < \frac{1}{3p}\left\{\frac{9}{4}p^2 - \frac{3}{2}p + \frac{13}{4}\right\},$$

and the right hand side is less than p if $p > 20$. Arguing as earlier, the theorem follows.

4. We have

Lemma 2. *Let* $\varphi(n) := n^2 + A$, $A \in \mathbb{N}, R \in \mathbb{N}$, $\beta(n) := R\varphi(n)$. *Let* $\Phi := \{\varphi(n) \mid n \in \mathbb{N}\}$, $B := \{\beta(n) \mid n \in \mathbb{N}\}$. *Then* $R \in \langle B\rangle$, *consequently* $\gamma \in \langle B\rangle$ *if and only if* $\gamma = R^\nu\sigma$, $\nu \in \mathbb{Z}$ *and* $\sigma \in \langle\Phi\rangle$.

Proof. This is clear. Since $\varphi(n+\varphi(n)) = \varphi(n)\varphi(n+1)$, therefore

$$R = \frac{\beta(n)\beta(n+1)}{\beta(n+\varphi(n))} \in \langle B\rangle.$$

The further part of the assertion is straightforward.

By using Lemma 2 and our result in [1] we can count $\langle 2n^2 + 2a \mid n \in \mathbb{N}\rangle$ from $\langle n^2 + a \mid n \in \mathbb{N}\rangle$.

5. Our next assertion is quite obvious. Let $a > 0$, $0 < b$, $(a,b) = 1$, $f_b(x) = ax + b$, $S_b := \langle f_b(n) \mid n \in \mathbb{N}_0$. Since $(a\nu+1)f_b(n_0) \equiv b \pmod{a}$ for every $\nu = 0, 1, 2, \ldots$, therefore $a\nu = 1 \in S_b$, and so $S_1 \subseteq S_b$. Furthermore, $b \in S_b$, and so $b^j \in S_b$. Let ν_0 be the smallest positive integer for which $b^{\nu_0} \equiv \pmod{a}$.

Theorem 5. *We have*

$$S_1 = \{r \in Q_x \mid r \equiv 1 \pmod{a}\}, \tag{5.1}$$

$$S_b = \langle 1, b, \ldots, b^{\nu_0 - 1}\rangle \otimes S_1. \tag{5.2}$$

Proof. Let $r \in S_1$. Then $r = \prod_{j=1}^{k} f_1(n_j)^{\varepsilon_j}$, whence from $f_1(n_j) \equiv$ $\equiv 1 \pmod{a}$ we obtain that $r \equiv 1 \pmod{a}$. Other hand, let $r = \dfrac{A}{B} \equiv 1 \pmod{a}$, i.e. $A, B \in \mathbb{N}$ and $A \equiv B \pmod{a}$. Let $B = A + ha$. Then the diophantine equation $A[an_1 + 1] = B[an_2 + 1]$ is solvable, since it is equivalent to $An_1 - Bn_2 = h$. Thus (5.1) is true.

To prove (5.2) we observe that $\langle 1, k, \ldots, b^{\nu_0-1}\rangle \otimes S_1 \subseteq S_b$. Other hand, if $\rho \in S_b$, then $\rho = f_b(m_1)^{\varepsilon_1} \ldots f_b(m_t)^{\varepsilon_t}$, and so

$$(\gamma :=)(f_b(m_1)b^{-1})^{\varepsilon_1} \ldots (f_b(m_t)b^{-1})^{\varepsilon_t} = b^{-(\varepsilon_1 + \ldots + \varepsilon_t)}\rho.$$

Since $f_b(m_j)b^{-1} \equiv 1 \pmod a$, therefore $\gamma \equiv 1 \pmod a$, $\gamma \in S_1$, $\rho = b^{(\varepsilon_1 \dots + \varepsilon_t)}\gamma$, $\gamma \in S_1$. The proof is completed.

Remark. We proved that every $r \in Q_x$, $r \equiv 1 \pmod a$ can be written in the form $r = \dfrac{f_1(n_1)}{f_1(n_2)}$ with suitable chosen $n_1, n_2 \in \mathbb{N}_0$.

6. Let $\alpha > 0$ irrational,

$$f(n) = [n\alpha] \qquad (n \in \mathbb{N}).$$

Assertion: $\langle \{f(n) \mid n \in \mathbb{N}\rangle = Q_x$.

Proof. Let $m \in \mathbb{N}$. Let $\Theta_n = \{n\alpha\}$, so $n\alpha = f(n) + \Theta_n$ is everywhere dense in $[0,1)$, therefore there exists an n for which $0 < \Theta_n < 1/m$. For such an n we have $n\alpha \cdot m = m \cdot f(n) + m\Theta_n$, $0 < m\Theta_n < 1$, and so $[nm\alpha] = f(mn) = m \cdot f(n)$, i.e. $m = \dfrac{f(mn)}{f(n)}$. Thus $m \in \langle \{f(n) \mid n \in \mathbb{N}\}\rangle$, and so the assertion is true.

Theorem 6. *Let $\alpha > 0$ be an irrational number, $\mathcal{P}_2$ be the set of those natural numbers which are either primes or products of two primes, i.e. $\mathcal{P}_2 = \{n = p \text{ or } n = pq, \quad p, q \in \mathcal{P}\}$.*

Let $\mathcal{H} := \{f(n) \mid n \in \mathcal{P}_2\}$. Then $\langle \mathcal{H} \rangle = Q_x$.

Proof. Since $\{p\alpha\}$ $(p \in \mathcal{P})$ is dense in $[0,1)$, therefore there exists such a p for which $0 < \Theta_p < 1/q$. Here $\Theta_n = \{n\alpha\}$.

We have $p\alpha = f(p) + \Theta_p$, $pq\alpha = qf(p) + q\Theta p$, $0 < q\Theta p < 1$, therefore $[pq\alpha] = f(pq) = qf(p)$, and so $q \in \langle \mathcal{H} \rangle$. Since $q \in \mathcal{P}$ is arbitrary, therefore the thorem is true.

Conjecture 1. *If α is a positive irrational number, then*

$$\langle \{[p\alpha] \mid p \in \mathcal{P}\}\rangle = Q_x.$$

7. Final remarks.

1. *Let $f(n) := [\alpha n^k]$, where $\alpha > 0$ is an irrational number, $k > 0$ is an integer.*
   Then a) $\mathcal{P}(\{f(n) \mid n \in \mathbb{N}\}) = \mathcal{P}$ and b) $\mathcal{P}(\{f(p) \mid p \in \mathcal{P}\}) = \mathcal{P}$.

These assertions are clear from the known theorems that sequences $f(n)$ $(n \in \mathbb{N})$, as well as $f(p)$ $(p \in \mathcal{P})$ are mod 1 uniformly distributed.

2. Let $q_1 < q_2 < \dots$ be a sequence of primes for which $\sum_{j=1}^{\infty} 1/q_j < \infty$. Let $\mathcal{R} := \{q_1 < q_2 < \dots\}$, and $\mathcal{B}$ be the whole set of positive integers m for

which $(m, q_j) = 1$ $(j = 1, 2, \ldots)$. Then the asymptotic density of $\mathcal{B}$ is positive, namely $\prod_{j=1}^{\infty}(1 - 1/q_j)$.

3. What can we assume for $\mathcal{D}$ $(\subseteq \mathbb{N})$ to satisfy $\mathcal{P}(\mathcal{D}) = \mathbb{N}$? Remark 2 shows the condition that $\mathcal{D}$ has positive density is not sufficient, while there exist sets satisfying $\mathcal{P}(\mathcal{D}) = \mathbb{N}$ which are relatively rare (Remark 1).

   Conjecture 2. *Let $\alpha > 0$ be an irrational number. Then*

$$\langle [\alpha n^2],\ n \in \mathbb{N} = Q_x,$$

and

$$\langle [\alpha p^2],\ p \in \mathcal{P} \rangle = Q_x.$$

References

[1] **Fehér J. and Kátai I.,** On sets of uniqueness for additive and multiplicative functions over the multiplicative group generated by the polynomial $x^2 + a$, *Annales Univ. Sci. Budapest. Sect. Math.,* **47** (2004), 3-16.

[2] **Elliott P.D.T.A.,** *Arithmetic functions and integer products,* Springer Verlag, 1985.

(Received December 11, 2006)

J. Fehér
Institute of Mathematics
and Informatics
University of Pécs
Ifjúság u. 6.
H-7624 Pécs, Hungary

I. Kátai
Department of Computer Algebra
Eötvös Loránd University
and Research Group of Applied
Number Theory of the
Hungarian of Academy of Sciences
Pázmány Péter sét. 1/C
H-1117 Budapest, Hungary
katai@compalg.inf.elte.hu