Annales Univ. Sci. Budapest., Sect. Comp. 22 (2003) 287-297

A CHARACTERIZATION OF SOME INTEGER–VALUED ARITHMETICAL MULTIPLICATIVE FUNCTIONS

J.-L. Mauclaire (Paris, France)

Dedicated to Professor Karl-Heinz Indlekofer on his sixtieth birthday

Abstract. Extending a result of Subbarao [4], we give a characterization of a class of integer-valued multiplicative functions satisfying some congruence relation.

1. Introduction

Starting with a famous article of Paul Erdős [1], the characterization of an additive arithmetical function as a logarithm has turned to be a rather classical problem in Probabilistic Number Theory, and similarly, the question of the determination of multiplicative functions has been considered. One of the oldest results, now quite classical, is due to Subbarao [4] who proved in 1966 that if f is an integer-valued multiplicative function defined on the semigroup of the positive integers N^*, $f(1) \neq 0$, and if for all positive integers m and n the relation $f(m+n) \equiv f(m) \bmod n$ holds, then there exists a non-negative integer k such that $f(n) = n^k$ for all n of N^*.

In this article, we shall give an extension of this result.

2. Result

We have the following result:

Theorem 1. *Let p be an odd prime number and a, b, c be elements of N^* relatively prime with p such that*

i) a is a primitive root mod p, *and $p^2 \nmid a^{p-1} - 1$, and is not a squarefull number, i.e. there is a prime q such that $q|a$, $q^2 \nmid a$.*

ii) b is a primitive root mod p, *and $p^2 \nmid a^{p-1} - 1$.*

iii) $c \neq 1$.

iiii) The numbers a, b, c are multiplicatively independent, which means that the relation $a^k b^l c^m = 1$, $k, l, m \in Z$, implies that $k = l = m = 0$.

We denote by S the semigroup generated by a, b, c.

Let f be an integer-valued function defined on S, multiplicative on S, i.e. if $n \in S$ and is written $n = a^k b^l c^m$, where k, l, m are non-negative integers, we have $f(n) = f(a^k b^l c^m) = f(a^k) f(b^l) f(c^m)$, and such that $f(1) \neq 0$.

Assume that there exists a sequence of positive integers $\alpha(k), k \in N^*$, such that $\lim_{k \to +\infty} \alpha(k) = +\infty$ and that

(H) for all positive elements m and n of S, the condition $n \equiv m \bmod p^k$ implies that $f(n) \equiv f(m) \bmod p^{\alpha(k)}$.

Then, f is the restriction to the semigroup S of a function F defined on the set of the elements of N^* relatively prime to p and either by $F(n) = n^r$, or $F(n) = \left(\frac{n}{p}\right) n^r$, where r is a non-negative integer and $\left(\frac{n}{p}\right)$ is the Legendre symbol mod p.

Remark 1. The proof will show that the number c is introduced essentially for technical reasons and, in fact, it is reasonable to do the following conjecture.

Conjecture 2. *Let p an odd prime number and a and b be elements of N^* relatively prime with p satisfying conditions i) and ii) of the above theorem and*

iii') the numbers a, b are multiplicatively independent, i.e. if $a^k b^l = 1$, $k, l \in Z$, then $k = l = 0$.

As above, we denote by S the semigroup generated by a and b, and f is an integer-valued function defined on S, multiplicative on S, $f(1) \neq 0$, and we assume that there exists a sequence of positive integers $\alpha(k), k \in N^*$, such that $\lim_{k \to +\infty} \alpha(k) = +\infty$, and that the condition (H) is satisfied.

Then, the same conclusion as in the above theorem still holds.

Remark 2. We underline the fact that the identification of f and F is valid only on the semigroup S, i.e. if $n \in S$ and is written $n = a^k b^l c^m$, where k, l, m are non-negative integers, the theorem will give only the following equalities:

$$\begin{aligned} f(n) = f(a^k b^l c^m) &= f(a^k) f(b^l) f(c^m) = \\ &= F(a^k b^l c^m) = F(a^k) F(b^l) F(c^m) = \\ &= F(a)^k F(b)^l F(c)^m = f(a)^k f(b)^l f(c)^m. \end{aligned}$$

Elsewhere, we have no more information concerning this identification.

Typically, if $f(m)$ is an ordinary positive multiplicative function and it satisfies the hypothesis of the above theorem with some a, b, c and for instance, $a = 4$, $f(4) = 4$, and $f(2) = 4$, the result will give that $f(4) = F(4)$, and so, $|F(2)| = 2$ since $F(4) = F(2)^2 = 4$, but evidently not that $|F(2)| = f(2)$ since we have $f(2) = 4$.

An immediate corollary of the above theorem is the following

Corollary 3. *Let f be an integer-valued multiplicative function defined on the semigroup of the positive integers N^*.*

Assume that $f(1) \neq 0$ and there exists a sequence of positive integers $\alpha(k)$, (resp. β_k), $k \in N^*$, such that $\lim\limits_{k \to +\infty} \alpha(k) = +\infty$, (resp. $\lim\limits_{k \to +\infty} \beta(k) = +\infty$), and two different odd prime numbers p and q such that

(H') for all positive elements m and n of N^*, the condition $n \equiv m \bmod p^k$ (resp. $n \equiv m \bmod q^k$) implies that $f(n) \equiv f(m) \bmod p^{\alpha(k)}$ (resp. $f(n) \equiv \equiv f(m) \bmod q^{\beta(k)}$).

Then, there exists a non-negative integer k such that $f(n) = n^k$ for all n of N^*.

Remark 3. An immediate consequence of this corollary is the result of Subbarao presented above.

3. Proofs

3.1. Proof of the theorem

1) Since f is integer-valued, it can be identified to a function with values in Z_p, the ring of the p-adic integers, and the hypothesis H give immediately that f is a uniformly continuous function on S for the p-adic topology, and as

a consequence, can be identified to the restriction of a continuous function F defined on $\overline{S}$, the p-adic closure of S, with values in Z_p.

Since a is a primitive root $\bmod p$, and $p^2 \nmid a^{p-1}-1$, the sequence $a^k,\ k \in \in N^*$, is dense in Z_p^*, the multiplicative group of the p-adic units ([5], Ch VI, 2-e, p.107) and so, we get that $\overline{S} = Z_p^*$.

2) As in the case of a, since b is a primitive root $\bmod p$, and $p^2 \nmid b^{p-1}-1$, the sequence $b^k,\ k \in N^*$, is dense in Z_p^*.

Let q be an element of Z^* such that $(q,p) = 1$, and let $\lambda_k(q)$ (resp. $\mu_k(q)$) be a sequence of positive integers such that $\lim\limits_{k\to+\infty} b^{\lambda_k(q)} = q$ (resp. $\lim\limits_{k\to+\infty} a^{\mu_k(q)} = q$).

It is clear that, if r is in N, by continuity of F, we have

$$F(q^r) = F\left(\left(\lim_{k\to+\infty} b^{\lambda_k(q)}\right)^r\right) = F\left(\lim_{k\to+\infty} b^{r\lambda_k(q)}\right) =$$
$$= \lim_{k\to+\infty} F\left(b^{r\lambda_k(q)}\right) = \lim_{k\to+\infty} f\left(b^{r\lambda_k(q)}\right),$$

and similarly for a, if s is in N, we have

$$F(q^s) = F\left(\left(\lim_{k\to+\infty} a^{\mu_k(q)}\right)^s\right) = F\left(\lim_{k\to+\infty} a^{s\mu_k(q)}\right) =$$
$$= \lim_{k\to+\infty} F\left(a^{s\mu_k(q)}\right) = \lim_{k\to+\infty} f\left(a^{s\mu_k(q)}\right).$$

This gives that, for any r and s in N, we have

$$F\left(q^{r+s}\right) = F(q^r q^s) = F\left(\left(\lim_{k\to+\infty} b^{r\lambda_k(q)}\right) \times \left(\lim_{k\to+\infty} a^{s\mu_k(q)}\right)\right)$$

since the sequences a^k and $b^k,\ k \in N^*$, are dense in Z_p^*,

$$= F\left(\lim_{k\to+\infty}\left(b^{r\lambda_k(q)} \times a^{s\mu_k(q)}\right)\right) = \lim_{k\to+\infty} F\left(b^{r\lambda_k(q)} \times a^{s\mu_k(q)}\right)$$

by continuity of F,

$$= \lim_{k\to+\infty} f\left(b^{r\lambda_k(q)} \times a^{s\mu_k(q)}\right)$$

since f and F coincide on S,

$$= \lim_{k\to+\infty}\left(f\left(b^{r\lambda_k(q)}\right) \times f\left(a^{s\mu_k(q)}\right)\right)$$

since f is multiplicative on S,

$$= \lim_{k\to+\infty} \left(F\left(b^{r\lambda_k(q)}\right) \times F\left(a^{s\mu_k(q)}\right)\right)$$

since f and F coincide on S,

$$= \lim_{k\to+\infty} \left(F\left(b^{r\lambda_k(q)}\right) \times \lim_{k\to+\infty} F\left(a^{s\mu_k(q)}\right)\right) = F(q^r) \times F(q^s)$$

by continuity of F.

As a consequence, we get that for all q in Z_p^*, if $\mu_k(q)$ is a sequence of positive integers such that $\lim\limits_{k\to+\infty} a^{\mu_k(q)} = q$, we have, since F is continuous,

$$F(q) = F\left(\lim_{k\to+\infty} a^{\mu_k(q)}\right) = \lim_{k\to+\infty} F\left(a^{\mu_k(q)}\right) =$$
$$= \lim_{k\to+\infty} f\left(a^{\mu_k(q)}\right) = \lim_{k\to+\infty} f(a)^{\mu_k(q)}.$$

Another consequence is that if $q \in S$ and is written $q = a^k b^l c^m$, where k, l, m are non-negative integers, we have

$$f(q) = f(a^k b^l c^m) = f(a)^k f(b)^l f(c)^m,$$

since

$$f(q) = f(a^k b^l c^m) = f(a^k) f(b^l) f(c^m) = F(a^k b^l c^m) =$$
$$= F(a^k) F(b^l) F(c^m) = F(a)^k F(b)^l F(c)^m = f(a)^k f(b^l) f(c)^m.$$

Moreover, we get also that $F(Z_p^*) \subseteq Z_p^*$.

For if $q \in Z_p^*$, we have, with the same notation as above,

$$F(q)^{l(p-1)} = F\left(q^{l(p-1)}\right) = F\left(\lim_{k\to+\infty} a^{l(p-1)\mu_k(q)}\right) =$$
$$= \lim_{k\to+\infty} F\left(a^{l(p-1)\mu_k(q)}\right) = \lim_{k\to+\infty} f\left(a^{l(p-1)\mu_k(q)}\right),$$

and if l is large enough, $f\left(a^{l(p-1)}\right) \in 1 + pZ_p$. So, F is a continuous representation of Z_p^* into Z_p^*.

3) Now, we define three numbers A, B, C, by $A = a^{p-1}$, $B = b^{p-1}$, $C = c^{p-1}$.

We remark that $A \in 1 + pZ_p$, but $A \notin 1 + p^2 Z_p$, and so, denoting by log the p-adic logarithm, $\log A$ is in pZ_p^*, and since $\log B \in pZ_p$ and $\log C \in pZ_p$, $\log B/\log A$ and $\log C/\log A$ are both in Z_p. As a consequence, we have, in Z_p,

$$\begin{aligned} A &= \exp(\log A), \\ B &= \exp\left((\log A)(\log B/\log A)\right), \\ C &= \exp\left((\log A)(\log C/\log A)\right). \end{aligned}$$

Now, since $F(A) = f\left(a^{p-1}\right) = f(a)^{p-1}$ and $f(a)$ is in Z_p^*, we know that $F(A)$ is in $1 + pZ_p$. As a consequence, we can write $F(A)$ in the form $F(A) = \exp(\log(F(A)))$. Moreover, since we have $B = \exp((\log A)(\log B/\log A))$, by continuity of F, we have

$$\begin{aligned} F(B) &= F\left(\exp((\log A)(\log B/\log A))\right) = F\left((\exp(\log A))^{(\log B/\log A)}\right) = \\ &= F(\exp(\log A))^{(\log B/\log A)} = F(A)^{(\log B/\log A)} = \\ &= f(A)^{(\log B/\log A)} = \exp(\log(f(A)) \times (\log B/\log A)), \end{aligned}$$

and similarly,

$$f(C) = \exp(\log(f(A)) \times (\log C/\log A)).$$

Consider now Σ, the Z-module generated by the three p-adic integers 1, $\log B/\log A$, $\log C/\log A$. Σ is a group of rank 3 on Z, for if there exist k, l, m in Z such that $k + l(\log B/\log A) + m(\log C/\log A) = 0$, this means that $k \log A + l \log B + m \log C = 0$, and since A, B, C are multiplicatively independent, we have $k = l = m = 0$. Now, we remark that for all $\sigma \in \Sigma$, $\exp(\sigma \log A)$ and $\exp(\sigma \log f(A))$ exist and take only rational values. We recall now the p-adic version given by Serre [3] of the well-known "six exponentials theorem" of Lang [2]:

Theorem 4. *Let A be a free subgroup of Q_p of finite rank $a \geq 3$ on Z, b_1 and $b_2 \in Q_p$, $b_1, b_2 \neq 0$. Assume that for all $z \in A$, $\exp b_1 z$ and $\exp b_2 z$ are algebraic on Q. Then, b_1 and b_2 are dependent on Q, i.e. $b_1/b_2 \in Q$.*

Remark 4. It is in order to mention now that the our conjecture is in fact essentially the well-known "four exponentials conjecture", which can be formulated like that:

Conjecture 5. *Let A be a free subgroup of Q_p of finite rank $a \geq 2$ on Z, b_1 and $b_2 \in Q_p$, $b_1, b_2 \neq 0$. Assume that for all $z \in A$, $\exp b_1 z$ and $\exp b_2 z$ are algebraic on Q. Then, b_1 and b_2 are dependent on Q, i.e. $b_1/b_2 \in Q$.*

We check now that this allows to assert that $\log A$ and $\log f(A)$ are rationally dependent, i.e. there exist integers r and s such that $r \log A = s \log f(A)$.

First, Σ is a subgroup of Q_p since it is generated as a Z-module by 1, $\log B/\log A$, $\log C/\log A$, which are elements of Z_p, and Σ is a free group of rank 3 on Z.

Second, for all $\sigma \in \Sigma$, $\exp(\sigma \log A)$ and $\exp(\sigma \log f(A))$ are algebraic on Q since they take only rational values.

So, the "six exponentials theorem" gives that $\log A$ and $\log f(A)$ are rationally dependent, i.e. there exist integers r and s such that $r \log A = s \log f(A)$.

This means exactly that $A^r = f(A)^s$, i.e. $a^{(p-1)\cdot r} = f(a)^{(p-1)\cdot s}$.

We shall drop the trivial case when r and s are equal to 0.

If $rs \neq 0$, since a and $f(a)$ are integers, we get that $a^r = |f(a)|^s$, which gives us that r and s are positive integers.

Now, since a is not squarefull, there exists a prime q such that $q \| a$, and so, $q^r \| \, |f(a)|^s$. This gives us that if $q^l \| \, |f(a)|$, then $r = ls$, and so, s divides r and we have $a^k = |f(a)|$ for some k in N^*.

4) Now, let u be any prime number different of p. We chose a non-negative integer r such that $u.a^r \equiv 1 \bmod p$. $u.a^r$ will be denoted by U.

We remark that since U is in $1 + pZ_p$, we can write $\log U$ as

$$\log U = (\log A)(\log U/\log A).$$

This gives us that

$$F(U) = F(\exp((\log A).(\log U/\log A)))$$

and by continuity of F, this can be written as

$$F(U) = (F(\exp \log A))^{(\log U/\log A)}.$$

Since $F(A) = A^k$ and A is a generator of $1 + pZ_p$, we get that

$$(F(\exp \log A)) = F(A) = \exp \log A^k = \exp(k \log A),$$

and so, we obtain that

$$F(U) = (F(\exp \log A))^{(\log U/\log A)} =$$

$$= (\exp k \log A)^{(\log U/\log A)} = \exp k \log U = U^k.$$

So, this means that

$$F(u.a^r) = (u.a^r)^k.$$

But we know that

$$F(u.a^r) = F(u)F(a^r),$$

and that

$$F(a^r) = f(a^r),$$

since a is in S.

Now, since $f(a^r)$ is an integer and

$$f(a^r) = f(a)^r$$

using the fact that

$$|f(a)| = a^k,$$

we get that

$$\begin{aligned}(u.a^r)^k = F(u.a^r) = F(u)F(a^r) = F(u)f(a^r) = \\ = F(u)|f(a)|^r(f(a)/|f(a)|)^r = F(u)a^{rk}(f(a)/|f(a)|)^r,\end{aligned}$$

and this gives us that

$$(u.a^r)^k = F(u)a^{rk}(f(a)/|f(a)|)^r,$$

and so

$$a^{rk}(u^k - F(u)(f(a)/|f(a)|)^r) = 0,$$

and since Z_p has no divisors of zero, this implies that

$$u^k = F(u)(f(a)/|f(a)|)^r.$$

Now, the fact that $(f(a)/|f(a)|)^r$ takes the values 1 or -1 gives us that $F(u)$ is an integer and moreover, $|F(u)| = u^k$, the constant k being independent of u.

A consequence is that for all n in N^* relatively prime with p,

$$|F(n)| = n^k.$$

5) We remark that since for all n in N^* relatively prime with p, $|F(n)| = n^k$, the function $\chi(n)$ defined by $\chi(n) = F(n)/|F(n)|$ exists, is completely multiplicative on the set of the n such that $(n, p) = 1$, and takes only the values 1 or -1. Now, since F is uniformly continuous on Z_p^*, by density in Z_p^* of the n in N^* relatively prime with p, there exists an l such that if $m \equiv n \bmod p^l$, then

$F(m) - F(n)$ belongs to pZ_p. This means that $(\chi(m)|F(m)| - \chi(n)|F(n)|) \in$ $\in pZ_p$, and we deduce that since

$$\chi(m)|F(m)| - \chi(n)|F(n)| =$$

$$= (\chi(m)(|F(m)| - |F(n)|) - (\chi(n) - \chi(m))|F(n)|) \in pZ_p$$

and $(|F(m)| - |F(n)|) = m^k - n^k \in pZ_p$, then $(\chi(n) - \chi(m))|F(n)| \in pZ_p$, i.e. $(\chi(n) - \chi(m))n^k \in pZ_p$, which implies that $\chi(n) = \chi(m)$ because $(n, p) = 1$ and $\chi(n) = \pm 1$. This allows to assert that there exists some r in N such that the equality $\chi(n) = \chi(n + p^r)$ holds for all integers n such that $(n, p) = 1$.

Now, let n be any positive integer, $(n, p) = 1$, $1 \leq n \leq p^r - 1$. Viewed as a p-adic integer, n can be written in a unique way as $n = a(1 + pu)$, where a is a $(p - 1)$-root of the unity, and u is in Z_p. Since $\chi(n) = \pm 1$ and p is odd, we have $\chi(n)^{p^{r-1}} = \chi(n)$. This can be written as

$$\chi(n) = \chi(n)^{p^{r-1}} = \chi(a(1 + pu))^{p^{r-1}} = \chi(a^{p^{r-1}}(1 + pu)^{p^{r-1}}) =$$
$$= \chi(a^{p^{r-1}}).\chi((1 + pu)^{p^{r-1}}) = \chi(a),$$

since $a^{p^{r-1}} = a$ and $(1 + pu)^{p^{r-1}} \equiv 1 \mod p^r$.

Hence we get that $\chi(n) = \chi(n \bmod p)$, i.e. χ is a character mod p.

If χ is not identically equal to 1, denoting by $\left(\frac{n}{p}\right)$ the Legendre symbol, we have

$$\chi(n) = 1 \quad \text{if} \quad \left(\frac{n}{p}\right) = 1,$$

since $\left(\frac{n}{p}\right) = 1$ means that $n \equiv x^2 \mod p$ for some x and so, $\chi(n) = \chi(x^2) =$ $= \chi(x)^2 = 1$.

Now, since χ is a real character, we have

$$\sum_{1 \leq m \leq p-1} \chi(n) = 0 =$$

$$= \sum_{1 \leq m \leq p-1,\ \left(\frac{n}{p}\right)=1} \chi(n) + \sum_{1 \leq m \leq p-1,\ \left(\frac{n}{p}\right)=-1} \chi(n) =$$
$$= (p - 1)/2 + \sum_{1 \leq m \leq p-1,\ \left(\frac{n}{p}\right)=-1} \chi(n),$$

for there are $(p-1)/2$ quadratic residues mod p and so, we get that

$$\sum_{1\le m\le p-1,\ \left(\frac{n}{p}\right)=-1} \chi(n) = -(p-1)/2,$$

which implies that

$$\chi(n) = -1 \quad \text{if} \quad \left(\frac{n}{p}\right) = -1,$$

for there are $(p-1)/2$ non-quadratic residues mod p, and this gives us that

$$\chi(n) = \left(\frac{n}{p}\right).$$

3.2. Proof of the corollary

First, we apply the theorem to get that on the set of the elements of N^* relatively prime to p, we have either $f(n) = n^k$ or $f(n) = \left(\frac{n}{p}\right) n^k$, where k is a non-negative integer. Similarly, the theorem gives that on the set of the elements of N^* relatively prime to q, we have either $f(n) = n^{k'}$ or $f(n) = \left(\frac{n}{q}\right) n^{k'}$, where k' is also non-negative integer.

Clearly, this implies that $k = k'$ since we have $|f(n)| = n^k = n^{k'}$ for all $n \in N^*$ such that $(n, pq) = 1$.

Now, on the same set of the $n \in N^*$ such that $(n, pq) = 1$, we must have $f(n)/n^k = 1$ or $\left(\frac{n}{p}\right)$, or $\left(\frac{n}{q}\right)$. It is clear that neither the equality $\left(\frac{n}{p}\right) = \left(\frac{n}{q}\right)$, nor $\left(\frac{n}{p}\right) = 1$ or $\left(\frac{n}{q}\right) = 1$, can hold on the whole set of the n such that $(n, pq) = 1$, and so, $f(n)/n^k = 1$ for all n in N^*.

References

[1] **Erdős P.,** On the distribution function of additive arithmetical functions, *Annals of Math.,* **46** (1945), 1-20.

[2] **Lang S.,** *Nombres transcendants*, Séminaire Bourbaki, 18ième année, **305** (1965/1966).

[3] **Serre J.P.,** *Dépendance d'exponentielles p-adiques*, Séminaire Delange-Pisot-Poitou, 7ième année, **15** (1965/1966).

[4] **Subbarao M.V.,** Arithmetic functions satisfying congruence property, *Canad. Math. Bull.,* **9** (1966), 143-146.

[5] **Vinogradov I.M.,** *Elements of number theory*, Dover, 1954.

J.-L. Mauclaire
Théorie des nombres
Institut de mathématiques (UMR 75867 du CNRS)
Université Pierre et Marie Curie
175 Rue de Chevaleret, Plateau 7D
F-75013 Paris, France