# On the iteration of a multiplicative function defined on the Gaussian integers 

By M. van ROSSUM-WIJSMULLER (Philadelphia)

## 1. Introduction

The iterates of completely multiplicative functions were studied by I. KÁtai in [1] and [2], in which papers the discussion dealt mainly with the specific function $\vartheta(n)=\vartheta_{a}(n)$ defined by

$$
\vartheta(p)=p+a \quad \text { for all primes } p
$$

where $a$ is a fixed positive integer. The iterates are defined by

$$
\vartheta_{1}(n)=\vartheta(n) \text { and } \vartheta_{k}(n)=\vartheta\left(\vartheta_{k-1}(n)\right) \text { for } k=2,3, \ldots .
$$

The kernel $K=K_{a}$ of the iteration was defined as the set of primes which, for some integer $n$, are divisors of $\vartheta_{k}(n)$ for infinitely many $k$ and it was shown that $K$ is finite for all $a$; in fact if $p \in K$ then $p \leq(2 b-1) a$ where $b>1$ and coprime to $a$. This bound was lowered by R. M. Pollack, H. N. Shapiro and G. H. Sparer in [3] where Theorem 3.3 states:

If $p \in K$ then $p \leq b+(b-1) a$ where $b$ is the smallest prime not dividing $a$.
In the present paper we study the kernel of the iteration of a similar function $\vartheta=\vartheta_{\alpha}$ which is defined on the set of Gaussian integers. To make questions of growth meaningful we restrict ourselves to those Gaussian integers which are in the first quadrant. We show that also in this case the kernel of the iteration is finite and give an upperbound for the norm of the elements in the kernel. This upperbound depends upon $\alpha$.

## 2. Notation and definitions

We denote the set of Gaussian integers by $\mathfrak{G}$ while $\mathfrak{G}_{1}$ indicates the set of nonzero Gaussian integers which lie in the first quadrant, i.e. with argument in $\left[0, \frac{\pi}{2}\right)$. For every $\alpha \in \mathfrak{G}$ the norm of $\alpha$ will be denoted by $\mathfrak{N}(\alpha)$; thus for $\alpha=a+b i, \mathfrak{N}(\alpha)=a^{2}+b^{2}$. Greek letters will be used for
the elements of $\mathfrak{G}$; the letter $\varepsilon$ will be reserved for a unit in $\mathfrak{G}$ while $\rho$ and $\eta$ indicate primes in $\mathfrak{G}$. The letters $a, b, c, \ldots$ represent rational integers; $p$ and $q$ are used only for rational primes.

Let $\alpha$ be a fixed element of $\mathfrak{G}_{1}$ and $\vartheta=\vartheta_{\alpha}$ a completely multiplicative function defined on $\mathfrak{G}$; i.e. satisfying the relation

$$
\vartheta(\beta \gamma)=\vartheta(\beta) \vartheta(\gamma) \text { for all } \beta \text { and } \gamma \text { in } \mathfrak{G} .
$$

For each prime $\rho$ in $\mathfrak{G}$ let $\varepsilon=\varepsilon_{\rho}$ be a unit such that $\varepsilon \rho \in \mathfrak{G}_{1}$ and define

$$
\vartheta(\rho)=\varepsilon \rho+\alpha
$$

Following I. KÁtai we define the iterates of $\vartheta$ by

$$
\vartheta_{1}(\beta)=\vartheta(\beta) \text { and } \vartheta_{k}(\beta)=\vartheta\left(\vartheta_{k-1}(\beta)\right) \text { for } k=2,3, \ldots ; \beta \in \mathfrak{G} .
$$

It is obvious that $\vartheta_{k}(\beta)$ is also a completely multiplicative function for any integer $k$.

For each $\beta \in \mathfrak{G}$ let $E(\beta)$ denote the set of primes $\rho$ in $\mathfrak{G}_{1}$ which divide $\vartheta_{k}(\beta)$ for infinitely many $k$. Clearly

$$
\begin{equation*}
E(\beta)=E\left(\vartheta_{k}(\beta)\right) \text { for } k=1,2, \ldots \tag{1}
\end{equation*}
$$

The kernel of the iteration $K=K_{\alpha}$ is defined to be $\bigcup_{\beta \in \mathfrak{G}} E(\beta)$.
We will show that $K$ is finite for every $\alpha$ in $\mathfrak{G}_{1}$ and describe some characteristics of the primes in $K$.

## 3. $(1+i)$ is in $K$

In [3] it is proved that the prime 2 belongs to $K_{a}$ for every integer $a$. The following theorem is the complex analogue of this results.

Theorem 1. The prime $(1+i)$ belongs to $K$ for all $\alpha$.
Proof. If $\rho$ divides $\alpha$ then $\rho \mid(\rho+\alpha)=\vartheta(\rho)$ from which it follows that $\rho \mid \vartheta_{k}(\rho)$ for all $k$ and $\rho$ is in $K$. Therefore, if $(1+i) \mid \alpha$ it follows that $(1+i) \in K$. On the other hand if $(1+i) \nmid \alpha$ and $\alpha=a+b i$ then $a \not \equiv b(\bmod 2)$. The same holds for the real and imaginary parts of any prime $\rho$ which divides $\alpha$. Let $\rho$ be such a prime. Then $\rho \in K$ and, since $(1+i) \mid(\rho+\alpha)$ it follows that $(1+i) \in K$.

## 4. When $(1+i)$ does not divide $\alpha$

While the first lemma is rather obvious, its usefulness warrents its statement if not its proof.

Lemma 1. If $(1+i) \nmid \alpha, \rho \neq(1+i)$ and $\rho_{1} \mid(\rho+\alpha)$ then

$$
\mathfrak{N}\left(\rho_{1}\right)<\mathfrak{N}(\rho)+\mathfrak{N}(\alpha) .
$$

Proof. W.l.o.g. we may assume that $\alpha \neq \rho$. It is easy to show that $\mathfrak{N}(\rho+\alpha)<2 \mathfrak{N}(\rho)+2 \mathfrak{N}(\alpha)$ for all $\rho \neq \alpha$. Since $(1+i) \mid(\rho+\alpha)$ the result follows immediately.

Lemma 2. Let $\rho_{1}, \rho_{2}$, and $\rho_{3}$ be primes $\left(\in \mathfrak{G}_{1}\right)$, all different from $(1+i)$. If $\rho_{2} \mid \vartheta\left(\rho_{1}\right)$ and $\rho_{3} \mid \vartheta\left(\rho_{2}\right)$ then

$$
\mathfrak{N}\left(\rho_{3}\right)<\frac{\mathfrak{N}\left(\rho_{1}\right)+5 \mathfrak{N}(\alpha)}{2}
$$

Proof. When $\vartheta\left(\rho_{1}\right)=(1+i) \cdot \beta \cdot \rho_{2}$ with $\mathfrak{N}(\beta)>1$ then

$$
\mathfrak{N}\left(\rho_{2}\right)<\frac{\mathfrak{N}\left(\rho_{1}\right)+\mathfrak{N}(\alpha)}{\mathfrak{N}(\beta)}<\frac{\mathfrak{N}\left(\rho_{1}\right)+\mathfrak{N}(\alpha)}{2}
$$

and

$$
\mathfrak{N}\left(\rho_{3}\right)<\mathfrak{N}\left(\rho_{2}\right)+\mathfrak{N}(\alpha)<\frac{\mathfrak{N}\left(\rho_{1}\right)+3 \mathfrak{N}(\alpha)}{2}
$$

Similarly, if $\vartheta\left(\rho_{2}\right)=(1+i) \cdot \beta \cdot\left(\rho_{3}\right)$ with $\mathfrak{N}(\beta)>1$ then

$$
\mathfrak{N}\left(\rho_{3}\right)<\frac{\mathfrak{N}\left(\rho_{2}\right)+\mathfrak{N}(\alpha)}{2}<\frac{\mathfrak{N}\left(\rho_{1}\right)+2 \mathfrak{N}(\alpha)}{2} .
$$

There remains to consider the case where

$$
\vartheta\left(\rho_{1}\right)=(1+i) \cdot \varepsilon_{1} \cdot \rho_{2} \quad \text { and } \quad \vartheta\left(\rho_{2}\right)=(1+i) \cdot \varepsilon_{2} \cdot \rho_{3} .
$$

In this case there exist $\varepsilon$ and $\varepsilon^{\prime}$, both units in $\mathfrak{G}$, such that

$$
\begin{aligned}
& (1+i)^{2} \cdot \rho_{3}=(1+i) \cdot \varepsilon \cdot \vartheta\left(\rho_{2}\right)=(1+i) \cdot \varepsilon \cdot\left(\rho_{2}+\alpha\right)= \\
& \varepsilon^{\prime} \cdot \vartheta\left(\rho_{1}\right)+(1+i) \cdot \varepsilon \cdot \alpha=\varepsilon^{\prime} \cdot\left(\rho_{1}+\alpha\right)+(1+i) \cdot \varepsilon \cdot \alpha= \\
& \varepsilon^{\prime} \cdot \rho_{1}+\beta \cdot \alpha \text { with } \mathfrak{N}(\beta) \leq 5 .
\end{aligned}
$$

Therefore

$$
4 \mathfrak{N}\left(\rho_{3}\right)<2 \mathfrak{N}\left(\rho_{1}\right)+2 \mathfrak{N}(\beta \alpha) \leq 2 \mathfrak{N}\left(\rho_{1}\right)+10 \mathfrak{N}(\alpha)
$$

from which the result follows.
Since $\mathfrak{N}(\rho+\alpha)$ is even whenever $\rho \neq(1+i),(\rho+\alpha)$ is always composite and divisible by $(1+i)$. To distinguish between the cases where $\rho+\alpha$ has exactly two prime factors or when $\rho+\alpha$ factors into more than two factors we introduce the following notation:

$$
\begin{array}{lll}
\rho \rightarrow & \cdots & \text { indicates that } \rho+\alpha=(1+i) \cdot \rho . \\
\rho< & \cdots & \text { means that } \rho+\alpha=(1+i) \cdot(\text { composite number }) .
\end{array}
$$

Theorem 2. If $(1+i) \nmid \alpha$ and $\eta \in K$ then $\mathfrak{N}(\eta)<5 \mathfrak{N}(\alpha)$.
Proof. Let $F:=\left\{\eta \in \mathfrak{G}_{1} \mid \mathfrak{N}(\eta)<5 \mathfrak{N}(\alpha)\right\}$. Obviously for any $\beta$, $E(\beta)=\bigcup_{\rho \mid \beta} E(\rho)$ and we therefore investigate $E(\rho)$ for $\rho$ a prime.

When $\mathfrak{N}(\rho)>5 \mathfrak{N}(\alpha)$ we first consider the case that $\rho \rightarrow \rho_{1} \rightarrow \cdots \rightarrow$ $\rho_{i} \cdots$. Applying Lemma 2 repeatedly, it follows that there exists an integer $j$ such that $\mathfrak{N}\left(\rho_{j}\right)<5 \mathfrak{N}(\alpha)$. When $\rho \rightarrow \rho_{1} \rightarrow \cdots \rightarrow \rho_{i} 乙 \cdots, \mathfrak{N}\left(\rho_{i}\right)<$ $\mathfrak{N}(\rho)+\mathfrak{N}(\alpha)$ and if $\eta \mid \vartheta\left(\rho_{i}\right)$ then $\mathfrak{N}(\eta)<\mathfrak{N}(\rho)$. Therefore there exists a $k$ such that $\mathfrak{N}(\eta)<5 \mathfrak{N}(\alpha)$ if $\eta \mid \vartheta_{k}(\rho)$. By (1) it follows that $K=$ $\bigcup_{\mathfrak{N}(\rho)<5 \mathfrak{N}(\alpha)} E(\rho)$.

For primes $\rho$ with $\mathfrak{N}(\rho)<4 \mathfrak{N}(\alpha)$ it is trivial to show that $E(\rho) \subset F$. Hence we assume that $\mathfrak{N}(\rho)>4 \mathfrak{N}(\alpha)$.

When $\mathfrak{N}(\rho)<5 \mathfrak{N}(\alpha)$ and $\rho \rightarrow \rho_{1} \rightarrow \cdots \rightarrow \rho_{i} 乙 \cdots$, then $E\left(\vartheta_{i}(\rho)\right)=$ $E\left(\rho_{i}\right)$. By Lemma $2, \mathfrak{N}\left(\rho_{i}\right)<6 \mathfrak{N}(\alpha)$ and if $\eta \mid \vartheta\left(\rho_{i}\right)$ then $\mathfrak{N}(\eta)<4 \mathfrak{N}(\alpha)$ and $E(\rho)=E\left(\vartheta\left(\rho_{i}\right)\right) \subset F$.

When $\rho \rightarrow \rho_{1} \rightarrow \cdots \rightarrow \rho_{i} \cdots$, then $E\left(\rho_{i}\right)=E\left(\vartheta_{i}(\rho)\right)$ for all $i$. By Lemma 2 , $\mathfrak{N}\left(\rho_{2 i}\right)<5 \mathfrak{N}(\alpha)$ for all $i$ while there exists a $j$ such that $\mathfrak{N}\left(\rho_{2 i+1}\right)<5 \mathfrak{N}(\alpha)$ for $(2 i+1) \geq j$. Therefore $\mathfrak{N}\left(\rho_{i}\right)<5 \mathfrak{N}(\alpha)$ for all $i \geq j$ and $E(\rho)=E\left(\vartheta_{j}(\rho)\right) \subset F$, which finishes the proof.

## 5. When $(1+i)$ divides $\alpha$

When $(1+i) \nmid \alpha,(1+i)$ divides $(\rho+\alpha)$ except when $\rho=(1+i)$. But for those $\alpha$ which are divisible by $(1+i)$ it may be possible that $\rho+k \alpha$ is a prime for $k=1,2, \ldots, n$. How long this arithmetical progression of primes can be depends upon $\alpha$ and $\rho$. An upperbound for $n$ is obtained in Lemma 6, but first we need two lemma's in preparation.

Lemma 3. For a prime $\rho$ and $\alpha$ in $\mathfrak{G}_{1}$, where $\rho$ does not divide $\alpha$,

$$
\begin{equation*}
\mathfrak{N}(\rho+k \alpha)<\{\sqrt{\mathfrak{N}(\rho)}+k \cdot \sqrt{\mathfrak{N}(\alpha)}\}^{2} \tag{2}
\end{equation*}
$$

Proof. For $k=1,(2)$ follows from the triangular inequality. By induction (2) holds for all $k=1,2, \ldots$.

Lemma 4. If $a \not \equiv 0(\bmod p), a^{2}+c^{2} \equiv 0(\bmod p)$ and $r$ and $s$ are integers with $r^{2}+s^{2} \not \equiv 0(\bmod p)$ then

$$
\begin{equation*}
(r a+s c) \not \equiv 0 \quad(\bmod p) \tag{3}
\end{equation*}
$$

Proof. Since $a^{2}+c^{2} \equiv 0(\bmod p)$ and $a \not \equiv 0(\bmod p)$ it follows that $c \not \equiv 0(\bmod p)$. Suppose that $(r a+s c) \equiv 0(\bmod p)$, then

$$
r a^{2}+s c a \equiv-r c^{2}+s c a=c(s a-r c) \equiv 0 \quad(\bmod p) .
$$

This implies that

$$
\begin{equation*}
(s a-r c) \equiv 0 \quad(\bmod p) . \tag{4}
\end{equation*}
$$

Multiplying (3) and (4) by $s$ and $r$ respectively and subtracting the resulting congruences we obtain

$$
s^{2} c+r^{2} c=c\left(r^{2}+s^{2}\right) \equiv 0 \quad(\bmod p)
$$

This means that $r^{2}+s^{2} \equiv 0(\bmod p)$ which contradicts the hypothesis.
Lemma 5. Let $p$ be a rational prime, $p \equiv 1(\bmod 4)$ and $\alpha \in \mathfrak{G}_{1}$, with $\alpha=a+b i$ and $(a, b) \not \equiv(0,0)(\bmod p)$. For $\rho \in \mathfrak{G}_{1}$ with $\mathfrak{N}(\rho) \neq p$ there exists an integer $k \in\{1,2, \ldots, p-1\}$ such that

$$
\begin{equation*}
\mathfrak{N}(\rho+k \alpha) \equiv 0 \quad(\bmod p) \tag{5}
\end{equation*}
$$

Proof. We consider two cases, $a \equiv 0(\bmod p)$ and $a \not \equiv 0(\bmod p)$.
Case 1: If $a \equiv 0(\bmod p)$ then $b \not \equiv 0(\bmod p)$ and the set $\{k b \mid k=$ $1,2, \ldots, p-1\}$ is a reduced residue system modulo $p$. For $\rho=r+s i$,

$$
\mathfrak{N}(\rho+k \alpha) \equiv r^{2}+(s+k b)^{2} \quad(\bmod p)
$$

If $r \equiv 0(\bmod p)$ then $s \not \equiv 0(\bmod p)$ and there exists a unique value for $k$ for which (5) is true. If $r \not \equiv 0(\bmod p)$, because $r^{2}+s^{2} \equiv 0(\bmod p)$ and $p \equiv 1(\bmod 4),(5)$ has two solutions modulo $p$.

Case 2: When $a \neq 0(\bmod p)$ we define the set

$$
A=\{\beta \mid \beta=a+c i, \quad c=0,1, \ldots, p-1\} .
$$

Obviously $\mathfrak{N}(\rho+k \alpha) \equiv \mathfrak{N}(\rho+k \beta)(\bmod p)$ for some $\beta \in A$ and it is sufficient to prove that for every $\beta \in A$ there is some $k \in\{1,2, \ldots, p-1\}$ such that

$$
\begin{equation*}
\mathfrak{N}(\rho+k \beta) \equiv 0 \quad(\bmod p) \tag{6}
\end{equation*}
$$

Let $A_{0}=\{\beta \mid \beta \in A, \mathfrak{N}(\beta) \equiv 0(\bmod p)\}$ and $A_{1}=A-A_{0}$. Since $a \not \equiv 0(\bmod p) A_{0}$ has 2 elements and $A_{1}$ consists of the remaining $(p-2)$ elements of $A$. For each $\beta \in A_{0}$,

$$
\mathfrak{N}(\rho+k \beta) \equiv\left(r^{2}+s^{2}\right)+2 k(r a+s c) \quad(\bmod p)
$$

and it follows from Lemma 4 that (6) is a linear congruence modulo $p$. Therefore (6) has a unique solution for each $\beta \in A_{0}$. For $\beta \in A_{1}, \mathfrak{N}(\rho+k \beta)$ is a polynomial in $k$ of degree 2 and (6) has at most 2 solutions modulo $p$.

Let us define the set

$$
S=\{(\beta, k) \mid \beta \in A, 1 \leq k \leq p-1, \mathfrak{N}(\rho+k \beta) \equiv 0 \quad(\bmod p)\}
$$

The lemma is false if there is no solution for at least one element in $A_{1}$, which means that

$$
\begin{equation*}
|S| \leq 2\left\{\left|A_{1}\right|-1\right\}+2=2(p-3)+2=2 p-4 . \tag{7}
\end{equation*}
$$

We now calculate $|S|$ in a different way and obtain a contradiction. For a fixed $k$,

$$
\mathfrak{N}(\rho+k \beta)=(r+k a)^{2}+(s+k c)^{2} .
$$

If $(r+k a) \equiv 0(\bmod p)$ there is exactly one $c$ and therefore exactly one $\beta \in A$ such that (6) holds. In all other cases there are two distinct values for $c$ and therefore two distinct elements in $A$ for which (6) is true. Since $k$ can take on $(p-1)$ distinct values it follows that.

$$
|S|=1+(p-2) 2=2 p-3,
$$

which contradicts (7) and finishes the proof.
Lemma 6. Let $p$ be a rational prime, $p \equiv 1(\bmod 4)$ and $\alpha \in \mathfrak{G}_{1}$, with $\alpha=a+b i$ and $(a, b) \not \equiv(0,0)(\bmod p)$. For $\rho \in \mathfrak{G}_{1}$, with $\mathfrak{N}(\rho)>$ $(2 p+1) \mathfrak{N}(\alpha)$ there exists a positive integer $m \leq(p-1)$ such that $\rho, \rho+$ $\alpha, \ldots, \rho+(m-1) \alpha$ are all primes and $(\rho+m \alpha)$ is composite. Furthermore, if $\rho_{i} \mid(\rho+m \alpha)$ then $\mathfrak{N}\left(\rho_{i}\right)<\mathfrak{N}(\rho)$.

Proof. Obviously $\rho \nmid \alpha$ and $\mathfrak{N}(\rho) \neq p$. The existence of an integer $0<m \leq p-1$ such that $\rho+m \alpha$ is composite follows from Lemma 5. Therefore there is a smallest integer $m$ for which $\rho, \rho+\alpha, \ldots, \rho(m-1) \alpha$ are primes and $(\rho+m \alpha)$ is composite.

Let $\rho_{1}, \ldots, \rho_{t}$ be the prime divisors of $(\rho+m \alpha)$. We consider 3 cases:
Case1: The prime $p$ divides $\mathfrak{N}(\rho+m \alpha)$ and w.l.o.g. we assume that $\mathfrak{N}\left(\rho_{1}\right)=p$. Obviously $\mathfrak{N}\left(\rho_{1}\right)=p<(2 p+1) \mathfrak{N}(\alpha)<\mathfrak{N}(\rho)$.

For $\rho_{i}, i \neq 1$, we apply Lemma 3. Since $\mathfrak{N}(\rho)>(2 p+1) \mathfrak{N}(\alpha)$ it follows that

$$
\mathfrak{N}\left(\rho_{i}\right)<\frac{\{\sqrt{\mathfrak{N}(\rho)}+m \sqrt{\mathfrak{N}(\alpha)}\}^{2}}{p} \leq \frac{\mathfrak{N}(\rho)\left\{1+\frac{(p-1)}{\sqrt{2 p+1}}\right\}^{2}}{p} \leq \mathfrak{N}(\rho)
$$

since $p>4$. For the remaining cases we assume that $\mathfrak{N}\left(\rho_{1}\right) \leq \mathfrak{N}\left(\rho_{i}\right)$ for $i \neq 1$.

Case 2: The prime $p$ does not divide $\mathfrak{N}(\rho+m \alpha)$ and $\mathfrak{N}\left(\rho_{1}\right)=p^{*} \equiv 1$ $(\bmod 4)$.

If $p^{*}>p$ then

$$
\mathfrak{N}\left(\rho_{i}\right)<\frac{\{\sqrt{\mathfrak{N}(\rho)}+m \sqrt{\mathfrak{N}(\alpha)}\}^{2}}{p^{*}} \leq \frac{\{\sqrt{\mathfrak{N}(\rho)}+m \sqrt{\mathfrak{N}(\alpha)}\}^{2}}{p} \leq \mathfrak{N}(\rho)
$$

When $p^{*}<p$ one can show that the hypotheses of lemma 5 hold for the prime $p^{*}$. Therefore $m \leq\left(p^{*}-1\right)$ and since $\left(2 p^{*}+1\right)<(2 p+1)$ it follows that

$$
\mathfrak{N}\left(\rho_{i}\right)<\frac{\left\{\sqrt{\mathfrak{N}(\rho)}+\left(p^{*}-1\right) \sqrt{\mathfrak{N}(\alpha)}\right\}^{2}}{p^{*}} \leq \frac{\mathfrak{N}(\rho)\left\{1+\frac{\left(p^{*}-1\right)}{\sqrt{2 p+1}}\right\}^{2}}{p^{*}}<\mathfrak{N}(\rho) .
$$

Case 3: The prime $p$ does not divide $\mathfrak{N}(\rho+m \alpha)$ but $\mathfrak{N}\left(\rho_{1}\right)=q^{2}$ with $q \equiv 3(\bmod 4)$. Therefore

$$
\begin{equation*}
\operatorname{Re}(\rho+m \alpha) \equiv \operatorname{Im}(\rho+m \alpha) \equiv 0 \quad(\bmod q) . \tag{8}
\end{equation*}
$$

Since $m$ is the smallest positive integer such that $\rho+m \alpha$ is composite, it follows from (8) that we may assume $m \leq q-1$.

From Lemma 3 and the fact that $\mathfrak{N}(\alpha)<\mathfrak{N}(\rho)$ it follows that

$$
\mathfrak{N}\left(\rho_{i}\right)<\frac{\{\sqrt{\mathfrak{N}(\rho)}+(q-1) \sqrt{\mathfrak{N}(\alpha)}\}^{2}}{(q)^{2}}<\mathfrak{N}(\rho)
$$

This ends the proof of the lemma.
Lemma 7. Let $p$ be a rational prime, $p \equiv 1(\bmod 4)$ and $\alpha \in \mathfrak{G}_{1}$, with $\alpha=a+b i$ and $(a, b) \not \equiv(0,0)(\bmod p)$. For $\eta \in \mathfrak{G}_{1}$ with $p \neq \mathfrak{N}(\eta)<$ $(2 p+1) \mathfrak{N}(\alpha)$ there exists a positive integer $m \leq p-1$ such that $\eta, \eta+$ $\alpha, \ldots, \eta+(m-1) \alpha$ are all primes and $(\eta+m \alpha)$ is composite. Furthermore, if $\eta_{i} \mid(\eta+m \alpha)$ then $\mathfrak{N}\left(\eta_{i}\right)<(2 p+1) \mathfrak{N}(\alpha)$.

Proof. The proof is very similar to the proof of Lemma 6. Instead of factoring $\mathfrak{N}(\eta)$ out of $\{\sqrt{\mathfrak{N}(\eta)}+\sqrt{\mathfrak{N}(\alpha)}\}^{2}$ one factors $(2 p+1) \mathfrak{N}(\alpha)$ with the desired results.

We now are ready to discuss the kernel for those $\alpha$ 's that are divisible by $(1+i)$.

Theorem 3. Let $p$ be a rational prime with $p \equiv 1(\bmod 4)$. If $\alpha \in \mathfrak{G}_{1}$, $\alpha=a+b i$ with $(a, b) \not \equiv(0,0)(\bmod p)$ and $\eta$ is an element of $K$ then one of the following holds:

$$
\begin{gather*}
\mathfrak{N}(\eta)<(2 p+1) \mathfrak{N}(\alpha), \quad \text { or }  \tag{9}\\
\eta=\rho+k \alpha \text { with } \mathfrak{N}(\rho)<(2 p+1) \mathfrak{N}(\alpha) \text { and } k<(p-1) . \tag{10}
\end{gather*}
$$

Proof. Let $F=\left\{\eta \in \mathfrak{G}_{1} \mid \rho\right.$ satisfying (9) or (10) $\}$.
Let $\rho$ be a prime with $\mathfrak{N}(\rho)<(2 p+1) \mathfrak{N}(\alpha)$. W.l.o.g. we may assume that $\mathfrak{N}(\rho) \neq p$ and it follows immediately from Lemma 7 that $E(\rho) \subset F$.

When $\mathfrak{N}(\rho)>(2 p+1) \mathfrak{N}(\alpha)$, repeated application of Lemma 6 assures us that there exists a $k$ such that all prime divisors of $\vartheta_{k}(\rho)$ have norm less than $(2 p+1) \mathfrak{N}(\alpha)$. Therefore by (1) the result follows.

Corollary. For all $\alpha$ the kernel $K$ is finite.

## References

[1] I. KÁtai, Some problems on the iteration of multiplicative number-theoretical functions, Acta Math. Acad. Sc. Hung. 19 (1968), 441-450.
[2] I. KÁtai, On the iteration of multiplicative functions, Publ. Math. Debrecen 36 (1989), 129-134.
[3] R.M. Pollack, H.N. Shapiro and G.H. Sparer, On the graphs of I. Katai, Communications on Pure and Applied Mathematics 27 (1974), 669-713.
M. VAN ROSSUM-WIJSMULLER

DEPARTMENT OF MATHEMATICAL SCIENCES
LA SALLE UNIVERSITY,
PHILADELPHIA, PA. 19141-1199.
(Received October 31, 1991)

