Structure of associated sets to Midy’s property

John H. Castillo    Gilberto García-Pulgarín
Universidad de Nariño  Universidad de Antioquia

Juan Miguel Velásquez-Soto
Universidad del Valle

Received Oct. 10, 2011  Accepted Feb. 14, 2012

Abstract
Let $b$ be a positive integer greater than 1, $N$ a positive integer relatively prime to $b$, $|b|_N$ the order of $b$ in the multiplicative group $U_N$ of positive integers less than $N$ and relatively primes to $N$, and $x \in U_N$. It is well known that when we write the fraction $\frac{x}{N}$ in base $b$, it is periodic. Let $d, k$ be positive integers with $d \geq 2$ and such that $|b|_N = dk$ and $\frac{x}{N} = 0.a_1a_2\cdots a_{|b|_N}$ with the bar indicating the period and $a_i$ are digits in base $b$. We separate the period $a_1a_2\cdots a_{|b|_N}$ in $d$ blocks of length $k$ and let $A_j = [a_{(j-1)k+1}a_{(j-1)k+2}\cdots a_{jk}]_b$ be the number represented in base $b$ by the $j-th$ block and $S_d(x) = \sum_{j=1}^{d} A_j$. If for all $x \in U_N$, the sum $S_d(x)$ is a multiple of $b^k - 1$ we say that $N$ has Midy’s property for $b$ and $d$.

In this work we present some interesting properties of the set of positive integers $d$ such that $N$ has Midy’s property for $b$ and $d$.

Keywords: Period, decimal representation, order of an integer, multiplicative group of units modulo $N$

MSC(2000): 11A05, 11A07, 11A15, 11A63, 16U60

1 Introduction
Let $b$ be a positive integer greater than 1, $b$ will denote the base of numeration, $N$ a positive integer relatively prime to $b$, i.e $(N, b) = 1$, $|b|_N$ the order of $b$ in the multiplicative group $U_N$ of positive integers less than $N$ and relatively primes to $N$, and $x \in U_N$. It is well known that when we write the fraction $\frac{x}{N}$ in base $b$, it is periodic. By period we mean the smallest repeating sequence of digits in base $b$ in such expansion, it is easy to see that $|b|_N$ is the length of the period of the fractions $\frac{x}{N}$ (see Exercise 2.5.9 in [6]). Let $d, k$ be positive integers with $d \geq 2$ and such that $|b|_N = dk$ and $\frac{x}{N} = 0.a_1a_2\cdots a_{|b|_N}$ with the bar indicating the period and $a_i$ are digits in base $b$. We separate the period $a_1a_2\cdots a_{|b|_N}$ in $d$ blocks of length $k$ and let

$$A_j = [a_{(j-1)k+1}a_{(j-1)k+2}\cdots a_{jk}]_b$$

be the number represented in base $b$ by the $j-th$ block and $S_d(x) = \sum_{j=1}^{d} A_j$. If for all $x \in U_N$, the sum $S_d(x)$ is a multiple of $b^k - 1$ we say that $N$ has Midy’s
property for $b$ and $d$. It is named after E. Midy (1836), to read historical aspects about this property see [2] and its references.

If $D_b(N)$ is the number in base $b$ represented by the period of $\frac{1}{N}$, this is $D_b(N) = [a_1a_2 \cdots a_{|b|_N}]_b$, it is easy to see that $ND_b(N) = b^{|b|_N} - 1$. We denote with $\mathcal{M}_b(N)$ the set of positive integers $d$ such that $N$ has Midy’s property for $b$ and $d$ and we will call it Midy’s set of $N$ to base $b$. As usual, let $\nu_p(N)$ be the greatest exponent of $p$ in the prime factorization of $N$.

For example 13 has Midy’s property to the base 10 and $d = 3$, because $|13|_{10} = 6$, $1/13 = 0.076923$ and $07 + 69 + 23 = 99$. Also, 49 has Midy’s property to the base 10 and $d = 14$, since $|49|_{10} = 42$,

$$1/49 = 0.020408163265306122448979591836734693877551$$

and $020+408+163+265+306+122+448+979+591+836+734+693+877+551 = 7 * 999$. But 49 does not have Midy’s property to 10 and 7. Actually, we can see that $\mathcal{M}_{10}(13) = \{2, 3, 6\}$ and $\mathcal{M}_{10}(49) = \{2, 3, 6, 14, 21, 42\}$.

In [1] are given the following characterizations of Midy’s property.

**Theorem 1.** Let $N, b$ and $d$ as above, $d \in \mathcal{M}_b(N)$ if and only if $D_b(N) \equiv 0 \pmod{b^k - 1}$. Furthermore, if $d \in \mathcal{M}_b(N)$ and $D_b(N) = (b^k - 1)t$, for some integer $t$, then $b^{|b|_N} - 1 = (b^k - 1)Nt$.

**Theorem 2.** Let $N, b$ and $d$ as above, $d \in \mathcal{M}_b(N)$ if and only if for all prime $p$ divisor of $N$ it satisfies that if $|b|_p | k$, then $\nu_p(N) \leq \nu_p(d)$. Furthermore, if $d \in \mathcal{M}_b(N)$, then $\sum_{i=1}^{d} (b^{ik} \mod N) = m_b(d, N) N$.

**Theorem 3.** Let $N, b$ and $d$ as above, $d \in \mathcal{M}_b(N)$ if and only if for all prime $p$ divisor of $(b^k - 1, N)$ it satisfies that $\nu_p(N) \leq \nu_p(d)$.

2 Structure of $\mathcal{M}_b(N)$

Theorem 2 tells us that the subgroup generated by $b^k$ in $\mathbb{U}_N$, $\langle b^k \rangle = \{b^{jk} : j = 0, 1, \ldots, d - 1\}$; is the key of a method to obtain the value of the multiplier $m_b(d, N)$, because if $d \in \mathcal{M}_b(N)$, then

$$Nm_b(d, N) = \sum_{i=1}^{d} (b^{ik} \mod N).$$

The following result shows an interesting relationship between $\langle b^{k_2} \rangle$ and $\langle b^{k_1} \rangle$ when $k_2 \mid k_1$.

**Theorem 4.** If $|b|_N = k_1d_1 = k_2d_2$ and $d_2 = cd_1$ for some integer $c \in \mathbb{Z}$; then

$$\langle b^{k_2} \rangle = \bigcup_{r=0}^{c-1} \left( b^{rk_2} \langle b^{k_1} \rangle \right)$$

where $b^{rk_2} \langle b^{k_1} \rangle = \{b^{rk_2}x : x \in \langle b^{k_1} \rangle \}$. 
Proof. Since \(d_2 = cd_1\) the \(d_2\) values of \(j \in \{0, 1, \ldots, d_2 - 1\}\) can be divided by \(c\) obtaining a quotient between 0 and \(d_1 - 1\) and a remainder between 0 and \(c - 1\), in consequence this values are the numbers \(ci + r\) with \(0 \leq i \leq d_1 - 1\) and \(0 \leq r \leq c - 1\). Thus

\[
\langle b^{k_2} \rangle = \left\{ b^{j_{k_2}} : j = 0, 1, \ldots, d_2 - 1 \right\} = \left\{ b^{k_2(ci+r)} : i = 0, 1, \ldots, d_1 - 1, \ r = 0, 1, \ldots, c - 1 \right\} = \left\{ b^{k_1i+r} : i = 0, 1, \ldots, d_1 - 1, \ r = 0, 1, \ldots, c - 1 \right\} = \bigcup_{r=0}^{c-1} \left( b^{r} \langle b^{k_1} \rangle \right)
\]

We get the following result as a consequence of the above fact.

**Corollary 1.** Let \(d_1, d_2\) be divisors of \(|b|_N\) and assume that \(d_1 | d_2\) and \(d_1 \in \mathcal{M}_b(N)\), then \(d_2 \in \mathcal{M}_b(N)\).

The following result is a dual version of this corollary.

**Proposition 1.** Let \(N_1, N_2\) and \(d\) be integers such that \(d\) is a common divisor of \(|b|_{N_1}\) and \(|b|_{N_2}\), if \(d \in \mathcal{M}_b(N_2)\) and \(N_1 | N_2\) then \(d \in \mathcal{M}_b(N_1)\).

**Proof.** In fact, as \(N_1 | N_2\), if \(|b|_{N_2} = k_2d\) then \(|b|_{N_1} = k_1d\) with \(k_1 | k_2\). Thus \((b^{k_1} - 1, \ N_1) \ | \ (b^{k_2} - 1, \ N_2)\) and the result follows from Theorem 2 and from the fact that \(d \in \mathcal{M}_b(N_2)\). \(\Box\)

**Theorem 5.** If \(2 \in \mathcal{M}_b(N)\) and \(d\) divides \(|b|_N\) with \(d\) even, then \(d \in \mathcal{M}_b(N)\) and \(m_b(d, \ N) = \frac{d}{2}\).

**Proof.** In Theorem 4, letting \(d_1 = 2\), \(k_1 = \frac{|b|_N}{2}\), \(d_2 = d\) and therefore \(c = \frac{d}{2}\) and \(\langle b^{k_1} \rangle = \{1, \ N-1\}\) we obtain that \(\langle b^{k_2} \rangle\) is formed by \(c\) translations of \(\{1, \ N-1\}\) and so the sum of its elements is \(cN\), thus we have \(m_b(d, \ N) = c = \frac{d}{2}\). \(\Box\)

The hypothesis \(2 \in \mathcal{M}_b(N)\) is essential, as is shown in the following example due to Lewittes, see [2].

**Example 1.** Let \(N = 7 \times 19 \times 9901\), so \(|10|_N = 36\) and, in addition, \(N\) does not have M¨idy’s property for the base 10 and for any \(d = 2, 3, 6\); but it has this property when \(d = 4, 9, 12, 18\) and \(36\) and \(m_{10}(12, \ N) = 7\).

Next theorem has a big influence in our work.
Theorem 6 (Theorem 3.6 in [6]). Let $p$ be an odd prime not dividing $b$, $m = \nu_p(b^{[b]} - 1)$ and let $t$ be a positive integer, then

$$\left\{ \begin{array}{ll} |b|_p & \text{if } t \leq m, \\
p^{t-m}|b|_p & \text{if } t > m. \end{array} \right.$$  

For the base $b = 10$ the greatest $m$ known is 2, which is achieved with the primes 3, 487 and 56598313, see [4]. From the same paper we take the following example: if $b = 68$ and $p = 113$, then $|b|_p = |b|_{p^2} = |b|_{p^3}$. Something similar occurs for $b = 42$ and $p = 23$. For $m = 3$, these are the only cases with $p < 2^{32}$ and $2 \leq b \leq 91$.

Next theorem allows us to build $\mathcal{M}_b(p^n)$ from $\mathcal{M}_b(p)$.

Theorem 7. Let $b$, $p$, $n$ be integers where $p$ is a prime not dividing $b$, and $n$ positive. Let $m = \nu_p(b^{[b]} - 1)$, then

$$\mathcal{M}_b(p^n) = \bigcup_{i=0}^{n-m} p^{n-m-i} \mathcal{M}_b(p)$$  

Therefore:

$$|\mathcal{M}_b(p^n)| = \left\{ \begin{array}{ll} |\mathcal{M}_b(p)| & \text{if } n \leq m, \\
(n-m+1)|\mathcal{M}_b(p)| & \text{if } n > m. \end{array} \right.$$  

Proof. Let $|b|_p = kd$ and $d \in \mathcal{M}_b(p)$ then $(b^k - 1, p) = 1$. Suppose that $n \leq m$, as $(b^k - 1, p^n) = 1$ and $|b|_{p^n} = |b|_p = kd$ follows that $d \in \mathcal{M}_b(p^n)$ and thus $\mathcal{M}_b(p) \subset \mathcal{M}_b(p^n)$. It is also easy to prove that $\mathcal{M}_b(p^n) \subset \mathcal{M}_b(p)$.

We now consider the case when $n > m$. Let $d \in \mathcal{M}_b(p)$ and $|b|_p = kd$, and let $i$ be an integer with $0 \leq i \leq n - m$, by Theorem 6 we have $|b|_{p^n} = p^{n-m}|b|_p = kp^i(p^{n-m-i}d)$. We affirm that $(b^{kp^i} - 1, p^n) = 1$ because $b^{kp^i} \equiv (b^k)^{p^i} \equiv b^k \mod p \neq 1 \mod p$. As $(b^{kp^i} - 1, p^n) = 1$ and $|b|_{p^n} = kp^i(p^{n-m-i}d)$ it follows from Theorem 3 that $p^{n-m-i}d \in \mathcal{M}_b(p^n)$. In this way we have proved that $p^{n-m-i} \mathcal{M}_b(p) \subset \mathcal{M}_b(p^n)$.

Similarly, we can show that $\mathcal{M}_b(p^n) \subset p^{n-m-i} \mathcal{M}_b(p)$. The second part of the theorem is a direct consequence from the first part.

Theorem 3 says that if $p$ is prime and $d > 1$ is a divisor of $|b|_p$, then $d \in \mathcal{M}_b(p)$ and therefore $|\mathcal{M}_b(p)| = \tau(o_p(b)) - 1$, where $\tau(n)$ denote the number of positive divisors of $n$.

Theorem 8. Let $N$, $M$ be integers such that $|b|_M = |b|_N$, then

1. $\mathcal{M}_b(MN) \subseteq \mathcal{M}_b(N)$.  

2. If $N$ and $M$ are relatively primes, then

$$\mathcal{M}_b(MN) = \left\{ d \in \mathcal{M}_b(N) : |b|_N = kd \text{ and } \forall (r \text{ primo})(r | (b^k - 1, M) \Rightarrow \nu_r(M) \leq \nu_r(d) \right\}.$$ 

3. In particular, if $p$ is a prime not dividing $N$, $|b|_p$ is a divisor of $|b|_N$, and $s = \nu_p(|b|_N)$, then

$$\mathcal{M}_b(p^{s+1}N) = \left\{ d \in \mathcal{M}_b(N) : |b|_N = kd \text{ and } (b^k - 1, p) = 1 \right\}.$$

**Proof.** To prove the first part we show that if $d \notin \mathcal{M}_b(N)$, then $d \notin \mathcal{M}_b(MN)$. In fact, as $|b|_N = |b|_M = kd$ and $d \notin \mathcal{M}_b(N)$ from Theorem 3, there exists a prime $q$, divisor of $(b^k - 1, N)$ such that $\nu_q(N) > \nu_q(d)$. As $(b^k - 1, N)$ is a divisor of $(b^k - 1, MN)$ and $\nu_q(MN) \geq \nu_q(N)$ Theorem 3 guarantees that $d \notin \mathcal{M}_b(MN)$.

We now add the hypothesis $(M, N) = 1$ and let $|b|_N = |b|_MN = kd$ with $d \in \mathcal{M}_b(N)$. Consider a prime $r$ divisor of $(b^k - 1, MN)$. Since $M$ and $N$ are relatively primes then either $r | (b^k - 1, M)$ or $r | (b^k - 1, N)$, but not both. If $r | (b^k - 1, N)$, as $d \in \mathcal{M}_b(N)$ from Theorem 3 follows that $\nu_r(N) \leq \nu_r(d)$ and as $M$ and $N$ are relatively primes we have $\nu_r(N) = \nu_r(MN)$ and therefore $d \in \mathcal{M}_b(MN)$. If $r | (b^k - 1, M)$, as $r \nmid N$, we have $\nu_r(MN) = \nu_r(M)$ and from the assumption and Theorem 3 we get that $d \in \mathcal{M}_b(MN)$. The third part now is clear, because $|b|_{p^{s+1}}$ is a divisor of $|b|_N$ and $p$ and $N$ are relatively primes. \qed

**Theorem 9.** Let $N$, $p$ be integers with $(N, b) = 1$ with $p$ a prime divisor of $b - 1$. Then there exists a positive integer $s$ such that for all integer $t$, with $t > s$, we have $\mathcal{M}_b(p^tN) = \emptyset$.

**Proof.** Without loss of generality we can suppose that $p$ is not a divisor of $N$. Let $s = \nu_p(|b|_N)$, as $|b|_p = 1$ we are in the conditions of the third part of Theorem 8 and the result is immediately because $(b^k - 1, p) = p$ for any $k$. \qed

The result of previous theorem is true for any divisor $n$, not necessarily a prime, of $b - 1$. Also note that the value of the integer $s - \nu_p(N)$ is the smallest that satisfies the theorem because $\mathcal{M}_b(p^{s-\nu_p(N)}N)$ is non empty by the second part of Theorem 8.

We now study the following question. Given $N$ and $b$ with $\mathcal{M}_b(N) \neq \emptyset$, is it possible to find a positive integer $z$ such that $\mathcal{M}_b(zN) = \{|b|_N\}$? The next result, from [5], will be useful in the sequel.

**Lemma 1** (Corollary 2 in [5]). Let $b \geq 2$ and $n \geq 2$. Then there exists a prime $p$ with $n = |b|_p$ in all except the following pairs: $(n, b) = (2, 2^\gamma - 1)$ with $\gamma \geq 2$ or $(6, 2)$.

To answer the question we will need the following result.
Lemma 2. Let $N$ and $b$ be integers such that $\mathcal{M}_b(N) \neq \emptyset$. Let $q$ a prime divisor of $|b|_N$. Then there exists a positive integer $z$ that satisfies the following properties

1. $|b|_z = |b|_N$,
2. $\mathcal{M}_b(zN) \neq \emptyset$,
3. If $d \in \mathcal{M}_b(zN)$, then $\nu_q(d) = \nu_q(|b|_N)$.

Proof. We will study two cases

1.) Assume that either $q \neq 2$ or $b+1$ is not a power of 2. From Lemma 1 there exists an odd prime $p$ such that $|b|_p = q$. In the sequel, we denote with $c = \nu_p(N)$, $s = \nu_p(|b|_N)$ and $m = \nu_p(b^q - 1)$. If $p$ is not a divisor of $N$, from the third part of Theorem 8, we have when $d \in \mathcal{M}_b(zN)$, then $|b|_N = kd$ and $(b^k - 1, p) = 1$. Hence if $d \in \mathcal{M}_b(zN)$, then $\nu_q(d) = \nu_q(|b|_N)$. Thus, in this case, we take $z = p^{s+1}$. Since $(b - 1, zN) = (b - 1, N)$ and $|b|_N \in \mathcal{M}_b(N)$ we have $|b|_N \in \mathcal{M}_b(zN)$.

From now we suppose that $p$ is a divisor of $N$. Thus $c > 0$ and $N = p^cM$ with $M$ non divisible by $p$. We consider the following cases:

1. $c \geq s + 1$. Let $d \in \mathcal{M}_b(N)$ where $|b|_N = kd$, if $p$ divides $b^k - 1$, then from Theorem 3 it follows that $c = \nu_p(N) \leq \nu_p(d) \leq s$, which is a contradiction. In consequence, we get that $d \in \mathcal{M}_b(N)$, implies that $|b|_N = kd$ and $\nu_q(d) = \nu_q(|b|_N)$ and we take $z = 1$.

2. $c < s + 1$. We consider two subcases, depending if either $q$ is or not a divisor of $|b|_M$.

Firstly, we assume that $q \mid |b|_M$. Since $|b|_N = \left[|b|_p, |b|_M\right]$ and $|b|_{p^{s+1}M} = \left[|b|_{p^{s+1}}, |b|_M\right]$ from Theorem 6, $|b|_N = [qp^\delta, |b|_M]$ and $|b|_{p^{s+1}M} = [qp^\epsilon, |b|_M]$; where $\delta = \max(0, c - m)$ and $\epsilon = \max(0, s - m + 1)$.

We claim that $|b|_{p^{s+1}M} = |b|_N = |b|_M$. In fact, since $|b|_N = [qp^\delta, |b|_M]$, $s = \nu_p(|b|_N)$ and $\delta < s$, we obtain that $\nu_p(|b|_M) = s$ and hence $|b|_N = |b|_M$. Also as $\epsilon \leq s$, we get that $|b|_{p^{s+1}M} = |b|_M$.

By the third part of Theorem 8 we have $d \in \mathcal{M}_b(p^{s+1}M)$, implies that $\nu_q(d) = \nu_q(|b|_N)$. So we take $z = p^{s-c+1}$. Again, as $(b - 1, zN) = (b - 1, N)$ and $|b|_N \in \mathcal{M}_b(N)$, then $|b|_N \in \mathcal{M}_b(zN)$.

Assume that $q \nmid |b|_M$. Similar as in the above paragraph we can show that $|b|_{p^{s+1}M} = |b|_N = q|b|_M$. We affirm that

$$\mathcal{M}_b(p^{s+1}M) = \{d'q : d' \in \mathcal{M}_b(M)\}.$$
Let $d \in \mathcal{M}_b(p^{s+1}M)$. Since $|b|_{p^{s+1}M} = q |b|_M$ we have $d$ is either a divisor of $|b|_M$ or $d = q$ or $d = d'q$ where $d' > 1$ is a divisor of $|b|_M$. If $d$ is a divisor of $|b|_M$ with $|b|_M = kd$, then as $p$ divides $(b^{kq} - 1, p^{s+1}M)$ and $s+1 = \nu_p(p^{s+1}M) > \nu_p(d)$ by Theorem 3 we obtain that $d \notin \mathcal{M}_b(p^{s+1}M)$. Now assume that $d = q$. Since $p$ divides $|b|_M$ there exists a prime $r$ divisor of $(b^{b|_M} - 1, p^{s+1}M)$, with $r \neq q$. By Theorem 3 we get a contradiction.

Finally if $d = d'q$ with $|b|_M = kd'$, it is easy to see that $d \in \mathcal{M}_b(p^{s+1}M)$ implies that $d' \in \mathcal{M}_b(M)$.

Thus, in this case we take $z = p^{s-c+1}$. We showed that if $d \in \mathcal{M}_b(zN)$, then $d = d'q$ where $|b|_N = kd$, $d' \in \mathcal{M}_b(M)$ and $\nu_q(d) = \nu_q(|b|_N)$. Since $|b|_M \in \mathcal{M}_b(M)$ then $|b|_N = q |b|_M \in \mathcal{M}_b(zN)$.

2.) Assume that $q = 2$ and $b = 2^\gamma - 1$ for some positive integer $\gamma \geq 2$. We know, from Lemma 1, that we can not find a prime $p$ such that $|b|_p = 2$. So we follow a different procedure in this case. It is clear that $|b|_q = |b|_2 = 1$. Let $s = \nu_2(|b|_N)$ and $c = \nu_2(N)$. Note that $c$ can not be strictly greater than $s$, because 2 divides $(b^k - 1, N)$ and $\mathcal{M}_b(N) \neq \emptyset$. We study the following cases:

1. $c = s$. By the assumption $c > 0$. Suppose that there exists a $d \in \mathcal{M}_b(N)$ such that $k$ is even. Thus $\nu_2(d) < s$. As 2 divides $(b^k - 1, N)$ from Theorem 3 we have $c = \nu_2(N) \leq \nu_2(d)$ which is a contradiction. Therefore, it is enough to take $z = 1$.

2. $s > c$. In this case we take $z = 2^{s-c}$. Since $|b|_{2^s}$ divides $2^{s-1}$, then $|b|_{zN} = [|b|_{2^s}, |b|_M] = |b|_M = |b|_N$. Hence, $\mathcal{M}_b(zN) = \{d \in \mathcal{M}_b(N) : |b|_N = kd \text{ and } \nu_2(d) = \nu_2(|b|_N)\}$.

Indeed, from Theorem 3 we have $d \in \mathcal{M}_b(N)$ is an element of $\mathcal{M}_b(zN)$ if and only if $s = \nu_2(zN) \leq \nu_2(d)$ and this is equivalent to say that $\nu_2(d) = s$. Since $|b|_N \in \mathcal{M}_b(N)$ and $s = \nu_2(|b|_N)$, we have $|b|_N \in \mathcal{M}_b(zN)$.

\[\square\]

**Theorem 10.** Let $N$ and $b$ be integers such that $|\mathcal{M}_b(N)| > 1$. Then, there exists a positive integer $z$ such that $\mathcal{M}_b(zN) = \{|b|_N\}$.

**Proof.** Let $|b|_N = q_1^{l_1} \ldots q_i^{l_i}$ be the prime factorization of $|b|_N$.

Applying Lemma 2 to $q_1$ and $N$ we can find a positive integer $z_1$ such that $|b|_{z_1N} = |b|_N$, $\mathcal{M}_b(z_1N) \neq \emptyset$ and when $d \in \mathcal{M}_b(z_1N)$, then $\nu_{q_1}(d) = \nu_{q_1}(|b|_N)$. Again using Lemma 2 with $q = q_2$ and $z_1N$, we get a positive integer $z_2$ such that $|b|_{z_1z_2N} = |b|_N$, $\mathcal{M}_b(z_1z_2N) \neq \emptyset$, and $d \in \mathcal{M}_b(z_1z_2N)$, implies that $\nu_{q_2}(d) = \nu_{q_2}(|b|_N)$. From Theorem 8 we know that $\mathcal{M}_b(z_1z_2N) \subseteq \mathcal{M}_b(z_1N)$. In this way for each $d \in \mathcal{M}_b(z_1z_2N)$ we also have that $\nu_{q_1}(d) = \nu_{q_1}(|b|_N)$.

Repeating this process we get positive integers $z_1, \ldots, z_l$ such that if $z = \prod_{i=1}^l z_i$, the following properties hold...
1. $|b|_{zN} = |b|_N$,
2. $\mathcal{M}_b(zN) \neq \emptyset$,
3. If $d \in \mathcal{M}_b(zN)$, then $\nu_{q_i}(d) = \nu_{q_i}(|b|_N)$ for all $i \in \{1, \ldots, l\}$.

Since the $q_i$’s are the prime factors of $|b|_N$, we conclude that $d = |b|_N$ and therefore $\mathcal{M}_b(zN) = \{|b|_N\}$.

Acknowledgements

The authors are members of the research group: Álgebra, Teoría de Números y Aplicaciones, ERM. J.H. Castillo was partially supported by CAPES, CNPq from Brazil and Universidad de Nariño from Colombia. J.M. Velásquez-Soto was partially supported by CONICET from Argentina and Universidad del Valle from Colombia.

References


Authors’ address

John H. Castillo — Departamento de Matemáticas y Estadística, Universidad de Nariño, San Juan de Pasto-Colombia

Gilberto García-Pulgarín — Departamento de Matemáticas, Universidad de Antioquia, Medellín-Colombia

Juan Miguel Velásquez-Soto — Departamento de Matemáticas, Universidad del Valle, Cali-Colombia