ON A PARTICULAR CASE OF THE DIRICHLET’S THEOREM AND THE MIDY’S PROPERTY

JOHN H. CASTILLO, GILBERTO GARCÍA-PULGARÍN, AND JUAN MIGUEL VELÁSQUEZ-SOTO

Abstract. We give new characterizations of the Midy’s property and using these results we obtain a new proof of a special case of the Dirichlet’s theorem about primes in arithmetic progression.

1. Preliminaries

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 $\mathbb{U}_N$ of positive integers less than $N$ and relatively primes to $N$, and $x \in \mathbb{U}_N$. 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 [Nat00]). Let $d, k$ be positive integers with $|b|_N = dk$, $d > 1$ and $x = \frac{a_1a_2 \cdots a_{|b|_N}}{b}$, where the bar indicate the period and $a_i$’s 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 $x \in \mathbb{U}_N$, the sum $S_d(x)$ is a multiple of $b^k - 1$ we say that $N$ has the Midy’s property for $b$ and $d$. It is named after E. Midy (1836), to read historical aspects about this property see [Lew07] and its references.

We denote with $\mathcal{M}_b(N)$ the set of positive integers $d$ such that $N$ has the Midy’s property for $b$ and $d$. It is named after E. Midy (1836), to read historical aspects about this property see [Lew07] and its references.

As usual, let $\nu_p(N)$ be the greatest exponent of $p$ in the prime factorization of $N$.

For example 13 has the Midy’s property to the base 10 and $d = 3$, because $|13|_{10} = 6$, $1/13 = 0.076923$ and $0 + 7 + 6 + 9 + 2 + 3 = 29$. Also, 75 has the Midy’s property to the base 8 and $d = 4$, since $|75|_8 = 20$, $1/75 = [0.0066472015164033235]_8$ and $[00664]_8 + [72015]_8 + [51640]_8 + [33235]_8 = 2 * (8^5 - 1)$. But 75 does not have the Midy’s property to 8 and 5. Actually, we can see that $\mathcal{M}_{10}(13) = \{2, 3, 6\}$ and $\mathcal{M}_{8}(75) = \{4, 20\}$.  

2000 Mathematics Subject Classification. 11A05, 11A07, 11A15, 11A63, 16U60.
In \cite{GPG09} is given the following characterization of Midy’s property.

**Theorem 1.** If $N$ is a positive integer and $|b|_N = kd$, then $d \in M_b(N)$ if and only if $\nu_p(N) \leq \nu_p(d)$ for all prime divisor $p$ of $(b^k - 1, N)$.

The next theorem is a different way to write Theorem 1.

**Theorem 2.** Let $N$ be a positive integer and $d$ a divisor of $|b|_N$. The following statements are equivalent

1. $d \in M_b(N)$
2. For each prime divisor $p$ of $N$ such that $\nu_p(N) > \nu_p(d)$, there exists a prime $q$ divisor of $|b|_N$ that satisfies $\nu_q(|b|_p) > \nu_q(|b|_N) - \nu_q(d)$.

In \cite{CGPVS11} the authors prove the following theorem.

**Theorem 3.** Let $d_1, d_2$ be divisors of $|b|_N$ and assume that $d_1 \mid d_2$ and $d_1 \in M_b(N)$, then $d_2 \in M_b(N)$.

The following result has a big influence on our work, it is Theorem 3.6 in \cite{Nat00}.

**Theorem 4.** Let $p$ be an odd prime not divisor of $b$, $m = \nu_p(b^{b^p} - 1)$ and let $t$ a positive integer, then

$$|b|_p^t = \begin{cases} |b|_p & \text{if } t \leq m, \\ p^{t-m} |b|_p & \text{if } t > m. \end{cases}$$

The Dirichlet’s theorem about primes in arithmetic progression states that there are infinitely many primes in any arithmetic progression of initial term $a$ and common difference $l$, with $(a, l) = 1$. It was conjectured by Carl Friedrich Gauss and it was first proved in 1826 by Peter Gustav Lejeune Dirichlet. The theorem which establishes that there are infinitely many primes is a particular case of the Dirichlet’s theorem, taking $a = 1$ and $l = 1$.

A related result, to the Dirichlet’s theorem, proved by B. Green and T. Tao in 2004, guarantees that we can find lists of primes in arithmetic progression of arbitrary length; see \cite{GT04}.

The biggest list of primes in arithmetic progression has 26 terms, it was founded in April 12, 2010 by Benot Perichon and PrimeGrid. It is formed by the numbers $43142746595714191 + 23681770 \cdot 23\# \cdot n$, for $0 \leq n \leq 25$ where $a\#$ denotes the primorial of $a$, it is the product of all primes less or equal to $a$; see \cite{And12}.

## 2. Other characterizations of Midy’s Property.

In this section, we will study some consequences of Theorem 2.
Theorem 5. Let $N$ be a positive integer and $|b|_N = kd$. If, for all prime divisor $p$ of $N$, we have $\nu_p (N) > \nu_p (d)$, then the following statements are equivalent

1. $(b^k - 1, N) = 1$
2. $d \in M_b(N)$
3. For each prime divisor $p$ of $N$, there exists a prime $q$ divisor of $d$ such that $\nu_q (|b|_p) > \nu_q (|b|_N) - \nu_q (d)$.

Proof. The equivalence between (2) and (3) is immediate from Theorem 2.

By Theorem 1 we get that (1) implies (2). Now we prove that (2) implies (1). Suppose that $d \in M_b(N)$ and let $g = (b^k - 1, N)$. If there exists a prime divisor $p$ of $g$, from Theorem 1 we have $0 < \nu_p (N) \leq \nu_p (d)$ and this is impossible because $\nu_p (d) < \nu_p (N)$. Therefore $(b^k - 1, N) = 1$. \hspace{1cm} \square

We now will study Theorem 4 of [Lew07], which is attributed by its author to M. Jenkins (1867). Let $p_1, p_2, \ldots, p_t$ be different primes such that $d \in M_b(p_i)$ for each $i$ and let $h_1, h_2, \ldots, h_t$ be positive integers, when does $N = p_1^{h_1} p_2^{h_2} \cdots p_t^{h_t}$ have the Midy’s property for $b$ and $d$? The Jenkins’ Theorem gives the answer to this question and the same is independent from the $h_i$’s.

By simplicity we go to study the case when $t = 3$, but the argument is true for any $t$. Let $p_1, p_2, p_3$ be different primes such that $d \in M_b(p_i)$, $|b|_{p_i} = dk_i$, $m_i = \nu_{p_i} (b^{dk_i} - 1)$ for $i = 1, 2, 3$ then

$$|b|_N = d \left[ p_1^{h_1-m_1}k_1, p_2^{h_2-m_2}k_2, p_3^{h_3-m_3}k_3 \right] = dk.$$

We have to check up the prime divisors of $(b^k - 1, N)$, to determine when $d \in M_b(N)$. As $d$ is a divisor of $|b|_{p_1}$ thus $d \leq p_1 - 1$ and if, say, $p_1 \mid (b^k - 1, N)$ we get that $h_1 = \nu_{p_1} (N) > 0 = \nu_{p_1} (d)$ and so $N$ does not have the Midy’s property for $b$ and $d$. In consequence $d \in M_b(N)$ if and only if $(b^k - 1, N) = 1$. It is clear that $(b^k - 1, N) = 1$ is equivalent to say that for each $i$, $|b|_{p_i} \nmid k$. We will see when this fact is verified. Let $d = \prod_{i=1}^{s} q_i^{n_i}$ be the prime decomposition of $d$, for each $i = 1, 2, 3$ take $c_i = \nu_{q_i} (k_i)$ and

$$p_1^{h_1-m_1}k_1 = \left( d^{c_1} \prod_{i=1}^{s} q_i^{c_i} \right) y_1$$

$$p_2^{h_2-m_2}k_2 = \left( d^{c_2} \prod_{i=1}^{s} q_i^{c_i} \right) y_2$$

$$p_3^{h_3-m_3}k_3 = \left( d^{c_3} \prod_{i=1}^{s} q_i^{c_i} \right) y_3$$
where \((q_i, y_j) = 1\) for \(i = 1, 2, \ldots, s\) and \(j = 1, 2, 3\). Then

\[
 k = \left[ p^{h_1-m_1}k_1, p^{h_2-m_2}k_2, p^{h_3-m_3}k_3 \right] = \left[ d^c \prod_{i=1}^{s} q_i^{\alpha_i^{(1)}}, d^{c^2} \prod_{i=1}^{s} q_i^{\alpha_i^{(2)}}, d^{c^3} \prod_{i=1}^{s} q_i^{\alpha_i^{(3)}} \right] [y_1, y_2, y_3].
\]

We want, as was said before, that \(k\) not be divisible for any \(|b|_{p_i}, i = 1, 2, 3\). Now if, say, \(k = |b|_{p_1} l\) with \(l\) integer, then \(k = |b|_{p_1} l = (k_1 d) l\) therefore \(k/l\) is a multiple of \(d\), and as the \(y_s\)'s are relatively primes with \(d\) this is equivalent to

\[
\frac{d^c \prod_{i=1}^{s} q_i^{\alpha_i^{(1)}}, d^{c^2} \prod_{i=1}^{s} q_i^{\alpha_i^{(2)}}, d^{c^3} \prod_{i=1}^{s} q_i^{\alpha_i^{(3)}}}{d^c \prod_{i=1}^{s} q_i^{\alpha_i^{(1)}}} \equiv 0 \mod d.
\]

From the above analysis follows the next theorem.

**Theorem 6 (Jenkins' Theorem).** Let \(p_1, p_2, \ldots, p_t\) be different primes such that \(d \in M_0(p_i)\) for each \(i\), let \(h_1, h_2, \ldots, h_t\) be positive integers and \(N = p_1^{h_1} p_2^{h_2} \cdots p_t^{h_t}\). With the notations introduced above we obtain that \(d \in M_0(N)\) if and only if, for each \(j = 1, 2, \ldots, t\) is satisfied

\[
\frac{d^c \prod_{i=1}^{s} q_i^{\alpha_i^{(1)}}, d^{c^2} \prod_{i=1}^{s} q_i^{\alpha_i^{(2)}}, \ldots, d^{c^t} \prod_{i=1}^{s} q_i^{\alpha_i^{(t)}}}{d^c \prod_{i=1}^{s} q_i^{\alpha_i^{(1)}}} \not\equiv 0 \mod d.
\]

Our next result has a similar flavor of the Jenkins' Theorem, although its statement and proof are simpler.

**Theorem 7.** Let \(N, q, v\) be integers with \(q\) prime and \(v > 0\). Then \(q^v \in M_0(N)\) if and only if \(N = q^v p_1^{h_1} p_2^{h_2} \cdots p_t^{h_t}\) where \(n\) is a non-negative integer, \(p_i\)'s are different primes and \(h_i\)'s are non-negatives integers not all zero, verifying \(0 \leq n \leq v, \nu_q(|b|_{p_i}) > 0\) and

\[
\max_{1 \leq i \leq t} \left\{ n - m, \nu_q(|b|_{p_i}) \right\} - v < \min_{1 \leq i \leq t} \left\{ \nu_q(|b|_{p_i}) \right\}
\]

where \(m = \nu_q(b^{[b]_q} - 1)\).

**Proof.** We write \(|b|_N = q^t k\), with \((q, k) = 1\) and \(t \geq v\). Let us denote \(g = \left( b^{q^{v-t}} - 1, N \right)\). Suppose that \(g^v \in M_0(N)\). By Theorem 1 we know that \(g\) can not be divisible by other prime different from \(q\) and that \(\nu_q(N) \leq v\). Let \(p \neq q\) be a prime divisor of \(N\). Because \(p\) not divides \(g\), we have \(|b|_p \not\mid q^{t-v}\) and thus \(\nu_q(|b|_p) > t - v \geq 0\) and it is easy to see that \(t = \max_{1 \leq i \leq t} \left\{ n - m, \nu_q(|b|_{p_i}) \right\}\). Therefore for all prime divisor \(p\) of \(N\) we get that

\[
\nu_q(|b|_p) > \max_{1 \leq i \leq t} \left\{ n - m, \nu_q(|b|_{p_i}) \right\} - v.
\]
Conversely, from the hypothesis the unique prime divisor of $N$ that could be a divisor of $g$ is $q$ and thus Theorem 1 implies that $q^v \in M_b(N)$. □

As a special case, if in the above theorem we do $v = 1$ and since for any $p$ prime divisor of $N$ we have $\nu_q(|b|_N) \geq \nu_q(|b|_p)$ and thus we obtain the next corollary.

**Corollary 8.** Let $N$ be a positive integer and let $q$ be a prime divisor of $|b|_N$, then $q \in M_b(N)$ if and only if

1. If $(N, q) = 1$, then $\nu_q(|b|_p) = \nu_q(|b|_N)$ for all $p$ prime divisor of $N$.
2. If $(N, q) > 1$, then $q^2$ not divides $N$ and $\nu_q(|b|_p) = \nu_q(|b|_N)$ for all $p$ prime divisor of $N$ different from $q$.

Note that, from the last theorem, the smallest number $N$ such that $q^v \in M_b(N)$ has to be a prime $P$ which satisfies $\nu_q(|b|_P) > 0$ and $q^v | |b|_P$. We obtain the below corollary, recalling that $|b|_P$ divides $P - 1$.

**Corollary 9.** If $q$ is a prime and $v$ is a positive integer, then the smallest integer $N$ such that $q^v \in M_b(N)$ is a prime congruent with $1$ mod $q^v$.

As a consequence of the above corollary we have a particular case of the Dirichlet’s Theorem about primes in arithmetic progressions.

**Corollary 10.** If $q$ is a prime and $v$ is a positive integer, there are infinitely many primes which are congruent to $1$ modulo $q^v$.

**Proof.** By the last corollary there exists a prime $P_1$ congruent with $1$ modulo $q^v$ and which satisfies $q^v \in M_b(P_1)$. Take $t_1$ an integer such that $q^{t_1v} > P_1$. Once again, we can find a prime $P_2$ congruent with $1$ modulo $q^{t_1v}$ such that $q^{t_1v} \in M_b(P_2)$ and so on. □

**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**

[And12] Jens Kruse Andersen, Primes in arithmetic progression records, retrieved 05 March 2012. URL http://users.cybercity.dk/~dsl522332/math/aprecords.htm (2012).

[CGPVS11] John H. Castillo, Gilberto García-Pulgarín, and Juan Miguel Velásquez-Soto, Structure of associated sets to Midy’s Property, accepted to publication in Matemáticas: Enseñanza Universitaria, arXiv:1110.3308v2 [math.NT] (2011).

[GPG09] Gilberto García-Pulgarín and Hernán Giraldo, Characterizations of Midy’s property, Integers 9 (2009), A18, 191–197. MR MR2506150

[GT04] Ben Green and Terence Tao, The primes contain arbitrarily long arithmetic progressions, arXiv:math/0404188v6 [math.NT] (2004).
[Lew07] Joseph Lewittes, *Midy’s theorem for periodic decimals*, Integers 7 (2007), A2, 11 pp. (electronic). MR MR2282184 (2008c:11004)

[Nat00] Melvyn B. Nathanson, *Elementary methods in number theory*, Graduate Texts in Mathematics, vol. 195, Springer-Verlag, New York, 2000. MR 1732941 (2001j:11001)

John H. Castillo, Departamento de Matemáticas y Estadística, Universidad de Nariño, San Juan de Pasto-Colombia
E-mail address: jhcastillo@gmail.com

Gilberto García-Pulgarín, Universidad de Antioquia, Medellín-Colombia
E-mail address: gigarcia@ciencias.udea.edu.co

Juan Miguel Velásquez-Soto, Departamento de Matemáticas, Universidad del Valle, Cali-Colombia
E-mail address: jumiveso@univalle.edu.co