#A18 INTEGERS 9 (2009), 191-197

CHARACTERIZATIONS OF MIDY'S PROPERTY

Gilberto García-Pulgarín
Universidad de Antioquia, Medellín, Colombia, Grupo de Álgebra, Teoría de Números y Aplicaciones, ERM
gigarcia@member.ams.org

Hernán Giraldo[1]
Universidad de Antioquia, Medellín, Colombia, Grupo de Álgebra, Teoría de Números y Aplicaciones, ERM
heragis@matematicas.udea.edu.co

Received: 5/30/08, Revised: 3/4/09, Accepted: 3/3/09

Abstract

In 1836 E. Midy published in France an article where he showed that if p is a prime number, such that the smallest repeating sequence of digits in the decimal expansion of $\frac{1}{p}$ has an even length, when this sequence is broken into two halves of equal length if these parts are added then the result is a string of 9s. Later, J. Lewittes and H. W. Martin generalized this statement when the length of the smallest repeating sequence of digits is $e = kd$ and the sequence is broken into d blocks of equal length and the expansion is over any number base; that fact was named Midy's property. We will give necessary and sufficient conditions (that are easy to check) for the integer N to satisfy Midy's property.

1. Introduction

By *period* we mean the smallest repeating sequence of digits in the decimal expansion of $\frac{1}{N}$, with N a positive integer. According to [2], E. Midy published in France, in 1836, a paper where he showed that if p is a prime number, such that the decimal expansion of $\frac{1}{p}$ has a period of even length, when the period is broken into two halves of equal length if these parts are added then we get a string of $9's$; this result is called the *property of nines*. For instance, $1/7 = 0.\overline{142857}$, the bar indicating the period, if the period is broken into halves of equal length and then added we get $142 + 857 = 999$. We have a similar situation for $1/19 = 0.\overline{052631578947368421}$ with period length 18 and the halves are 052631578 and 947368421.

The property of nines has gained interest over the last few years, as it is shown by the papers of Gupta and Sury [1], J. Lewittes [2] and the work of H. W. Martin [3]. These last two works generalized this property when the period length is any positive integer e, the period is broken into d blocks, where d is a divisor of e and the expansion of $1/N$ is over any number base.

Let us fix some notation. Let B be an integer greater than 1, B is the number base, and N a positive integer relatively prime to B. We denote by $e = o_N(B)$ the order of B in the multiplicative group $\mathbb{U}_N$, where this group is the set of positive integers less than N and relatively prime to it, and the multiplication is the product modulo N.

We know that e is the period length of x/N, where $x \in \mathbb{U}_N$ (see [2]). Assume $e = kd$ for some integers k and d. Then $\frac{x}{N} = 0.\overline{a_1 a_2 \cdots a_e}$ and the period $a_1 a_2 \cdots a_e$

[1]Partial support from COLCIENCIAS and CODI (Universidad de Antioquia).

can be broken into d blocks of equal length k. Let A_j be the number represented by the base B numeral consisting of the jth block of k B-digits in the period. We denote by $S_d(x) = \sum_{j=1}^{d} A_j$.

With the above notation, if for all $x \in \mathbb{U}_N$ the sum $S_d(x)$ is a multiple of $B^k - 1$ then we say that N has the Midy's property for the base B and the divisor d of e, the period length; in that case we write $N \in M_d(B)$.

We denote by $D_B(N)$ the number represented by the base B numeral consisting of the e B-digits of the period of the fraction $\frac{1}{N}$. It is easy to prove that $ND_B(N) = B^e - 1$.

Using similar methods to those in [1], we shall prove the following characterizations of Midy's property.

Theorem 1. *With the above notation: $N \in M_d(B)$ if and only if $D_B(N) \equiv 0 \pmod{B^k - 1}$. Furthermore, if $N \in M_d(B)$ and $\frac{B^e-1}{B^k-1} = Nt$ for some integer t, then $D_B(N) = (B^k - 1)t$.*

Theorem 2. *Let N, B, $e = kd = o_N(B)$ be as above and p^t be the highest power of p that divide N. Then, $N \in M_d(B)$ if and only if for every prime factor p of N, the following is true: if $o_p(B) \mid k$ then $p^t \mid d$.*

Furthermore, if $N \in M_d(B)$ and $\sum_{i=1}^{d}(B^{ik} \mod N) = rN$ for some integer r, then $\sum_{j=1}^{d} A_j = (B^k - 1)r$.

Theorem 3. *Under the same conditions of Theorem 2, $N \in M_d(B)$ if and only if for every prime divisor p of $\gcd(B^k - 1, N)$, we have $p^t \mid d$.*

2. Previous Results

Theorem 2 of [2] or Theorem 1 of [3], can be written with our notation in the following way.

Theorem 4. *The following are equivalent:*

1. *$N \in M_d(B)$.*
2. *For some $x \in \mathbb{U}_N$, $S_d(x) \equiv 0 \pmod{B^k - 1}$.*
3. *$\frac{B^e-1}{B^k-1} \equiv 0 \pmod{N}$.*

Furthermore, if $B^k - 1$ and N are relatively prime, then $N \in M_d(B)$.

It is clear from part three of this theorem that d cannot be 1, so we always assume $e = kd$ with $d > 1$.

The following result extends Theorem 3 of [3].

Theorem 5. *Let N be a positive integer relatively prime to the number base B and $e = kd$ the period length of $1/N$. If for every prime factor p of N the integer k is not a multiple of the period length of $1/p$ then $N \in M_d(B)$.*

Proof. From our assumption, if p is a prime factor of N, then $\gcd(p, B^k - 1) = 1$ and therefore $\gcd(p^s,\ B^k - 1) = 1$, for every integer s. Thus, $\gcd(N,\ B^k - 1) = 1$ and the result is a consequence of Theorem 4. □

3. Main Results

Proof of Theorem 1. According to Theorem 4, $N \in M_d(B)$ if and only if $\frac{B^e-1}{B^k-1} \equiv 0 \pmod{N}$. But $ND_B(N) = B^e - 1$ and we get the result of the theorem. □

From Theorem 1 we conclude immediately that if $B-1$ is not a divisor of $D_B(N)$ then N has not the Midy's property for any factor d of the order e of B modulo N.

Now, we will give some previous results for the proof of Theorem 2.

Let $\frac{1}{N} = 0.\overline{a_1 a_2 \cdots a_e}$ be a rational number, where the period is $a_1 a_2 \cdots a_e$. We denote this number by $\frac{1}{N} = 0.\overline{A_1 \circledcirc A_2 \circledcirc \cdots \circledcirc A_d}$, where the period was broken into d blocks of equal length k, that is, $e = kd$. So, as we said above, A_j be the number represented by the base B numeral consisting of the jth block of k B-digits of the period. And $A_i \circledcirc A_j$ denotes the integer represented by the base B numeral formed by the juxtaposition of the digits of A_i and A_j, for $1 \le i, j \le d$.

Theorem 6. *Let p and t be positive numbers with p a prime number such that $B \not\equiv 1 \bmod p$. Suppose that $e = o_{p^t}(B) = kd$. If*

$$\frac{1}{p^t} = 0.\overline{A_1 \circledcirc A_2 \circledcirc \cdots \circledcirc A_d},$$

then

$$\sum_{j=1}^{d} A_j = \begin{cases} \frac{(B^k-1)(p^t-p^i+2)}{2p^i} & \text{if there is } i, 1 \le i \le t-1, \text{ such that } d = p^{t-i}, \\ 0 \bmod B^k - 1 & \text{in other case.} \end{cases}$$

Proof. We have the following:

$$\begin{aligned} \frac{1}{p^t} &= 0.\overline{A_1 \circledcirc A_2 \circledcirc \cdots \circledcirc A_d}, \\ \frac{B^k}{p^t} &= A_1.\overline{A_2 \circledcirc A_3 \circledcirc \cdots \circledcirc A_d \circledcirc A_1}, \\ \frac{B^{2k}}{p^t} &= A_1 \circledcirc A_2.\overline{A_3 \circledcirc A_4 \circledcirc \cdots \circledcirc A_1 \circledcirc A_2}, \qquad (1) \\ &\vdots \\ \frac{B^{(d-1)k}}{p^t} &= A_1 \circledcirc A_2 \circledcirc \cdots \circledcirc A_{d-1}.\overline{A_d \circledcirc A_1 \circledcirc \cdots \circledcirc A_{d-1}}. \end{aligned}$$

Adding all these equations we get:

$$\begin{aligned}\frac{B^e-1}{p^t(B^k-1)} &= A_1 + A_1 \circledcirc A_2 + \cdots + A_1 \circledcirc A_2 \circledcirc \cdots \circledcirc A_{d-1} \\ &\quad + 0.\overline{A_1 \circledcirc A_2 \circledcirc \cdots \circledcirc A_d} + 0.\overline{A_2 \circledcirc A_3 \circledcirc \cdots \circledcirc A_d \circledcirc A_1} \\ &\quad + \cdots + 0.\overline{A_d \circledcirc A_1 \circledcirc \cdots \circledcirc A_{d-1}}.\end{aligned} \tag{2}$$

Notice that on the right side of the last equation, the sum of the values smaller than 1 is,

$$\frac{A_1 + A_2 + \cdots + A_d}{B^k - 1}.$$

On the other hand,

$$A_1 \circledcirc A_2 \circledcirc \cdots \circledcirc A_i = \left\lfloor \frac{B^{ik}}{p^t} \right\rfloor,$$

where $\lfloor x \rfloor$ is the floor function of x. But $B^{ik} = p^t \left\lfloor \frac{B^{ik}}{p^t} \right\rfloor + r_i$ with $r_i \equiv B^{ik} \mod p^t$, from Equation 2 we have

$$\frac{B^e-1}{p^t(B^k-1)} = \sum_{i=0}^{d-1} \frac{B^{ik} - r_i}{p^t} + \frac{A_1 + A_2 + \cdots + A_d}{B^k - 1}$$

and therefore

$$\frac{A_1 + A_2 + \cdots + A_d}{B^k - 1} = \frac{\sum_{i=0}^{d-1} r_i}{p^t},$$

so that

$$\sum_{j=1}^{d} A_j = \frac{(B^k-1)\sum_{i=0}^{d-1} r_i}{p^t}. \tag{3}$$

Hence $r_i \equiv B^{ik} \mod p^t$, so the set $\{r_i \mid i = 0, 1, \cdots d-1\}$ is a subgroup of $\mathbb{U}_{p^t}$, and the result of the theorem follows from the next lemma. □

Lemma 7. *Let p and t be positive integers with p an odd prime. Let d be a factor of $p^{t-1}(p-1)$ and let $\mathbb{U}(p,t,d)$ be the unique subgroup of order d of $\mathbb{U}_{p^t}$. Then d is a power of p, $d = p^{t-i}$, if and only if, for all $a \in \mathbb{U}(p,t,d)$ we have $a \equiv 1 \mod p$. Furthermore*

$$\sum_{g \in \mathbb{U}(p,t,d)} g = \begin{cases} \frac{p^{t-i}(p^t - p^i + 2)}{2} & \text{if } d = p^{t-i} \\ 0 \mod p^t & \text{otherwise} \end{cases}.$$

Proof. If $d = p^{t-i}$, we have

$$\mathbb{U}(p,t,p^{t-i}) = \left\{1,\ 1+p^i,\ 1+2p^i, \ldots,\ 1+(p^{t-i}-1)p^i\right\}.$$

Because this set is closed under the product modulo p^t, we are done. If $d \nmid p^{t-1}$, then there exists $a \in \mathbb{U}(p,t,d)$ such that $a \neq 1$ and $o_{p^t}(a) \mid p-1$ so that $a \notin \mathbb{U}(p,t,p^{t-1})$ and hence $a \not\equiv 1 \mod p$. We have $\{ag \mid g \in \mathbb{U}(p,t,d)\} = \mathbb{U}(p,t,d)$, so in the group $\mathbb{U}_{p^t}$,

$$\sum_{g \in \mathbb{U}(p,t,d)} ag = \sum_{g \in \mathbb{U}(p,t,d)} g.$$

Therefore, $(a-1) \sum_{g \in \mathbb{U}(p,t,d)} g = 0$, but $a \not\equiv 1 \mod p$, and then $\sum_{g \in \mathbb{U}(p,t,d)} g \equiv 0 \mod p^t$. □

When $p = 2$, it is known that the group $\mathbb{U}_{2^t}$ with $t > 2$ has two subgroups of order 2^{t-i} for $i = 1, 2, \cdots, t-1$. These are,

$$\mathbb{U}_1(2,t,2^{t-i}) = \left\{1,\ 1+1\cdot 2^i,\ 1+2\cdot 2^i,\ 1+3\cdot 2^i,\ \ldots,\ 1+(2^{t-i}-1)2^i\right\}$$

and

$$\mathbb{U}_2(2,t,2^{t-i}) = \left\{ \begin{array}{l} 1,\ 1\cdot 2^i-1,\ 2\cdot 2^i-1,\ 3\cdot 2^i-1,\ \ldots, \\ \quad (2^{t-i}-2)2^i-1,\ (2^{t-i}-1)2^i-1 \end{array} \right\}.$$

With this, we get the following proposition.

Proposition 8. *With the above notation,*

$$\sum_{g \in \mathbb{U}(2,t,2^{t-i})} g = \left\{ \begin{array}{ll} 2^{t-i-1}(2^t - 2^i + 2) & \text{if } \ \mathbb{U}(2,t,2^{t-i}) = \mathbb{U}_1(2,t,2^{t-i}), \\ \\ 2^{t-i-1}(2^t - 2^i) & \text{if } \ \mathbb{U}(2,t,2^{t-i}) = \mathbb{U}_2(2,t,2^{t-i}). \end{array} \right.$$

Note that the sum of the elements of the subgroup $\mathbb{U}_1(2,t,2^{t-i})$ is the same as the first sum of Lemma 7.

From Theorem 6, we get the following statement.

Theorem 9. *Let p and t be positive numbers with p prime and not a divisor of B. Let $N = p^t$ and $e = o_N(B) = kd$. Then $N \in M_d(B)$ if and only if $d \nmid p^{t-1}$. Furthermore, if $N \in M_d(B)$ and $\sum_{g \in \mathbb{U}(p,t,d)} g = rp^t$ for some integer r then $\sum_{j=1}^{d} A_j = (B^k - 1)r$.*

In a similar way as we get Equation 3, we can prove that if $gcd(N,\ B) = 1$, $o_N(B) = kd$ and $r_i \equiv B^{ik} \mod N$, then

$$\sum_{j=1}^{d} A_j = \frac{(B^k - 1)\sum_{i=1}^{d} r_i}{N}.$$

Therefore

$$\frac{\sum_{j=1}^{d} A_j}{(B^k-1)} = \frac{\sum_{i=1}^{d} r_i}{N}. \tag{4}$$

In others words, the last equation says that to prove that $N \in M_d(B)$ is equivalent to asking if the sum $\sum_{i=1}^{d} r_i$ is a multiple of N. If we have the decomposition of N in prime factors $N = p_1^{t_1} p_2^{t_2} \cdots p_s^{t_s}$, it is well known from the Chinese Remainder Theorem that there is an isomorphism between the groups $\mathbb{U}_N$ and $\mathbb{U}_{p_1^{t_1}} \times \mathbb{U}_{p_2^{t_2}} \times \cdots \times \mathbb{U}_{p_s^{t_s}}$; for this reason, $\sum_{i=1}^{d} r_i$ is a multiple of N if and only if it is a multiple of $p_j^{t_j}$ for all $j = 1, 2, \ldots, s$.

Proof of Theorem 2. Let p be a prime divisor of N and p^t the highest power of p that divides N, and let σ be the canonical projection of $\mathbb{U}_N \cong \mathbb{U}_{p_1^{t_1}} \times \mathbb{U}_{p_2^{t_2}} \times \cdots \times \mathbb{U}_{p_s^{t_s}}$ over $\mathbb{U}_{p^t}$. We have $o_N(B) = e = kd$; hence $p \mid B^e - 1$ and therefore $o_p(B) \mid e$.

Suppose that $o_p(B) \nmid k$. We know $o_p(B) \mid p-1$, $o_p(B) \mid e$ and $e = kd$, so we have that d cannot be a power of p and by Lemma 7, we get that $\sum_{i=1}^{d} r_i = \sum_{i=1}^{d} (B^{ik} \mod p^t)$ is divisible by p^t.

If $o_p(B) \mid k$ then $p^t \mid d$, and therefore $r_i \equiv B^{ik} \equiv 1 \mod p$ for $i = 1, 2, \ldots, d$.

Now, the set $\mathcal{B} = \left\{ B^{ik} \mid i = 1, 2, \cdots, d \right\}$ is a subgroup of $\mathbb{U}_N$ so we have that $\sigma(\mathcal{B})$ is a subgroup of $\mathbb{U}_{p^t}$. By Lemma 7 it has order p^{t-i}, so $\sigma(\mathcal{B}) = \mathbb{U}(p, t, p^{t-i})$. But,

$$\mathcal{B} = \bigcup_{g \in \mathbb{U}(p,t,p^{t-i})} \sigma^{-1}(g),$$

again by Lemma 7, we have that

$$\sum_{i=1}^{d} r_i = \frac{d}{p^{t-i}} \times \frac{p^{t-i}(p^t - p^i + 2)}{2}$$

is a multiple of d and therefore of p^t.

For any prime p that divides N, we conclude that the sum $\sum_{i=1}^{d} r_i$ is a multiple of p^t. So we can apply the isomorphism (given by the Chinese Remainder Theorem) between the groups $\mathbb{U}_N$ and $\mathbb{U}_{p_1^{t_1}} \times \mathbb{U}_{p_2^{t_2}} \times \cdots \times \mathbb{U}_{p_s^{t_s}}$, to prove that this sum is divisible by N; from Equation 4 we may conclude that $\sum_{j=1}^{d} A_j$ is a multiple of $B^k - 1$ and finally that $N \in M_d(B)$.

Reciprocally, let $N \in M_d(B)$, and p be a prime divisor of N. If $o_p(B) \nmid k$ the result is immediate.

Suppose that $o_p(B) \mid k$. Then $r_i \equiv B^{ik} \equiv 1 \mod p$ for $i = 1, 2, \ldots, d$. Again, the set $\sigma\left(\left\{ B^{ik} \mid i = 1, 2, \ldots, d \right\}\right)$ is a subgroup of $\mathbb{U}_{p^t}$ of the type $\mathbb{U}(p, t, p^{t-i})$. Therefore, by Lemma 7,

$$\sum_{i=1}^{d} r_i = \frac{d}{p^{t-i}} \times \frac{p^{t-i}(p^t - p^i + 2)}{2} = d\left(\frac{p^t - p^i + 2}{2}\right).$$

We know that $N \in M_d(B)$ so that $p^t \mid \sum_{i=1}^{d} r_i$ and therefore, $p^t \mid d$. □

Finally, Theorem 3 is immediate from Theorem 2 and it gives an easy characterization of Midy's Property.

References

[1] A. Gupta and B. Sury, *Decimal expansion of $\frac{1}{p}$ and subgroup sums*, Integers: Electronic Journal Of Combinatorial Number Theory **5** (2005), # A19, 5 pp. (electronic). MR 2192238

[2] J. Lewittes, *Midy's theorem for periodic decimals*, Integers: Electronic Journal Of Combinatorial Number Theory **7** (2007), #A02, 11 pp. (electronic). MR 2282184

[3] H. W. Martin, *Generalizations of Midy's theorem on repeating decimals*, Integers: Electronic Journal Of Combinatorial Number Theory **7** (2007), #A03, 7 pp. (electronic). MR 2282186