q-PSEUDOPRIMALITY: A NATURAL GENERALIZATION OF STRONG PSEUDOPRIMALITY

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

Abstract. In this work we present a natural generalization of strong pseudoprime to base b, which we have called q-pseudoprime to base b. It allows us to present another way to define a Midy's number to base b (overpseudoprime to base b). Besides, we count the bases b such that N is a q-probable prime base b and those ones such that N is a Midy's number to base b. Furthemore, we prove that there is not a concept analogous to Carmichael numbers to q-probable prime to base b as with the concept of strong pseudoprimes to base b.

1. Introduction

Recently, Grau et al. [7] gave a generalization of Pocklignton's Theorem (also known as Proth's Theorem) and Miller-Rabin primality test, it takes as reference some works of Berrizbeitia, [1, 2], where it is presented an extension to the concept of strong pseudoprime, called ω-primes. As Grau et al. said it is right, but its application is not too good because it is needed m-th primitive roots of unity, see [7, 12].

In [7], it is defined when an integer N is a p-strong probable prime base a, for p a prime divisor of $N-1$ and $\gcd(a,N)=1$. In a reading of that paper, we discovered that if a number N is a p-strong probable prime to base 2 for each p prime divisor of $N-1$, it is actually a Midy's number or a overpseudoprime number to base 2. For instance, they said that 2047, 3277, 4033, 8321, 65281, 80581, 85489 and 88357 are the first p-strong pseudoprimes to base 2 for any prime $p \mid N-1$. Indeed, these integers are Midy's numbers to base 2 and the first terms of the sequence $A141232$ at the Online Encyclopedia of Integers Sequences, OEIS, where we called them overpseudoprimes to base 2.

It is important to highlight that the definition of p-strong probable prime to base a, does not require each divisor of $N-1$ to be congruent with 1 module p. And this fact gives some difficulties as those ones showed in our Theorem 11.

2010 *Mathematics Subject Classification.* 11A51, 11Y11, 11Y55, 11B83.

Key words and phrases. Period, decimal representation, order of an integer, multiplicative group of units modulo N, pseudoprime, strong pseudoprime, overpseudoprime.

We organize this paper as follows. In the second section, we present the definition of Midy's property and recall some known results about it, in particular we recall the Midy's number concept, some of its properties and some connections between it and other former concepts of pseudoprimes. We study properties of the set of integers b such that N is a Midy's number to base b and as new result we count the number of them.

In the third section we recall our concept of q-pseudoprimality to base b and we stablish a formula that gives the number of bases of q-pseudoprimality.

Finally, in the fourth section, we make some comments about the recent paper of Grau et al. [7], where in an independent way are presented some of our ideas.

2. Midy's Property and Midy's numbers

Let N and b be positive integers relatively primes, $b > 1$ the base of numeration, $|b|_N$ the order of b in the multiplicative group $\mathbb{U}_N$ of positive integers less than N and relatively primes with 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 fraction $\frac{x}{N}$ (see Exercise 2.5.9 in [10]). Let d, k be positive integers with $|b|_N = dk$, $d > 1$ and $\frac{x}{N} = 0.\overline{a_1 a_2 \cdots a_{|b|_N}}$ where the bar indicate the period and a_i's are digits in base b. We separate the period $a_1 a_2 \cdots a_{|b|_N}$ 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 [8] and its references.

We denote with $\mathcal{M}_b(N)$ the set of positive integers d divisors of $|b|_N$ such that N has the Midy's property for b and d and we will call it the 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 and $\omega(N)$ denotes the number of prime divisors of N.

For example 13 has the Midy's property to the base 10 and $d = 3$, because $|13|_{10} = 6$, $1/13 = 0.\overline{076923}$ and $07 + 69 + 23 = 99$. Also, 49 has the Midy's property to the base 10 and $d = 14$, since $|49|_{10} = 42$, $1/49 = 0.\overline{020408163265306122448979591836734693877551}$ and $020 + 408 + 163 + 265 + 306 + 122 + 448 + 979 + 591 + 836 + 734 + 693 + 877 + 551 = 7 * 999$. But 49 does not have the 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 [6] was given the following characterization of Midy's property.

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

Last theorem stablishes that if d is a divisor of $|b|_N$ then $d \in \mathcal{M}_b(N)$ if and only if 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 $\nu_q\left(|b|_p\right) > \nu_q(|b|_N) - \nu_q(d)$.

We demonstrated, see [3, Cor. 1], that if $d_1 \in \mathcal{M}_b(N)$ and d_2 is a divisor of $|b|_N$ and $d_1 \mid d_2$ then $d_2 \in \mathcal{M}_b(N)$, in this way the set $\mathcal{M}_b(N)$ is closed "for multiples".

In [4, Th. 2.4], we proved the next result.

Theorem 2. *Let N, q, v be integers with q prime and $v > 0$. Then $q^v \in \mathcal{M}_b(N)$ if and only if $N = q^n p_1^{h_1} p_2^{h_2} \cdots p_l^{h_l}$ 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*

$$\nu_q(|b|_N) - v < \min_{1 \leq i \leq l} \left\{ \nu_q(|b|_{p_i}) \right\}.$$

Observe that when N is a prime number, Theorem 1 is satisfied for any base b and each prime divisor of $|b|_N$ and therefore it is also verified for any divisor greater than 1 of $|b|_N$. Composite numbers with this property for a fixed base b were studied in [4] and [11], under the name of Midy numbers to base b or overpseudoprimes to base b.

Definition 3. *We say that a number N is a Midy's number to base b (or overpseudoprime to base b) if N is an odd composite number relatively prime to both b and $|b|_N$ and for all divisor $d > 1$ of $|b|_N$ we get that $d \in \mathcal{M}_b(N)$.*

It is easy to see, from [4, Th. 2.10] or [11, Th. 12], that an odd composite number N with N relatively prime with b, is a Midy's number to base b if and only if $|b|_N = |b|_p$ for every prime p divisor of N. Thereby, we have that an odd composite N is a Midy's number to base b if and only if each divisor of N is either a prime or a Midy's number to base b. Observe that $|1|_N = 1$ for any positive integer N, for that reason for now on we accept b to be equal to 1, although it does not make sense to consider the Midy's property to the base 1.

The result below, Theorem 2.3 of [9], allows us to give another characterization of Midy's numbers.

Theorem 4 (Theorem 2.3 of [9])**.** *Let m, $b \geq 2$, $n \geq 3$ and r be integers, where r is the greatest prime divisor of n. Then m is a divisor of $\Phi_n(b)$ if and only if $b^n \equiv 1 \mod m$ and every prime divisor p of m satisfies that*

$$n = \begin{cases} |b|_p & \text{if } r \neq p, \\ r^e\,|b|_r & \text{if } r = p. \end{cases}$$

We denote with $\Phi_n(x)$ the n-th cyclotomic polynomial with rational coefficients. From the above theorem we get immediatly the next characterization of Midy's numbers.

Theorem 5. *A composite number N with $\gcd(N, |b|_N) = 1$, is a Midy's number to base b if and only if $\Phi_{|b|_N}(b) \equiv 0 \mod N$.*

Theorem 4 allow us to conclude, in particular, that if n and b are integers with $n \geq 3$ and $b \geq 2$ then, $\gcd(n, \Phi_n(b))$ is either 1 or the greatest prime divisor of n, therefore this result give us a way to produce Midy's numbers. Indeed, if p is a prime divisor of $\frac{\Phi_N(b)}{\gcd(N,\ \Phi_N(b))}$, then $|b|_p = N$ and so we get the following result.

Theorem 6. *Let $N > 2$ and $f_N(b) = \frac{\Phi_N(b)}{\gcd(N,\ \Phi_N(b))}$. If $f_N(b)$ is composite, then $f_N(b)$ is a Midy's number to base b.*

With the help of this generating way of Midy's numbers, it is easy to prove that if b is an even number then the generalized Fermat number $b^{2^n} + 1$ is either a prime or a Midy's number; the same happens with the generalized Mersenne numbers $\frac{b^p-1}{b-1}$ where p is prime which not divides $b - 1$. In this way Fermat and Mersenne were not totally wrong about the primality of their numbers.

Now, we study some connections between Midy's numbers and some kind of pseudoprimes. The composite integer N is called a pseudoprime (or Fermat pseudoprime) to base b if $\gcd(b, N) = 1$ and $b^{N-1} \equiv 1 \mod N$. An integer which is pseudoprime for all possible bases b is called a Carmichael number or an absolute pseudoprime. An odd composite N such that $N-1 = 2^s t$ with t an odd integer and $\gcd(b,\ N) = 1$, is said to be a strong pseudoprime to base b if either $b^t \equiv 1 \mod N$ or $b^{2^i t} \equiv -1 \mod N$, for some $0 \leq i < s$. It can be prove that an odd composite integer N is a strong pseudoprime to base b if and only if N is pseudoprime to base b and there is a non-negative integer k such that $\nu_2(|b|_N) = \nu_2\left(|b|_p\right) = k$ for all prime p divisor of N.

The set of bases of Midy pseudoprimality is closed under taking powers, although it is not closed under multiplication as we can see when take $N = 91$ which is Midy's number to bases 9 and 16 but it is not to 53, their product modulo N.

Theorem 7. *If N is a Midy's number to base b, then N is a strong pseudoprime to base b.*

Proof. Since N is a Midy's number to base b implies that $|b|_N = |b|_n$ for each divisor n of N and thus there is a non-negative integer k such that for all prime divisor p of N we get that $\nu_2\left(|b|_{p^{\nu_p(N)}}\right) = k$ and the result follows. □

The reciprocal is not true. For example $N = 91$ is a strong pseudoprime to base 53, but it is not a Midy's number to this base. Additionally, from

the last theorem we could say that the Midy's numbers are "stronger" than strong pseudoprimes.

We finish this section counting the number of positive integers b such that N is a Midy pseudoprime to base b.

Theorem 8. *Let $N = \prod_{1\leq i\leq \omega(N)} p_i^{e_i}$ be an integer where p_i are different primes and $D = \gcd\left(p_1 - 1,\ p_2 - 1,\ \ldots,\ p_{\omega(N)} - 1\right)$, then the number of elements $b \in \mathbb{U}_N$ such that N is a Midy's number base b is given by*

$$B_m(N) = \sum_{d|D} \phi(d)^{\omega(N)}. \tag{2.1}$$

Proof. Take b such that N is a Midy's number base b. From [11, Theorem 12] we know that $|b|_{p_i} = |b|_{p_1}$ for each $i = 2, \ldots, \omega(N)$ and for that reason $|b|_{p_1}$ is a divisor of D. On the other hand, if d is a divisor of D, for each i there are $\phi(d)$ elements $b_i \in \mathbb{U}_{p_i}$ of order d. The Chinese Remainder Theorem allow us to obtain an element b such that $b \equiv b_i \mod p_i$ where $1 \leq i \leq \omega(N)$ and thus if we take all these elements b_i, we get $\phi(d)^{\omega(N)}$ possible bases b and the result follows. □

3. q-pseudoprimality: A natural generalization of strong pseudoprimality.

If N is a Midy's number to base b, we have showed that $\nu_q\left(|b|_N\right) = \nu_q\left(|b|_p\right)$ for all primes q and p, with $p \mid N$. This last fact and the characterization of strong pseudoprimality suggest the following definition:

Definition 9. *Let N, b be integers with $\gcd(b, N) = 1$ and $b^{N-1} \equiv 1 \pmod N$ and q a prime number such that for every prime p divisor of N, q divides $p - 1$. We say that N is a q-probable prime base b if there is a non negative integer k such that for every prime p divisor of N we have $\nu_q\left(|b|_p\right) = k$. Morever, if N is composite we say that N is q-pseudoprime to base b.*

Even though, in the above definition it is necessary to calculate $|b|_p$, for each prime p divisor of N, and to verify that q appears the same number of times in each one of these numbers, actually we can decide the q-probable primality of a given number with a procedure similar to the Miller's Test. We proved it in [4] and we present it in the next theorem.

Theorem 10 (Theorem 3.6 of [4])**.** *Assume that N is and odd integer, b a positive integer relatively prime with N and q a prime that divides $p-1$ for all prime divisor p of N. Write $N - 1 = q^s t$ with $\gcd(q, t) = 1$, then N is a q-probable prime base b if and only if one of the following conditions holds:*

1. $b^t \equiv 1 \pmod N$.
2. *There exists with $0 \leq i < s$ such that N divides $\Phi_q\left(b^{q^i t}\right)$.*

Furthermore, if the second condition holds, then every prime divisor of N is congruent with 1 modulo q^{i+1}.

Grau et al. [7] defined the concept of q-strong probable prime to base b. Their idea is similar to our Definition 9, although they do not require q to be a divisor of $p-1$ for each prime p divisor of N and this could leave to inconvenient facts as we show in the following result.

Theorem 11 (Theorem 3.9 of [4])**.** *Let N be a Carmichael number and q a prime with $N-1=q^s t$ where q does not divide t and such that, for each prime divisor p of N, q does not divide $p-1$, then $b^t \equiv 1 \pmod{N}$, for each integer b relatively prime with N.*

In consequence, if we removed the condition that each prime factor of N to be of the form $hq+1$, one would define an analogue concept to Carmichael number from the concept of q-probable prime.

For instance, this is the case of the Carmichael number:

$$N = 2\,333\,379\,336\,546\,216\,408\,131\,111\,533\,710\,540\,349\,903\,201$$

which is product of 23 primes, as follows

$$\begin{aligned} N =& 11 \times 13 \times 17 \times 19 \times 29 \times 31 \times 37 \times 41 \times 43 \times 47 \times 61 \times 71 \times \\ & \times 73 \times 101 \times 109 \times 113 \times 127 \times 139 \times 163 \times 211 \times 337 \times 421 \times 541. \end{aligned}$$

Taking $q = 12\,068\,159$ which is prime and $N-1=qt$ where

$$t = 193\,350\,065\,784\,368\,304\,074\,474\,949\,634\,864\,800$$

and if b is relatively prime with N then $b^t \equiv 1 \pmod{N}$. For that reason, in the concept of Grau et al. [7], it is a q-strong probable prime, while it does not make sense to talk about the q-probable primality of N.

We denote the number of bases of probable primality of N with $B_{pp}(N)$ and its number of bases of strong probable primality with $B_{spp}(N)$. It is well known that, see [5, Exercises 3.14 and 3.15]:

$$B_{pp}(N) = \prod_{p|N} \gcd(p-1,\ N-1) \tag{3.1}$$

$$B_{spp}(N) = \left(1 + \frac{2^{\nu(2,N)\omega(N)}-1}{2^{\omega(N)}-1}\right) \prod_{p|N} \gcd(p-1,\ t), \tag{3.2}$$

where $N-1=2^s t$ with t an odd number, $\omega(N)$ the number of prime divisors of N and for a prime q we write

$$\nu(q,N) = \nu_q\left(\gcd\left(p_1-1, p_2-1, \ldots, p_{\omega(N)}-1\right)\right).$$

Now we will count the number of bases b such that N is a q-probable prime base b and we denote it with $B_{qpp}(N)$.

Theorem 12. *Suppose that N is an odd integer and q a prime number such that each prime divisor of N is congruent with 1 modulo q. Assume that $N-1=q^s t$ where q and t are relatively primes, then*

$$B_{qpp}(N)=\left(1+(q-1)^{\omega(N)}\,\frac{q^{\nu(q,N)\omega(N)}-1}{q^{\omega(N)}-1}\right)\prod_{p|N}\gcd(\,p-1,\ t)\,.$$

Proof. Suppose that N is a q-probable prime base b. By Theorem 10 we will consider two cases. Firstly, we assume that there exists an integer i such that $0\leq i<\nu(q,N)$, $\gcd\left(b^{q^i t}-1,\ N\right)=1$ and $b^{q^{i+1}t}\equiv 1 \bmod N$. Let p be a prime divisor of N. Thus, we get that $\gcd\left(b^{q^i t}-1,\ p^{\nu_p(N)}\right)=1$ and $b^{q^{i+1}t}\equiv 1 \bmod p^{\nu_p(N)}$. Taking $m=q^i t$ it follows that $b^{qm}\equiv 1 \bmod p^{\nu_p(N)}$ and $b^m\not\equiv 1 \bmod p$, therefore the number of bases b, denoted by h_p, is

$$\begin{aligned}h_p&=\gcd\left(qm,\ \phi(p^{\nu_p(N)})\right)-\gcd(m,\ p-1)\\&=q^{i+1}\gcd(t,\ p-1)-q^i\gcd(t,\ p-1)\\&=(q-1)\,q^i\gcd(\,p-1,\ t)\,.\end{aligned}$$

By the Chinese Remainder Theorem, we get that the number of solutions of $\gcd\left(b^{q^i t}-1,\ N\right)=1$ and $b^{q^{i+1}t}\equiv 1 \bmod N$, is the product of h_p when p is a prime divisor of N. Thus the number of these solutions is

$$(q-1)^{\omega(N)}\,q^{i\omega(N)}\prod_{p|N}\gcd(\,p-1,t)\,.$$

Because i takes values from 0 until $\nu(q,N)-1$, then the number of bases b which satisfied the condition (2) of the Theorem 10 is

$$(q-1)^{\omega(N)}\prod_{p|N}\gcd(p-1,\ t)\sum_{i=o}^{\nu(q,N)-1}q^{i\omega(N)};$$

which implies

$$(q-1)^{\omega(N)}\,\frac{q^{\nu(q,N)\omega(N)}-1}{q^{\omega(N)}-1}\prod_{p|N}\gcd(p-1,\ t)\,. \tag{3.3}$$

Similarly, we count the number of bases b verifying the first condition of the Theorem 10, i.e. $b^t\equiv 1 \bmod N$. This number is equals to

$$\prod_{p|N}\gcd(p-1,\ t)\,. \tag{3.4}$$

The statement of the theorem follows when we add (3.3) and (3.4). □

4. Acknowledgments

The authors are members of the research group: Álgebra, Teoría de Números y Aplicaciones, ERM. The results of this article are part of the research project "Construcciones de conjuntos $B_h[g]$, propiedad de Midy, y algunas aplicaciones" CÓDIGO: 110356935047 partially financied by COLCIENCIAS.

References

1. Pedro Berrizbeitia and T. G. Berry, *Generalized strong pseudoprime tests and applications*, J. Symbolic Comput. **30** (2000), no. 2, 151–160. MR 1777169 (2001f:11201)
2. Pedro Berrizbeitia and Aurora Olivieri, *A generalization of Miller's primality theorem*, Proc. Amer. Math. Soc. **136** (2008), no. 9, 3095–3104. MR 2407072 (2009g:11164)
3. John H. Castillo, Gilberto García-Pulgarín, and Juan Miguel Velásquez-Soto, *Structure of associated sets to Midy's Property*, Mat. Enseñ. Univ. (N. S.) **XX** (2012), no. 1, 21–28.
4. ———, *De los números de Midy a la primalidad*, Revista Integración (2014), Accepted.
5. Richard Crandall and Carl Pomerance, *Prime numbers. A computational perspective*, second ed., Springer, New York, 2005. MR 2156291 (2006a:11005)
6. Gilberto García-Pulgarín and Hernán Giraldo, *Characterizations of Midy's property*, Integers **9** (2009), A18, 191–197. MR MR2506150
7. José María Grau, Antonio M. Oller-Marcén, and Daniel Sadornil, *A primality test for $kp^n + 1$ numbers*, Math. Comp. (Published electronically: june 10, 2014).
8. Joseph Lewittes, *Midy's theorem for periodic decimals*, Integers **7** (2007), A2, 11 pp. (electronic). MR 2282184 (2008c:11004)
9. Kaoru Motose, *On values of cyclotomic polynomials. II*, Math. J. Okayama Univ. **37** (1995), 27–36 (1996). MR 1416242 (97h:11151)
10. Melvyn B. Nathanson, *Elementary methods in number theory*, Graduate Texts in Mathematics, vol. 195, Springer-Verlag, New York, 2000. MR 1732941 (2001j:11001)
11. Vladimir Shevelev, John H. Castillo, Gilberto García-Pulgarín, and Juan Miguel Velásquez-Soto, *Overpseudoprimes, and Mersenne and Fermat Numbers as Primover Numbers*, J. Integer Seq. **15** (2012), no. 7, Article 12.7.7.
12. Zhenxiang Zhang, *On the effectiveness of a generalization of Miller's primality theorem*, J. Complexity **26** (2010), no. 2, 200–208. MR 2607733 (2011d:11292)

John H. Castillo, Departamento de Matemáticas y Estadística, Universidad de Nariño
E-mail address: jhcastillo@gmail.com, jhcastillo@udenar.edu.co

Gilberto García-Pulgarín, Universidad de Antioquia
E-mail address: gilberto.garcia@udea.edu.co

Juan Miguel Velásquez Soto, Departamento de Matemáticas, Universidad del Valle
E-mail address: juan.m.velasquez@correounivalle.edu.co