MATHEMATICS OF COMPUTATION
S 0025-5718(2014)02849-4
Article electronically published on June 10, 2014

A PRIMALITY TEST FOR $Kp^n + 1$ NUMBERS

JOSÉ MARÍA GRAU, ANTONIO M. OLLER-MARCÉN, AND DANIEL SADORNIL

Abstract. In this paper we generalize the classical Proth's theorem and the Miller-Rabin test for integers of the form $N = Kp^n + 1$. For these families, we present variations on the classical Pocklington's results and, in particular, a primality test whose computational complexity is $\widetilde{O}(\log^2 N)$ and, what is more important, that requires only one modular exponentiation modulo N similar to that of Fermat's test.

1. Introduction

In 1877 P. Pepin [13] presented the following result about the primality of Fermat numbers:

Theorem 1.1. *Let F_n be the n-th Fermat number, i.e., $F_n = 2^{2^n+1}$ with $n > 1$. Then, F_n is prime if and only if $3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$.*

Although this theorem has not certified the primality of any new Fermat prime (by 1877 the 5 Fermat primes were already known), it is the first result which leads to a deterministic primality test requiring only one modular exponentiation similar to that of Fermat's test modulo N, thus of $\widetilde{O}(\log^2 N)$ complexity. One year after, using the same underlying ideas, Proth [15] proved the following primality criterion for numbers of the form $N = K2^n+1$, where K is odd and $K < 2^n$ (Proth numbers).

Theorem 1.2. *Let $N = K2^n + 1$, where K is odd and $K < 2^n$. If $a^{\frac{N-1}{2}} \equiv -1 \pmod{N}$ for some $a \in \mathbb{Z}$, then N is prime.*

The next important step was made in 1914 by Pocklington [14]; his result is the first generalization of Proth's theorem suitable for numbers of the form $N = Kp^n + 1$.

Theorem 1.3. *Let $N = Kp^n + 1$ with $K < p^n$. If, for some $a \in \mathbb{Z}$*

i) $a^{N-1} \equiv 1 \pmod{N}$,

ii) $\gcd(a^{\frac{N-1}{p}} - 1, N) = 1$.

Then, N is prime.

Proth and Pocklington results are still useful. In fact they are the base of the popular software created by Yves Gallot (Proth.exe) for the search of Proth and generalized Proth ($N = Kp^n + 1$) primes. Other software based on a variation of Pocklington's Theorem presented by Brillhart, Lehmer and Selfridge [7, 8] is

Received by the editor June 12, 2012 and, in revised form, May 13, 2013.
2010 *Mathematics Subject Classification.* Primary 11Y11, 11Y16, 11A51, 11B99.
Daniel Sadornil was partially supported by the Spanish Government under projects MTM2010-21580-C02-02 and MTM2010-16051.

OpenPFGW with which some records have been broken in different families of integers. A drawback of this software is that it usually requires the use of several bases and, consequently, the computation of several exponentiations modulo N.

In recent times the most active researcher looking for primality criteria for numbers of the form $N = Kp^n + 1$ has been P. Berrizbeitia. Berrizbeitia and his collaborators have found very efficient criteria for this kind of number for a variety of primes p [2–4]. Even though similar criteria had been previously presented by H.C. Williams and his collaborators [17,18], the methodology used by Berrizbeitia et al. is clearer and more efficient. For these generalizations an analogue of the Legendre symbol, the *m-th power residue symbol*, has been used. It assumes values over the m-th roots of unity and it satisfies a *higher order law of reciprocity*. However, the use of the m-th power residue symbol presents technical difficulties, mainly because the ring $\mathbb{Z}[e^{2\pi i/m}]$ is not a UFD in general. Other authors, A. Guthmann [10] and W. Bosma [6], have also given generalizations of Proth's theorem using similar techniques but limited to the case $p = 3$.

In this paper we present a primality criterion for integers of the form $N = Kp^n+1$, p prime and $K < p^n$, using techniques similar to those in [9] for generalized Cullen Numbers ($N = np^n + 1$), which do not require the use of any m-th power residue symbol.

2. A generalization of Proth's theorem

The primality test which follows from Proth's theorem is very useful since, if $N = K2^n + 1$ is a prime, then half of the possible values for a satisfy the condition of the theorem. In particular it is satisfied by those a which are a quadratic non-residue modulo N; i.e., such that the Jacobi symbol $(\frac{a}{N}) = -1$.

Theorem 2.1. *Let $N = K2^n+1$, where K is odd and $K < 2^n$. Assume that $a \in \mathbb{Z}$ is such that $\left(\frac{a}{N}\right) = -1$, then:*

$$N \text{ is a prime if and only if } a^{\frac{N-1}{2}} \equiv -1 \pmod{N}.$$

In spite of the various generalizations presented in the introduction, the most natural generalization of this theorem had not yet been exhibited. We do so in the following result. In what follows, $\Phi_p(X)$ will denote the p-th cyclotomic polynomial.

Theorem 2.2. *Let $N = Kp^n + 1$, where p is a prime and $K < p^n$. Assume that $a \in \mathbb{Z}$ is a p-th power non-residue modulo N, then*

$$N \text{ is a prime if and only if } \Phi_p(a^{\frac{N-1}{p}}) \equiv 0 \pmod{N}.$$

Proof. If N is a prime, then $a^{N-1} \equiv 1 \pmod{N}$. Now, $0 \equiv a^{N-1} - 1 = (a^{\frac{N-1}{p}} - 1)\Phi_p(a^{\frac{N-1}{p}}) \pmod{N}$. Since a is a p-th power non-residue, then $a^{\frac{N-1}{p}} - 1 \not\equiv 0 \pmod{N}$ and this implies, N being prime, that $\Phi_p(a^{\frac{N-1}{p}}) \equiv 0 \pmod{N}$.

Conversely, assume that $\Phi_p(a^{Kp^{n-1}}) \equiv 0 \pmod{N}$. Put $X = a^K$, then

$$\Phi_p(X^{p^{n-1}}) \equiv 0 \pmod{N}.$$

It follows that $X^{p^n} \equiv 1 \pmod{N}$. Now, let $q \leq \sqrt{N}$ be a prime divisor of N, then it also holds that $\Phi_p(X^{p^{n-1}}) \equiv 0 \pmod{q}$ and $X^{p^n} \equiv 1 \pmod{q}$. Thus, the order of X in $\mathbb{Z}_q^*$ is a divisor of p^n, but if $X^{p^j} \equiv 1 \pmod{q}$ with $j < n$ would imply that $p = \Phi_p(1) \equiv 0 \pmod{q}$ which is clearly a contradiction. Consequently,

the order of X in $\mathbb{Z}_q^*$ is p^n. It follows that $p^n | q-1$ and $p^n < q \leq \sqrt{N}$ and then $p^{2n} \leq N = Kp^n + 1$, so $p^n \leq K$ is a contradiction. □

This theorem can be restated in the following way.

Theorem 2.3. *Let $N = Kp^n + 1$, where p is a prime. If $p^n > K$, then*

$$\Phi_p(a^{\frac{N-1}{p}}) \equiv 0 \pmod{N} \Leftrightarrow N \text{ is prime and } a \text{ is a } p\text{-th power non-residue modulo } N.$$

Proof. It is enough to observe that if $\Phi_p(a^{\frac{N-1}{p}}) \equiv 0 \pmod{N}$, then N is prime (as in the previous proof) and $a \not\equiv x^p \pmod{N}$ for, if it was the case, then $0 \equiv \Phi_p(a^{\frac{N-1}{p}}) \equiv \Phi_p(x^{N-1}) \equiv \Phi_p(1) = p \pmod{N}$; a contradiction. □

This result, like Proth's theorem, is really useful since if Kp^n+1 is prime, a is a p-th power residue modulo N only for $\frac{1}{p}$ of the possible choices of such a. Nevertheless, the interest of this result is mainly theoretical as a genuine generalization of Proth's theorem. An even more useful generalization, not requiring an adequate choice for a, will be presented in forthcoming sections.

3. A generalization of Miller-Rabin primality test

The so-called Miller-Rabin probabilistic primality test applies to integers in the form $N = K2^n + 1$ (K odd) and it is based on Fermat's little theorem and on the fact that, the only solutions of $x^2 \equiv 1 \pmod{p}$ (p prime) are $x \equiv \pm 1 \pmod{p}$.

Theorem 3.1 ([8, Theorem 3.5.1.])**.** *Let $N = K2^n + 1$ be prime. If a is an integer such that $\gcd(a, N) = 1$, then one of the following holds:*

i) $a^K \equiv 1 \pmod{N}$.
ii) *There exists $0 \leq j < n$ such that $a^{K2^j} \equiv -1 \pmod{N}$.*

The probabilistic version states that conditions i) and ii) are satisfied for a composite number only for at most 1/4 of possible values for a. This probabilistic test, in spite of being more demanding than Fermat's test, presents many pseudoprimes and is specially unreliable if n is small. Nevertheless, for big values of n, as in the case of Proth numbers, the test is very reliable and, as we will see in the next section, it allows us to certify the primality of the numbers that pass it.

We must point out that a generalization for the Miller-Rabin test is really simple, even though more than two decades passed until the first publication in this direction was made [1, 5]. A natural generalization for the Miller-Rabin test (that we shall call the p-Miller-Rabin test) is based in the following result:

Theorem 3.2. *Let $N = Kp^n + 1$ with p a prime number. If N is prime, then for every integer a such that $\gcd(a, N) = 1$ one of the following holds:*

i) $a^K \equiv 1 \pmod{N}$.
ii) *There exists $0 \leq j \leq n-1$ such that $\Phi_p(a^{Kp^j}) \equiv 0 \pmod{N}$.*

Proof. If N is a prime, then $a^{Kp^n} \equiv 1 \pmod{N}$. If $a^K \not\equiv 1 \pmod{N}$, let $1 \leq r \leq n$ be the smallest integer such that $a^{Kp^r} \equiv 1 \pmod{N}$. Then $a^{Kp^{r-1}} \not\equiv 1 \pmod{N}$ and the primality of N implies that $\Phi_p(a^{Kp^{r-1}}) \equiv 0 \pmod{N}$ as in Theorem 6. It is enough to put $j = r - 1$ to complete the proof. □

Definition 3.3. A *p-strong probable prime to base a* is a number satisfying conditions i) and ii) of Theorem 3.2 for some p, prime divisor of $N-1$. If it is in fact composite, we will say that it is a *p-strong pseudoprime to base a*.

This generalization allows us to choose the most appropriate prime factor of $N-1$ in which the test is used. In the case of generalized Proth numbers $N = Kp^n + 1$ it seems that the prime p should be the most suitable choice, nevertheless, computational experiments reveal that the proportion of q-strong pseudoprimes does not depend significantly on the chosen divisor of $N-1$. Moreover, the classic Miller-Rabin test presents in general less pseudoprimes than the proposed generalization. Nonetheless, this new test can be modified to become a deterministic primality test for numbers $Kp^n + 1$, p prime with $K < p^n$. This modification (presented in practical form in Corollary 4.4) is the main contribution of this paper and will be developed in the following section. Also, since $N-1$ will have in general several prime divisors, it can be natural to combine the new test not only using different bases, but also using different prime divisors of $N-1$. However, computational evidence suggest that it is more convenient to use the test combining different bases rather than different prime divisors of $N-1$. For example, the smallest 2-strong pseudoprime to bases 2 and 3 is 1373653, while there are eight numbers N that are p-strong pseudoprimes to base 2 for any $p \mid N-1$ smaller than 100000; namely: 2047, 3277, 4033, 8321, 65281, 80581, 85489, and 88357.

4. Variations on Pocklington's results

The following result is based on a more general work by Lenstra [12] and can be seen as a generalization of Pocklington's result presented in Theorem 1.3 above. See [11, Proposition 3.15] for details.

Proposition 4.1. *Let $N > 3$ be an integer, and let s be a divisor of $N-1$ which is larger than $\sqrt{N}$ and whose prime factorization is known. If there is an integer a satisfying:*

i) $a^s \equiv 1 \pmod{N}$,
ii) $\gcd(a^{s/q} - 1, N) = 1$ *for each prime divisor q of s,*

then N is prime.

As a direct consequence of this proposition we have the next result.

Theorem 4.2. *Let $N = Kp^n + 1$ where p is a prime. If there exists $1 \le j \le n$ such that*

i) $\Phi_p(2^{Kp^{j-1}}) \equiv 0 \pmod{N}$,
ii) $2j > \log_p(K) + n$,

then N is prime.

Proof. Since $\Phi_p(2^{Kp^{j-1}}) \equiv 0 \pmod{N}$ if and only if $2^{Kp^j} \equiv 1 \pmod{N}$ and $\gcd(a^{Kp^{j-1}} - 1, N) = 1$, we can put $s = p^j$ and $a = 2^K$, so the result follows from Proposition 4.1. □

This theorem can be restated in a more useful form, from the computational point of view, in the following ways.

Corollary 4.3. *Let $N = Kp^n + 1$ where p is a prime number. Let us consider the sequence $S_0 = 2^K$, $S_i = S_{i-1}^p$ for all $i \ge 1$. If for some $j > \frac{1}{2}(\log_p(K) + n)$ it holds that $\Phi_p(S_j) \equiv 0 \pmod{N}$, then N is prime.*

Corollary 4.4. *Let $N = Kp^n + 1$ where p is a prime number. Let us consider the sequence $S_0 = 2^K$, $S_i = S_{i-1}^p$ for all $i \geq 1$. If for some $j > \frac{1}{2}(\log_p(K) + n)$ it holds that $\gcd(S_{j-1} - 1, N) = 1$ and $S_j \equiv 1 \pmod N$, then N is prime.*

Remark 4.5. Note that both results are still true if we replace 2 by any other base a.

5. Algorithm and computational complexity

Using Corollary 4.4, we can describe an algorithm to test the primality of $N := Kp^n + 1$ which requires just one modular exponentiation. Namely:

Algorithm.

INPUT: $K, p, n, a.$; $N := Kp^n + 1$. $S_0 := a^K$.
STEP 1: If $S_0 \equiv 1 \pmod N$
then RETURN: "N is a p-strong-probable prime to base a". STOP.
STEP 2: For $i = 1$ to n
$S_i \equiv S_{i-1}^p \pmod N$
If $S_i \equiv 1 \pmod N$ and $gcd(S_{i-1} - 1, N) = 1$
then Let j:=i. GOTO STEP 3
If $S_i \equiv 1 \pmod N$ and $gcd(S_{i-1} - 1, N) \neq 1$
then RETURN: "N is COMPOSITE" . STOP.
End
RETURN: "N is COMPOSITE". STOP.
STEP 3: If $2j \leq \log_p K + n$
then RETURN: "N is a p-strong-probable prime to base a". STOP.
If $2j > \log_p K + n$ RETURN: "N is PRIME". STOP.

Now, we analyze the complexity of the algorithm above.

Proposition 5.1. *For $N = Kp^n + 1$ with fixed K and p, the complexity of the algorithm above is $\tilde{O}(\log^2 N)$.*

Proof. Only steps 1 and 2 cause complexity, since step 3 is obviously irrelevant.

Complexity of step 1 is that of the modular exponentiation $a^K \pmod N$. Taking into account that products modulo N can be performed by the Schoenhage-Strassen algorithm [16] with complexity $O(\log(N)\log(\log(N))\log(\log(\log(N))))$, this is the complexity of step 1. In step 2, n modular exponentiations with the same complexity as in step 1 are carried out. Thus, since $n = \log_p(\frac{N-1}{K})$, the complexity of this step is $O(\log^2(N)\log(\log(N))\log(\log(\log(N))))$. Summarizing, the whole complexity is $\tilde{O}(\log^2(N)$. □

For generalized Proth numbers, $K < p^n$, let $S_J := a^{Kp^J}$ where

$$J := \left\lfloor \frac{\log_p K + n}{2} \right\rfloor.$$

It is easy to see that if $S_J \not\equiv 1 \pmod N$, then the algorithm always certifies the primality or compositeness of $Kp^n + 1$.

Steps 1 and 2 in the algorithm perform the computation of the power $a^{N-1} \pmod N$ in a controlled way in the sense that if for some $0 \leq i < n$, we have $a^{Kp^i} \equiv 1 \pmod N$ the computation stops. Thus, we can say that the computational

cost of the algorithm is that of one modular exponentiation of the kind a^{N-1} carried out by n modular exponentiations of order p taking into account that, recursively:

$$a^{kp^n} = ((a^k)^{p^{n-1}})^p.$$

For values of p with "many" 1's or "many" 0's in its binary expansion (like Mersenne or Fermat primes), the presented algorithm can use this fact to perform the p-th power in a faster way that with the standard repeat squaring technique; achieving an execution in half the time than the standard modular exponentiation. In fact, consider for instance the search for primes of the form $K \cdot 127^n + 1$; our algorithm requires us to perform n modular exponentiations of the kind b^{127}. For each of them, performed by the standard repeated squaring algorithm 12 modular products are required, but considering that $b^{127} = b^{128}/b$ only 7 products and a division would be required; a 33% save. More generally, for $p = 2^s - 1$ (a Mersenne prime) only s products and a division will be required, while the standard method requires $2(s-1)$ products. Thus, asymptotically, one gets a 50% save. Moreover, even though p is not a Mersenne or Fermat prime, if there are many 1's or 0's in the binary expansion of p, *ad hoc* strategies can be developed in order to optimize the computation.

We will now see that, for moderately big values of n, the probability that the algorithm does not certify the primality of a prime $N = Kp^n + 1$ without choosing more than one base is extremely small and that it decreases with p. This is not the case for the test based in Pocklington's theorem since the use of several bases to certify the primality of N is quite frequent. For this purpose we need the following well-known lemma.

Lemma 5.2. *let $N = Kp^n + 1$ be a prime number, the number of p^s-th powers modulo N (different from 0 and 1) is:*

$$\frac{N-1}{p^s} - 1 = Kp^{n-s} - 1.$$

Using this result, we can prove the following proposition.

Proposition 5.3. *Given a prime number $N = Kp^n + 1$ ($K < p^n$) and a random base $0 < a < n$, the probability that the algorithm returns "p-strong probable prime" is:*

$$\frac{Kp^{\left\lfloor \frac{\log_p(K)+n}{2} \right\rfloor} - 1}{Kp^n - 1}.$$

Proof. The algorithm returns "N is p-strong probable prime" when $J := \left\lfloor \frac{\log_p(K)+n}{2} \right\rfloor$ satisfies that $a^{Kp^J} \equiv 1 \pmod{N}$. This will happen if a is a residual power of order p^{n-J} modulo N. But, by the previous lemma, the probability that this happens is:

$$\frac{Kp^J - 1}{N-2} = \frac{Kp^{\left\lfloor \frac{\log_p(K)+n}{2} \right\rfloor} - 1}{Kp^n - 1}.$$ □

Remark 5.4. Note that if $N = Kp^n + 1$ is prime and K is "much smaller" than p^n, then a random choice of a will most likely determine the primality of N. In particular, this is the case when K is fixed and n increases (which is usually the case when one searches for primes of this form) and the proposition above implies that for big values of n the probability that a prime of the form $N = Kp^n + 1$ is certified as a p-strong probable prime is about $p^{-n/2}$.

Nevertheless, if $p^{n-1} \leq K < p^n$ and N is prime, then the test will give a "p-strong probable prime" with probability approximately equal to $1/p$, which is not very good.

Taking into account that our algorithm requires a number of computations similar to that of Fermat's test, it could be preferable to any algorithm based on Pocklington's test or on its variations. On the other hand, the proposed algorithm certifies primality using, is some cases, less bases than OpenPFGW. For example, for $N = 2 \cdot 3^{1175232} + 1$, the algorithm requires two bases with probability about 8.25×10^{-280365} and OpenPFGW uses the bases 2, 3 and 5 to certify its primality.

Acknowledgement

The authors are grateful to L. M. Pardo Vasallo for his help with computational complexity aspects. We are also grateful to David Broadhurst, who has helped us to better understand the working of OpenPFGW and whose search for primes of the form $2 \cdot 3^n + 1$ has allowed us to value our algorithm is a more appropriate way.

References

[1] Pedro Berrizbeitia and T. G. Berry, *Cubic reciprocity and generalised Lucas-Lehmer tests for primality of* $A \cdot 3^n \pm 1$, Proc. Amer. Math. Soc. **127** (1999), no. 7, 1923–1925, DOI 10.1090/S0002-9939-99-04786-3. MR1487359 (99j:11006)

[2] Pedro Berrizbeitia and T. G. Berry, *Generalized strong pseudoprime tests and applications*, J. Symbolic Comput. **30** (2000), no. 2, 151–160, DOI 10.1006/jsco.1999.0343. MR1777169 (2001f:11201)

[3] Pedro Berrizbeitia, T. G. Berry, and Juan Tena-Ayuso, *A generalization of Proth's theorem*, Acta Arith. **110** (2003), no. 2, 107–115, DOI 10.4064/aa110-2-1. MR2008078 (2004g:11003)

[4] Pedro Berrizbeitia and Boris Iskra, *Deterministic primality test for numbers of the form* $A^2 \cdot 3^n + 1$, $n \geq 3$ *odd*, Proc. Amer. Math. Soc. **130** (2002), no. 2, 363–365 (electronic), DOI 10.1090/S0002-9939-01-06100-7. MR1862113 (2002i:11007)

[5] Pedro Berrizbeitia and Aurora Olivieri, *A generalization of Miller's primality theorem*, Proc. Amer. Math. Soc. **136** (2008), no. 9, 3095–3104, DOI 10.1090/S0002-9939-08-09303-9. MR2407072 (2009g:11164)

[6] Wieb Bosma, *Cubic reciprocity and explicit primality tests for* $h \cdot 3^k \pm 1$, High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams, Fields Inst. Commun., vol. 41, Amer. Math. Soc., Providence, RI, 2004, pp. 77–89. MR2076210 (2005e:11002)

[7] John Brillhart, D. H. Lehmer, and J. L. Selfridge, *New primality criteria and factorizations of* $2^m \pm 1$, Math. Comp. **29** (1975), 620–647. MR0384673 (52 #5546)

[8] Richard Crandall and Carl Pomerance, *Prime Numbers*: *A Computational Perspective*, 2nd ed., Springer, New York, 2005. MR2156291 (2006a:11005)

[9] José María Grau and Antonio M. Oller-Marcén, *An* $\tilde{O}(\log^2(N))$ *time primality test for generalized Cullen numbers*, Math. Comp. **80** (2011), no. 276, 2315–2323, DOI 10.1090/S0025-5718-2011-02489-0. MR2813363 (2012d:11244)

[10] Andreas Guthmann, *Effective primality tests for integers of the forms* $N = k \cdot 3^n + 1$ *and* $N = k \cdot 2^m 3^n + 1$, BIT **32** (1992), no. 3, 529–534, DOI 10.1007/BF02074886. MR1179238 (93h:11008)

[11] Franz Lemmermeyer, *Reciprocity Laws*: *From Euler to Eisenstein*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2000. MR1761696 (2001i:11009)

[12] H. W. Lenstra Jr. and P. Stevenhagen, *Artin reciprocity and Mersenne primes*, Nieuw Arch. Wiskd. (5) **1** (2000), no. 1, 44–54. MR1760775 (2001h:11006)

[13] Théophile Pépin, *Sur la Formule* $2^{2^n} + 1$, C. R. Acad. Sci. Paris, 85:329–331, 1877.

[14] H. C. Pocklington, *The determination of the prime or composite nature of large numbers by fermat's theorem*, Proc. Cambridge Philos. Soc., 18:29–30, 1914.

[15] François Proth. *Théorémes sur les nombre premiers*, C. R. Acad. Sci. Paris, 87:926, 1878.

[16] A. Schönhage and V. Strassen, *Schnelle Multiplikation grosser Zahlen* (German, with English summary), Computing (Arch. Elektron. Rechnen) **7** (1971), 281–292. MR0292344 (45 #1431)
[17] H. C. Williams, *A note on the primality of* $6^{2^n}+1$ *and* $10^{2^n}+1$, Fibonacci Quart. **26** (1988), no. 4, 296–305. MR967648 (89i:11013)
[18] H. C. Williams and C. R. Zarnke, *Some prime numbers of the forms* $2A3^n+1$ *and* $2A3^n-1$, Math. Comp. **26** (1972), 995–998. MR0314747 (47 #3299)

Departamento de Matemáticas, Universidad de Oviedo, Avda. Calvo Sotelo, s/n, 33007 Oviedo, Spain
E-mail address: grau@uniovi.es

Centro Universitario de la Defensa de Zaragoza, Ctra. de Huesca, s/n, 50090 Zaragoza, Spain
E-mail address: oller@unizar.es

Departamento de Matemáticas, Estadística y Computación, Universidad de Cantabria, F. Ciencias, Avda de los Castros s/n, 39005 Santander, Spain
E-mail address: sadornild@unican.es