MATHEMATICS OF COMPUTATION
Volume 80, Number 276, October 2011, Pages 2315–2323
S 0025-5718(2011)02489-0
Article electronically published on March 11, 2011

AN $\tilde{O}(\log^2(N))$ TIME PRIMALITY TEST FOR GENERALIZED CULLEN NUMBERS

JOSÉ MARÍA GRAU AND ANTONIO M. OLLER-MARCÉN

Abstract. Generalized Cullen Numbers are positive integers of the form $C_b(n) := nb^n + 1$. In this work we generalize some known divisibility properties of Cullen Numbers and present two primality tests for this family of integers. The first test is based in the following property of primes from this family: $n^{b^n} \equiv (-1)^b \pmod{nb^n + 1}$. It is stronger and has less computational cost than Fermat's test (to bases b and n) and than Miller-Rabin's test (if b is odd, to base n). Pseudoprimes for this new test seem to be very scarce, only 4 pseudoprimes have been found among the many millions of Generalized Cullen Numbers tested. We also present a second, more demanding, test for which no pseudoprimes have been found. These tests lead to an algorithm, running in $\tilde{O}(\log^2(N))$ time, which might be very useful in the search of Generalized Cullen Primes.

1. Introduction

The first major breakthrough in the general theory of primality testing was achieved by Adleman, Pomerance and Rumely (see [1]) giving a deterministic primality test running in $(\log n)^{O(\log\log\log n)}$ time. This algorithm, later improved by Cohen and Lenstra (see [5]), is known as the APRCL algorithm.

In 2004 three scholars from Kanpur University (Agrawal, Kayal and Saxena) introduced the AKS algorithm (see [2]), which was the first deterministic primality test running in polynomial time. In the second version of their paper they proved that the running time of their algorithm was $\tilde{O}((\log n)^{7.5})$. Nevertheless, and despite being one of the cornerstones of Computational Number Theory, this algorithm has not been very useful in practice. This is because numbers for which the AKS algorithm is faster than the usual ones are beyond current computation capacity. Even the so-called practical versions of the AKS algorithm (see [3], for instance) are not fast enough. As a consequence, prime "hunters" focus on families of integers for which primality can be determined by useful algorithms.

For restricted families of integers, much faster algorithms are known. The Lucas-Lehmer algorithm (see [16]), used for Mersenne Numbers, is deterministic and runs in $\tilde{O}((\log n)^2)$ time. Proth, in [17], also gives an algorithm running in $\tilde{O}((\log n)^2)$ time, which applies to numbers such that $\nu_2(n-1) > \frac{1}{2}\log_2 n$ where $2^{\nu_2(m)}$ is the biggest power of 2 dividing m and provided an integer a is given such that the Jacobi symbol $\left(\frac{a}{n}\right) = -1$. Proth's algorithm is not deterministic for every n. Later,

Received by the editor July 8, 2010 and, in revised form, September 21, 2010.
2010 *Mathematics Subject Classification.* Primary 11Y11, 11Y16, 11A51, 11B99.

Williams [20] or Konyagin and Pomerance [12] extended these techniques to wider families of integers.

Positive integers of the form $n2^n + 1$ are called Cullen Numbers and were first introduced by Father James Cullen in 1905 (see [6], [9, B20] or [13] for instance). Primes of this form are very scarce (in fact, in [10] it is shown that almost all Cullen Numbers are composite). Pseudoprimality of the Cullen Numbers was addressed from the statistical point of view in [15]. Also, primality criteria suitable for Cullen Numbers have been presented and discussed in [18]. The only known Cullen Primes are those for n equal to:

1, 141, 4713, 5795, 6611, 18496, 32292, 32469, 59656, 90825, 262419,
361275, 481899, 1354828, 6328548, 6679881 (sequence A005849 in OEIS).

The largest known Cullen Prime is $6679881 \times 2^{6679881} + 1$. It is a megaprime with 2,010,852 digits and was discovered by a *PrimeGrid* participant from Japan. It is the fifteenth biggest known prime. In [4] a sufficient condition for primality for Cullen Numbers was given.

A quite straightforward generalization of these numbers are the so-called Generalized Cullen Numbers (GCN for short) which are integers of the form $C_b(n) := nb^n + 1$. This family was introduced by H. Dubner in [8] and is one of the main sources for prime number "hunters". There exists a distributed computing project (http://www.primzahlenarchiv.de/) to find Generalized Cullen Primes (GCP for short) with the biggest GCP being $C_{151}(139948)$, an integer with 304,949 digits. Noteworthy, for 29 values of b smaller than 200 no GCP has been found.

To date, no specific primality test for Generalized Cullen Numbers has been introduced. This is the main goal of this work. The paper is organized as follows. In the second section we generalize some known divisibility properties of Cullen Numbers. In Section 3 we present two probabilistic primality tests for GCN. The first test (TEST1) is based on the fact that $n^{b^n} \equiv (-1)^b \pmod{C_b(n)}$ for every GCP $C_b(n)$. This test is stronger and has less computational cost than Fermat's test (for bases b and n) and than Miller-Rabin's test (if b is odd, to base n) and seems to have very few pseudoprimes. Thus, the probability of error is extremely small: among the millions of numbers tested, only four pseudoprimes have been found. We also present another test (TEST2), more demanding than TEST1, for which no pseudoprime has been found. In the fourth section we present a sufficient condition for primality based on TEST2, which has allowed us to certify the primality of nearly every known GCP with the use of very modest technological resources in just a few minutes. We are convinced that, with the use of better technology directed to an efficient modular exponentiation, this algorithm would help to break records for GCP. Finally, in Section 5, we establish the computational complexity of the presented tests; we give the running time of our algorithm for various cases; and we close the paper with an important conjecture.

2. Some divisibility properties

Although the main goal of the paper is to present primality tests for Generalized Cullen Numbers, it is interesting to study some divisibility properties of such numbers. First of all, we are interested in finding families of composite Generalized Cullen Numbers. A first result in this direction goes as follows.

Proposition 1. *Let $n_b(k,p) = (b^k - k)(p-1) - k$ and let p be a prime not dividing b. Then p divides $C_b(n_b(k,p))$.*

Proof. It is clear that $n_b(k,p) \equiv -b^k \pmod{p}$. Now, since $b^{p-1} \equiv 1 \pmod{p}$ we have that:

$$C_b(n_b(k,p)) \equiv -b^{(b^k-k)(p-1)} + 1 \equiv 0 \pmod{p}. \qquad \square$$

Observe that, if p divides $C_b(n)$, then p does not divide b, so if $n \neq n_b(k,p)$, we can apply the previous proposition to find another composite Generalized Cullen Number with the same base. Nevertheless, this process can be applied only in one step; i.e., given a prime divisor of $C_b(n)$ we only find (at most) another m such that p also divides $C_b(m)$. Thus, it is interesting to find a process that allows us to construct infinite families of Generalized Cullen Numbers divisible by the same prime. The next proposition goes in this direction.

Proposition 2. *Let p be a prime dividing $C_b(n)$ and let $h_p = exp_p(b)$; i.e., the smallest integer such that $b^{h_p} \equiv 1 \ (mod\, p)$. Then p also divides $C_b(n + mph_p)$ for every integer m.*

Proof. If $m = 1$, we have:

$$C_b(n + ph_p) = b^{ph_p}(C_b(n) - 1) + ph_p b^{n+ph_p} + 1 \equiv nb^n + 1 = C_b(n) \equiv 0 \pmod{p}$$

and the result follows inductively. $\square$

The propositions above generalize known results for the case $b = 2$ that can be found in [11] and [7].

Now, given two Generalized Cullen Numbers, it can be interesting to study their common divisors. For example, if we consider $C_b(n)$ and $C_\beta(n)$, it is easy to see that any common divisor of these numbers must also divide $|b^n - \beta^n|$. If we restrict ourselves to Generalized Cullen Numbers of the same base, we can present a more interesting result (see [14] for related considerations).

Proposition 3. *Let $C_b(n)$ and $C_b(m)$ be two different Generalized Cullen Numbers with $\alpha n = \beta m$. If d is a common divisor of $C_b(n)$ and $C_b(m)$, then d also divides $|n^\alpha + (-1)^{\alpha+\beta-1} m^\beta|$.*

Proof. First of all, note that d cannot divide b. Also, since d is a common divisor, it must, assuming $n \geq m$, divide $|C_b(n) - C_b(m)| = b^n|n - mb^{m-n}|$. Consequently, d divides $|n - mb^{m-n}|$.

Now, d also divides $nC_b(n) = n^2b^n + n$ and it follows that d divides $|n^2b^n + mb^{m-n}|$. If, for instance, $n < m - n$, we get that d divides $|n^2 - mb^{m-2n}|$. If $m - n < n$, we would get that d divides $|m + n^2b^{2n-m}|$.

Clearly, we can proceed in this way until both powers of b are the same. Furthermore, we will need to perform the previous computations exactly $\alpha + \beta - 1$ times and at every step, the middle sign changes and the exponent of either m or n increases by 1. Thus, the desired result is finally obtained. We omit the details. $\square$

It is worth remarking that the previous proposition does not depend on b. Thus, if $A_{m,n} = |n^\alpha + (-1)^{\alpha+\beta-1} m^\beta|$ is a prime, then $C_b(n)$ and $C_b(m)$ are either coprime or their greatest common divisor is $A_{m,n}$ for every value of b.

3. Two primality tests

This section is devoted to presenting two probabilistic primality tests for Generalized Cullen Numbers. The first one will be compared with Fermat and Miller-Rabin for some witnesses. The second one will be the basis of a sufficient condition for primality which will be introduced in the next section.

The proposition below presents the property of GCP in which TEST1 will be based.

Proposition 4. *If $C_b(n)$ is prime, then $n^{b^n} \equiv (-1)^b \pmod{C_b(n)}$.*

Proof. Clearly, $nb^n \equiv -1 \pmod{C_b(n)}$. On the other hand, since b and $C_b(n)$ are coprime, we have that $b^{nb^n} \equiv 1 \pmod{C_b(n)}$.

Now, taking this into account:

$$-(-1)^b \equiv (-1)^{b^n-1} \equiv (nb^n)^{b^n-1} \equiv n^{b^n-1}b^{nb^n-n} \equiv n^{b^n-1}b^{-n} \pmod{C_b(n)},$$

from where it follows that:

$$n^{b^n} \equiv -(-1)^b nb^n \equiv (-1)^b \pmod{C_b(n)},$$

where negative exponents make sense since we are working over a field. □

Let us now relate this test with Fermat and Miller-Rabin primality tests. In fact, we will see that our test is stronger than both of them in the sense that if a Generalized Cullen Number passes our test, it will also pass Fermat and Miller-Rabin tests (the latter only for odd b) for certain choices of the base.

Proposition 5. *If $n^{b^n} \equiv (-1)^b \pmod{C_b(n)}$ for an odd $C_b(n)$, then $C_b(n)$ is a Fermat (or weak) probable prime to base n.*

Proof. We have that:

$$n^{C_b(n)-1} = n^{nb^n} = (n^{b^n})^n \equiv (-1)^{bn} = 1 \pmod{C_b(n)},$$

since bn must be even. □

Remark. Although TEST1 is very similar to Fermat's test to base n, it has turned out to be more subtle. We have only found four pseudoprimes for our test. Namely: $C_{80}(2) = 12801$, $C_{3570}(3) = 136497879001$, $C_{570}(4) = 422240040001$ and $C_{1470}(4) = 18677955240001$. On the other hand, three more pseudoprimes ($C_7(4)$, $C_{63336}(2)$ and $C_{2355990}(2)$) appear for Fermat's test to base n. Observe that $C_{1470}(4)$ and $C_{570}(4)$ are Carmichael Numbers.

Proposition 6. *If $n^{b^n} \equiv (-1)^b \pmod{C_b(n)}$, then $C_b(n)$ is a Fermat (or weak) probable prime to base b.*

Proof. Since b and n are coprime with $C_b(n)$, they both have an inverse modulo $C_b(n)$. Moreover, $n^{-1} \equiv -b^n \pmod{C_b(n)}$.

Now:

$$(-1)^b \equiv n^{b^n} \equiv (-b^{-n})^{b^n} \equiv (-1)^b b^{-nb^n} \pmod{C_b(n)}.$$

Thus, $b^{-nb^n} \equiv 1 \pmod{C_b(n)}$ and, consequently, $b^{C_b(n)-1} = b^{nb^n} \equiv 1 \pmod{C_b(n)}$. □

Remark. Although TEST1 is theoretically stronger than Fermat's test to base b, we have not found pseudoprimes for this test which are not pseudoprimes for TEST1.

Proposition 7. *Let b be an odd integer. If $n^{b^n} \equiv (-1)^b (mod\ C_b(n))$, then $C_b(n)$ is a strong probable prime to base n; i.e., it passes the Miller-Rabin primality test.*

Proof. Put $n = 2^s k$ with k being an odd integer and $s \geq 0$. Then, $C_b(n) = 2^s k b^n + 1 = 2^s m + 1$ with $m = kb^n$. We have that m is odd and, moreover, $n^m = n^{kb^n} \equiv (-1)^{bk} \equiv -1 \pmod{C_b(n)}$. Consequently $C_b(n)$ passes the Miller-Rabin test to base n as claimed. $\square$

Remark. The previous result is no longer true for even values of b. For instance, $C_{80}(2)$ and $C_{3570}(3)$ pass TEST1 but do not pass the Miller-Rabin test for $n = 2$ and 3, respectively.

The following result is stronger than Proposition 4 and will give rise to another probabilistic test that we will denote by TEST2. This test involves cyclotomic polynomials of prime index and is more demanding than TEST1. It will be the basis of a sufficient condition for primality in the next section.

Theorem 1. *Let p be a prime number and $b = p^m b'$ with p not dividing b'. If $C_b(n) := nb^n + 1$ is prime, then one of the following holds:*

i) $(-n)^{\frac{b^n}{p^i}} \equiv 1$ *(mod $C_b(n)$) for every $i \in \{0, \dots, nm\}$.*
ii) *There exists $K < mn$ such that $(-n)^{\frac{b^n}{p^i}} \equiv 1$ (mod $C_b(n)$) for every $i \in \{0, \dots, K\}$ and $\Phi_p((-n)^{\frac{b^n}{p^{K+1}}}) \equiv 0$ (mod $C_b(n)$), where Φ_p is the p-th cyclotomic polynomial.*

Proof. Proposition 4 implies that $(-n)^{\frac{b^n}{p^0}} \equiv 1 \pmod{C_b(n)}$. If i) does not hold, let $K < mn$ be the biggest integer such that $(-n)^{\frac{b^n}{p^K}} \equiv 1 \pmod{C_b(n)}$. Put $x = (-n)^{\frac{b^n}{p^{K+1}}}$. Then $0 \equiv x^p - 1 = (x-1)\Phi_p(x) \pmod{C_b(n)}$. The maximality of K implies that $x - 1 \not\equiv 0 \pmod{C_b(n)}$ so, since $C_b(n)$ is prime, $\Phi_p(x) \equiv 0$ (mod $C_b(n)$) and the proof is complete. $\square$

Every Generalized Cullen Number satisfying Theorem 1 for some p, prime divisor of b, will be certified as a probable prime for TEST2 to base p. If it is composite, we will name it as a pseudoprime for TEST2 to base p. Among the four pseudoprimes found for TEST1, the only one that passes TEST2 for some prime divisor of b is the Carmichael Number $C_{1470}(4)$ which is a pseudoprime for TEST2 to base 2. Nevertheless, $C_{1470}(4)$ is certified as composite since it does not pass TEST2 for any other prime divisor of 1470. The other three pseudoprimes for TEST1 do not pass TEST2 for any base. The authors have not found any composite Generalized Cullen Number passing TEST2 for every prime divisor of b. In fact they conjecture that such GCN does not exist.

4. A sufficient condition for primality

We will now see that passing TEST2, together with a bounding condition on K, gives a sufficient condition for primality.

Theorem 2. *Let $b = p_1^{r_1} \cdots p_s^{r_s}$ be a positive integer. If there exist a prime p_j dividing b and $K \leq nr_j$ such that:*

i) $\Phi_{p_j}((-n)^{\frac{b^n}{p_j^{K+1}}}) \equiv 0$ *(mod $C_b(n)$),*
ii) $nr_j - K > \frac{1}{2}\log_{p_j} nb^n = \frac{1}{2}\log_{p_j} n + \frac{n}{2}\log_{p_j} b,$

then $C_b(n)$ is prime.

Proof. If q is a prime divisor of $C_b(n)$, we have that $\Phi_{p_j}((-n)^{\frac{b^n}{p_j^{K+1}}}) \equiv 0 \pmod q$. It follows that the order of $(-n)^{\frac{b^n}{p_j^{K+1}}}$ in $\mathbb{Z}_q^*$ is exactly p_j and, consequently, the order of $-n$ is a divisor of $\frac{b^n}{p_j^K} = p_1^{nr_1} \cdots p_j^{nr_j-K} \cdots p_s^{nr_s}$. Moreover, $(-n)^{\frac{b^n}{p_j^{K+1}}}$ is not congruent with 1. For if it was, then $0 \equiv \Phi_{p_j}(1) \pmod q$ which is a contradiction, q and p_j being coprime. Thus, the order of $-n$ does not divide $\frac{b^n}{p_j^{K+1}} = p_1^{nr_1} \cdots p_j^{nr_j-K-1} \cdots p_s^{nr_s}$. As a consequence, the order of $-n$ is a multiple of $p_j^{nr_j-K}$ and it follows that $p_j^{nr_j-K} | q-1$. Finally we obtain that:

$$q \geq p_j^{nr_j-K} + 1 > p_j^{\frac{1}{2}\log_{p_j} nb^n} + 1 = \sqrt{nb^n} + 1 \geq \sqrt{C_b(n)}.$$

This must hold for every prime divisor q of $C_b(n)$. Clearly it is a contradiction unless $q = C_b(n)$ is its only prime divisor and the result follows. □

If b is a prime-power, the previous result can be slightly simplified in the following way.

Corollary 1. *Let $b = p^m$ with p a prime. If $\Phi_p((-n)^{p^{K-1}}) \equiv 0 \ (mod\ C_b(n))$ with $nm \geq K > \frac{mn}{2} + \frac{1}{2}\log_p(n)$, then $C_b(n)$ is prime.*

Remark. The previous corollary generalizes [4] for $b = 2$ and $m = 1$. Observe that in such case, $\Phi_2((-n)^{2^{K-1}}) = n^{2^{K-1}} + 1$.

5. Computational complexity

Let us present the pseudo code of an algorithm implementing TEST1 and TEST2. We will also justify its polynomial complexity.

Algorithm (TEST1 and TEST2 to base P)**.**
INPUT: n and $b = p_1^{r_1} \dots p_s^{r_s}$; $M := r_j$; $P := p_j$ and $N := nb^n + 1$
***Step 1**: If $n^{b^n} \not\equiv (-1)^b \ (mod\ N)$*
then RETURN: N is a COMPOSITE NUMBER. Stop.
***Step 2**: If $n^{b^n} \equiv (-1)^b \ (mod\ N)$*
then RETURN: N is a PROBABLE PRIME for TEST1
and go to Step 3.
***Step 3**: Compute $K := \max\{i \leq nM \mid ((-n)^{\frac{b^n}{P^i}} \equiv 1 \ (mod\ N)\}$*
***Step 4**: If $K = nM$*
then RETURN: N is a PROBABLE PRIME for TEST2 to base P. Stop.
***Step 5**: If $K < nM$ and $\Phi_P((-n)^{\frac{b^n}{P^{K+1}}}) \equiv 0 \ (mod\ N)$*
then RETURN: N is a PROBABLE PRIME for TEST2 to base P
and go to Step 7.
***Step 6**: If $K < nM$ and $\Phi_P((-n)^{\frac{b^n}{P^{K+1}}}) \not\equiv 0 \ (mod\ N)$*
then RETURN: N is a COMPOSITE NUMBER. Stop.
***Step 7**: If $nM - K > \frac{1}{2}\log_P(N-1)$*
then RETURN: N is a PRIME NUMBER. Stop.

The correctness of the algorithm is a straightforward consequence of Proposition 4 and Theorems 1 and 2. To study its complexity, we first need to present a technical lemma.

Lemma 1. *Let $A = \{a_0, a_1, \ldots, a_n\}$ be a set with $a_n \neq a_0$ and with the property $a_s \neq a_0 \Rightarrow a_{s+1} \neq a_0$. If the computation of each a_i is of complexity $O(h)$, then the complexity of computing* $\max\{i \mid 0 \leq i \leq n,\ a_i = a_0\}$ *is $O(h \log_2(n))$.*

Proof. If $a_{\lfloor \frac{n}{2} \rfloor} = a_0$, then the maximum lies in the second half of the interval. Otherwise, it is in the first half. Iterating this process, the maximum will be found in about $\log_2 n$ steps and the result is then straightforward. □

Theorem 3. *If $N := nb^n + 1$, the complexity of the algorithm above is*

$$O(\log^3(W(N)) \log^2(N)) \subset \widetilde{O}(\log^2(N)),$$

where W is Lambert's W function; i.e., the inverse function of $f(w) = we^w$.

Proof. The complexity of steps 1 and 2 is that of the modular exponentiation $n^{(N-1)/n} \pmod N$. Taking into account that $O(n) = O(W(N)) \subset O(\log(N))$ and that products modulo N can be performed by the Schoenhage-Strassen algorithm (see [19]) with complexity

$$O(\log(N) \log(\log(N)) \log(\log(\log(N)))),$$

we get the complexity of these two steps to be:

$$T(N) := O\left(\log\left(\frac{N}{W(N)}\right) \log(N) \log(\log(N)) \log(\log(\log(N)))\right).$$

Step 3 requires performing at most $\log(nM)$ modular exponentiations with complexity analogous to that of step 1. Consequently, by the lemma above, the total complexity will be

$$O(T(N) \log(W(N))) \subset O(\log^3(W(N)) \log^2(N)) \subset \widetilde{O}(\log^2(N)).$$

Steps 4 through 7 do not increase the complexity since they are mere verifications of equalities and inequalities. □

From a computational point of view, this work is promising because it presents primality tests for GCN whose computational complexity is the same as that of modular exponentiation. This is the case, since only a relatively small number of modular power has to be computed. Other tests of general character are clearly inferior. For example, the Lucas test, which seems appropriate here due to the easy factorization of $C_b(n) - 1$, has problems if n has many prime divisors. Although the technology used by the authors limits them to using the *PowerMod* command in Mathematica® 6.0 (in an Intel core2 Duo P7450 @ 2.13 GHz with 4Gb of RAM), they have been able to certify primality for nearly every known GCP. We are sure that the tests presented in this work, using a better technology focused on efficient modular exponentiation, will allow to break records in the family of GCN.

Just to enlighten what we have just said, let us compare our primality test with the *PrimeQ* command implemented in Mathematica®. According to Mathematica® manual, this command uses the multiple Rabin-Miller test in bases 2 and 3 combined with a Lucas pseudoprime test. Below we present the running times for the certification of some known GCP (for $b = 3$, 8 and 20). We also show the number of modular exponentiations performed in the third step of the algorithm.

Note that *PrimeQ* is a probabilistic test (although according to Mathematica® manual no pseudoprime for this test has been found). In the examples above our test certified primality in a deterministic way and faster (except for two cases)

b=3, n =	1400	1850	2848	4874	7268	19290	337590
Number of digits of $C_3(n)$	672	886	1363	2330	3472	9208	161077
$K+1$ (Step 3)	1	2	2	1	1	1	?
TEST2 to base 3 (Time in s.)	0.06	0.17	0.56	1.49	4.55	54.16	?
PrimeQ (Time in s.)	0.09	0.17	0.50	2.04	6.06	71.19	?

b=8, n=	5	17	23	1911	20855	35945	42816
Number of digits of $C_8(n)$	6	17	23	1730	18839	32467	38672
$K+1$ (Step 3)	2	2	2	3	6	5	2
TEST2 to base 2 (Time in s.)				0.87	788.	2811.	2112.
PrimeQ(Time in s.)				0.93	464.	1933.	2930.

b=20, n=	3	6207	8076	22356
Number of digits of $C_{20}(n)$	5	8080	10512	29091
$K+1$ (Step 3)	1	1	1	2
TEST2 to base 5 (Time in s.)	0.	32.1	62.4	1347.
PrimeQ (Time in s.)	0.	50.88	99.6	1396.

than *PrimeQ*. The deterministic version of *PrimeQ* implemented in Mathematica®, *ProvablePrimeQ*, was so slow that it is not worth presenting the comparison.

To finish, we have to point out that the presented algorithm ultimately relies on the choice of a prime divisor of b. Also note that, for a fixed p, if the output of the presented algorithm is a PRIME NUMBER, the tested integer is certainly a prime, but it could be possible that it produces a false negative (i.e., a genuine GCP may not be certified as such). Nevertheless, computational evidence suggests that this is not the case for moderately big values of n; in fact, such primes have been found only for $n < b$. Moreover, the experiments also suggest that in step 3 the value of K is always very small with respect to n. These considerations lead us to the following conjecture.

Conjecture. *If $n > b$, there always exists p, a prime divisor of b, such that the algorithm* (*using base p*) *certifies the primality or the compositeness of $C_b(n)$. Note that, if b is a prime power, there is only one choice for p.*

Acknowledgements

We are grateful to L.M. Pardo Vasallo for his help in computational complexity aspects. We are also grateful to P. Berrizbeitia and J.G. Fernandes for providing the preprint of their paper [4] that inspired this work. Finally the authors wish to thank the anonymous referees for their useful comments and references which have helped us to improve the paper.

References

1. Leonard M. Adleman, Carl Pomerance, and Robert S. Rumely, *On distinguishing prime numbers from composite numbers*, Ann. of Math. (2) **117** (1983), no. 1, 173–206. MR683806 (84e:10008)
2. Manindra Agrawal, Neeraj Kayal, and Nitin Saxena, *PRIMES is in P*, Ann. of Math. (2) **160** (2004), no. 2, 781–793. MR2123939 (2006a:11170)
3. Pedro Berrizbeitia, *Sharpening "PRIMES is in P" for a large family of numbers*, Math. Comp. **74** (2005), no. 252, 2043–2059 (electronic). MR2164112 (2006e:11191)
4. Pedro Berrizbeitia and José Gregorio Fernandes, *Observaciones sobre la primalidad de los números de cullen*, Short communication in "Terceras Jornadas de Teoría de Números" (http://campus.usal.es/ tjtn2009/doc/abstracts.pdf).
5. H. Cohen and H. W. Lenstra, Jr., *Primality testing and Jacobi sums*, Math. Comp. **42** (1984), no. 165, 297–330. MR726006 (86g:11078)
6. James Cullen, *Question 15897*, Educ. Times (1905), no. Dec., 534.
7. A. Cunningham and H.J. Woodall, *Factorisation of* $Q = (2^q \mp q)$ *and* $(q2^q \mp 1)$, Messenger Math. **47** (1917), 1–38.
8. Harvey Dubner, *Generalized Cullen numbers*, J. Recreat. Math. **21** (1989), 190–194.
9. Richard K. Guy, *Unsolved problems in number theory*, third ed., Problem Books in Mathematics, Springer-Verlag, New York, 2004. MR2076335 (2005h:11003)
10. C. Hooley, *Applications of sieve methods to the theory of numbers*, Cambridge University Press, Cambridge, 1976, Cambridge Tracts in Mathematics, No. 70. MR0404173 (53:7976)
11. Wilfrid Keller, *New Cullen primes*, Math. Comp. **64** (1995), no. 212, 1733–1741, S39–S46, With a biographical sketch of James Cullen by T. G. Holt and a supplement by Keller and Wolfgang Niebuhr. MR1308456 (95m:11015)
12. Sergei Konyagin and Carl Pomerance, *On primes recognizable in deterministic polynomial time*, The mathematics of Paul Erdős, I, Algorithms Combin., vol. 13, Springer, Berlin, 1997, pp. 176–198. MR1425185 (98a:11184)
13. Michal Křížek, Florian Luca, and Lawrence Somer, *17 lectures on Fermat numbers*, CMS Books in Mathematics/Ouvrages de Mathématiques de la SMC, 9, Springer-Verlag, New York, 2001, From number theory to geometry, With a foreword by Alena Šolcová. MR1866957 (2002i:11001)
14. F. Luca, *On the greatest common divisor of two Cullen numbers*, Abh. Math. Sem. Univ. Hamburg **73** (2003), 253–270. MR2028519 (2004i:11001)
15. Florian Luca and Igor E. Shparlinski, *Pseudoprime Cullen and Woodall numbers*, Colloq. Math. **107** (2007), no. 1, 35–43. MR2283130 (2007i:11127)
16. Édouard Lucas, *Sur la recherche des grands nombres premiers*, Assoc. Francaise p. l'Avanc. des Science. Comptes Rendus (1876), no. 5, 61–68.
17. Francois Proth, *Théorèmes sur les nombres premiers*, Comptes Rendus Acad. des Sciences, Paris (1878), no. 87, 926.
18. Raphael M. Robinson, *A report on primes of the form* $k \cdot 2^n + 1$ *and on factors of Fermat numbers*, Proc. Amer. Math. Soc. **9** (1958), 673–681. MR0096614 (20:3097)
19. A. Schönhage and V. Strassen, *Schnelle Multiplikation grosser Zahlen*, Computing (Arch. Elektron. Rechnen) **7** (1971), 281–292. MR0292344 (45:1431)
20. Hugh C. Williams, *Édouard Lucas and primality testing*, Canadian Mathematical Society Series of Monographs and Advanced Texts, 22, John Wiley & Sons Inc., New York, 1998, A Wiley-Interscience Publication. MR1632793 (2000b:11139)

Department of Mathematics, University of Oviedo, Avda. Calvo Sotelo s/n, 33007, Oviedo, Spain

E-mail address: `grau@uniovi.es`

University of Zaragoza, Department of Mathematics, C/Pedro Cerbuna 12, 50009 Zaragoza, Spain

E-mail address: `oller@unizar.es`