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

JOSÉ MARÍA GRAU AND ANTONIO M. OLLER-MARCÉN

Abstract. In this paper we generalize the classical Proth's theorem for integers of the form $N = Kp^n + 1$. For these families, we present a primality test whose computational complexity is $\widetilde{O}(\log^2(N))$ and, what is more important, that requires only one modular exponentiation similar to that of Fermat's test. Consequently, the presented test improves the most often used one, derived from Pocklington's theorem, which usually requires the computation of several modular exponentiations together with some GCD's.

AMS 2000 Mathematics Subject Classification: 11Y11,11Y16,11A51,11B99

1. Introduction

In 1877 P. Pepin (see [18]) presented the following result about the primality of Fermat numbers:

Theorem 1 (Pepin, 1877)**.** *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 $3^{\frac{F_n-1}{2}} \equiv -1$ (mod 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 proved the following primality criterion for number of the form $N = K2^n + 1$, where K is odd and $K < 2^n$ (Proth numbers)

Theorem 2 (Proth, 1878)**.** *Let $N = K2^n + 1$, where K is odd and $K < 2^n$. If $a^{\frac{N-1}{2}} \equiv -1$ (mod N) for some $a \in \mathbb{Z}$, then N is prime.*

The next important step is the following 1914 result by Pocklington (see [17]), which is the first generalization of Proth's theorem suitable for numbers of the form $N = Kp^n + 1$:

Theorem 3 (Pocklington, 1914)**.** *Let $N = Kp^n + 1$ con $K < p^n$. If, for some $a \in \mathbb{Z}$:*

i) $a^{N-1} \equiv 1$ *(mod 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's (Proth.exe) for the search of Proth and generalized Proth ($N = Kp^n + 1$) primes. Other software based in a variation of Pocklington's Theorem presented by Brillhart, Lehmer and Selfridge (see [10] or [12]) is OpenPFGW with which some records have been broken in different families

of integers. For instance, David Broadhurst has recently broken the record for the family $N = 2 \cdot 3^n + 1$ (sequence A003306 in the OEIS) certifying primality for $n = 1175232$, a number with 560729 digits and the 87-th biggest known prime (see for instance http://primes.utm.edu/primes/lists/all.txt). An 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 numbers for a variety of primes p (see [5, 6, 7]). Even though similar criteria had been previously presented by H.C. Williams and his collaborators (see [23, 22]), the methodology used by Berrizbeitia et al. shows more clear and efficient. For these generalizations an analogous of Legendre symbol, the *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 present technical difficulties, mainly due to the fact that the ring $\mathbb{Z}[e^{2\pi i/m}]$ is not a UFD in general. Other authors, such A. Guthmann (see [14]) and W. Bosma (see [9]), have also given generalizations of Proth's theorem using similar techniques but limited to the case $p = 3$.

Our main contribution is a primality criterion for integers of the form $N = Kp^n + 1$ with p being any prime and $K < p^n$, using techniques similar to those in [13] for generalized Cullen Numbers ($N = np^n + 1$). These techniques do not require the use of any m-th power residue symbol or higher order law of reciprocity. In this way we have achieved an even more clear and efficient methodology than that of Berrizbeitia. In fact, our primality criterion requires only one modular exponentiation a^{N-1} without a previous search of a suitable a.

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 (Proth Prime), then half the values of 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 $(\frac{a}{N}) = -1$. This observation is captured in the following version of Proth's theorem:

Theorem 4 (Proth, 1878)**.** *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 been yet exhibited. We do so in the following result. In what follows $\Phi_p(X)$ will denote the p-th cyclotomic polynomial.

Theorem 5. *Let $N = Kp^n + 1$, where p is a prime, $K < p^n$ and $\gcd(K, p) = 1$. Assume that $a \in \mathbb{Z}$ is a p-th power non-residue, 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 $p^n \leq K$ a contradiction. □

The theorem above can be restated in the following way.

Theorem 6. *Let $N = Kp^n + 1$, where p is a prime and $\gcd(K, p) = 1$. If $p^n > K$, then:*

$\Phi_p(a^{\frac{N-1}{p}}) \equiv 0 (mod\ N) \Leftrightarrow N$ *is prime and a is a p-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 (like 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, only $\frac{1}{p}$ of the possible choices for a is a p-th power residue modulo N. 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 [20] test applies to integers in the form $N = K2^n + 1$ (K odd) and is based in Fermat's little theorem and in the fact that, the only solutions of $x^2 \equiv 1 \pmod p$ (p prime) are $x \equiv \pm 1 \pmod p$. In fact we have the following (see [12, Theorem 3.5.1.]):

Theorem 7. *Let $N = K2^n + 1$ be prime. If $a > 1$, then one of the following holds:*

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

This probabilistic test, in spite of being more demanding than Fermat's test, presents many pseudoprimes (called strong 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 to certify the primality of the numbers that pass it.

We must point out that the generalization of Miller-Rabin test is really simple, even though more than two decades passed by until the first publication in this direction. Berrizbeitia and Berry (see [4]) generalized the Strong Pseudoprime Test introducing the concept ω-prime to base a and more recent work by Berrizbeitia and Olivieri (see [8]) goes in the same direction. Nevertheless, we think that these works do not present a genuine generalization. In fact, Miller-Rabin test admits a very natural generalization for integers in the form $N = Kp^n + 1$ with p prime, K even and $\gcd(K, p) = 1$. This generalization (that we shall call the p-Miller-Rabin test) is based in the following result:

Theorem 8. *Let p be a prime number and K be and even number with* $\gcd(K,p)=1$. *If $N=Kp^n+1$ is prime, then for every integer $a>1$ such that* $\gcd(a,N)=1$ *one of the following holds:*

i) $a^K \equiv 1$ *(mod N).*
ii) *There exists* $0 \leq j \leq n-1$ *such that* $\Phi_p(a^{Kp^j}) \equiv 0$ *(mod 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 1. A *p-strong probable prime to base a* is a number satisfying conditions i) and ii) of Theorem 9 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 of Miller-Rabin test allows to choose the most appropriate prime factor of $N-1$ in which to base the test. 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 number 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 Proth numbers ($K<2^n$) and generalized Proth numbers ($N=Kp^n+1$ with $K<p^n$). This modification 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 makes sense to combine the new test not only using different bases, but also using different prime divisors of $N-1$. This idea suggests the following definition.

Definition 2. A p-strong probable prime (resp. p-strong pseudoprime) to base a for every p prime divisor of $N-1$, will be denoted as a *complete strong probable prime* (resp. *complete strong pseudoprime*) *to base a.*

Unfortunately, although the concept of complete strong probable prime is more subtle than that of p-strong probable prime, computational evidence suggest that it is more convenient to use the test combining different bases rather than different prime divisors of $N-1$. To illustrate this statement it is enough to point out that the smallest 2-strong pseudoprime to bases 2 and 3 is 1373653, while there are 10 complete strong pseudoprimes to base 2 smaller than that number; namely: 2047, 3277, 4033, 8321, 65281, 80581, 85489, 88357, 104653 and 130561.

4. A sufficient condition for the primality of generalized Proth numbers.

We will now see that passing the p-Miller-Rabin test, together with a bounding condition on j (see Theorem 8), gives a sufficient condition for primality.

Theorem 9. *Let $N=Kp^n+1$ where p is a prime and* $\gcd(K,p)=1$. *If there exists $1 \leq j \leq n$ such that:*

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

Then N is prime.

Proof. Put $X = 2^K$, then $X^{p^j} \equiv 1 \pmod N$. Let $q \leq \sqrt{N}$ be a prime divisor of N. It follows that the order of X in Z_q^* is exactly p^j. Consequently $p^j | q-1$ and $p^j < q \leq \sqrt{N}$ from which it follows that $p^{2j} < N = Kp^n + 1$. Finally, if $p^{2j} \leq Kp^n$ then $2j \leq \log_p K + n$; a contradiction and the proof is complete. □

Remark 1. The theorem above is still true if we replace 2 by any other base a. It is enough to put $X = a^K$ in the proof.

Corollary 1. *Let $N = Kp^n + 1$ where p is a prime number with $\gcd(K, p) = 1$. 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 $\Phi_p(S_j) \equiv 0$ (mod N), then N is prime.*

If we consider the case $p = 2$; i.e., the classical Proth numbers, then we get the following corollary.

Corollary 2. *Let $N = K2^n + 1$ with K an odd integer. Let us consider the sequence $S_0 = 2^K$, $S_i = S_{i-1}^2$ for all $i \geq 1$. If for some $j > \frac{1}{2}(\log_2(K) + n)$ it holds that $S_j \equiv -1$ (mod N), then N is prime.*

5. Algorithm and Computational complexity

Since 2004, when the polynomial time AKS algorithm was presented (see [2]), primality algorithms of general nature were ostracized. That was the case of the deterministic primality test running in $(\log n)^{O(\log\log\log n)}$ time presented by Adleman, Pomerance and Rumely (see [1]). This algorithm, later improved by Cohen and Lenstra (see [11]), is known as the APRCL algorithm. Nevertheless, and despite being one of the cornerstones of Computational Number Theory, AKS algorithm has not been very useful in practice. This is because numbers for which 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 in families of integers for which primality can be determined by useful algorithms. For restricted families of integers much faster algorithms are known, the most celebrated being the Lucas-Lehmer algorithm (see [16]), used for Mersenne Numbers, which runs in $\tilde{O}((\log n)^2)$ time. Proth, in [19], gives an algorithm running also 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, Williams [24] or Konyagin and Pomerance [15] have extended these techniques to wider families of integers.

Unless a surprising discovery is made, the computational complexity of any primality test has a lower bound given by the complexity of the modular exponentiation required by Fermat's test. With this idea in mind, the best that a primality test for an integer N can do is to run in $O(\log^2(N)\log(\log(N))\log(\log(\log(N))))$ time. However, even for this complexity, there can be great differences between two different tests depending on the number of modular exponentiations a^{N-1} required. Below we describe an algorithm implementing Corollary 1 which, in fact, requires just one modular exponentiation of the kind a^{N-1} through n modular exponentiations each of them of complexity $O(\log(N)\log(\log(N))\log(\log(\log(N))))$.

Algorithm.

INPUT: $K, p, n, a.$; $N := Kp^n + 1$. $\mathrm{S}_0 := a^K$.

STEP 1: If $\mathrm{S}_0 \equiv 1 \pmod N$
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 $\Phi_p(S_{i-1}) \equiv 0 \pmod N$
then Let j:=i. GOTO STEP 3
If $S_i \equiv 1 \pmod N$ and $\Phi_p(S_{i-1}) \not\equiv 0 \pmod N$
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.

Proposition 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 steps 1 is that of the modular exponentiation $a^K \pmod N$. Taking into account that products modulo N can be performed by Schoenhage-Strassen algorithm (see [21]) with complexity:

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

this is the complexity of step 1.

In step 2 n modular exponentiation 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:

$$O(\log^2(N)\log(\log(N))\log(\log(\log(N)))).$$

And, summarizing, the whole complexity is $\tilde{O}(\log^2(N)$. □

For generalized Proth numbers ($K < p^n$). If we consider $S_J := a^{Kp^J}$ 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 $Kp^n + 1$. In this case we can consider the following algorithm:

Algorithm.

INPUT: $K, p, n, a.$; $N := Kp^n + 1$. $J := \left\lfloor \frac{\log_p K+n}{2} \right\rfloor$. $S_J := a^{Kp^J}$.

STEP 1: If $S_J \equiv 1 \pmod N$
then RETURN: "N is a p-strong-probable prime to base a". STOP.
else RETURN: "N will be certified either as prime or composite".

STEP 2: For $i = J + 1$ to n
$S_i \equiv S_{i-1}^p \pmod N$
If $S_i \equiv 1 \pmod N$ and $\Phi_p(S_{i-1}) \equiv 0 \pmod N$
Then RETURN: "N is PRIME"
Else RETURN: "N is COMPOSITE" . STOP
End
RETURN: "N is COMPOSITE" . STOP

We will now see that for moderately big values of n, the probability that the algorithm does not certify the primality of a prime of the form $N = Kp^n+1$ without choosing more that 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, regardless the value of n, the use of several bases to certify the primality of N is quite frequent. To do so, we first present a quite well-known lemma.

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

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

With the use of this lemma we can prove the following proposition.

Proposition 2. *Given a prime $N = Kp^n + 1$ ($K < p^n$) 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 $a^J \equiv 1 \pmod N$. This will happen if a is residual power of order $n-J$ 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 2. For big values of n the probability that a prime of the form $N = Kp^n+1$ is certified as p-strong probable prime is about $p^{-n/2}$.

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 some power $a^{Kp^i} \equiv 1 \pmod N$ 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 taking into account that:

$$a^{kp^n} = ((a^k)^p)^{p^{\cdots^{(n}p}}.$$

Moreover, for values of p with "many" 1's or "many" 0's in its binary expansion (like for 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.

To sum up, the presented algorithm improves every primality test requiring more than the computation of a power of the kind $a^{N-1} \pmod N$ or similar. It also equals those requiring one such power, even performing better for some particular values of p.

6. Appeal to implementers

Although the authors have not implemented the proposed algorithm with an appropriate technology, and using Mathematica® only primes up to 100000 digits have been tested, they are in condition to make some considerations that might encourage implementers to create a software based in this paper. Taking into account that our algorithm requires a number of computations similar to that of Fermat's test (or even less) we have compared the time required to certify the primality of the four biggest known primes in the family $N = 2 \cdot 3^n + 1$, recently found by David Broadhurst with the estimated time required by our algorithm. Of course, the runtime of OpenPFGW depends on the "lucky" choice of the bases used to perform Pocklington's test (namely, the chosen base a should satisfy $\gcd(a^{\frac{N-1}{P}} - 1, N) = 1$). OpenPFGW also fails when the tested number is a Fermat pseudoprime for several bases (with a resounding failure when it is a Carmichael number), since it is unable to quickly detect the compositeness of these numbers. However, our algorithm would require only one modular exponentiation of the kind a^{N-1}, thus becoming preferable to any other algorithm for generalized Proth numbers. To be true, also our algorithm could require a second choice for the base. But this would happen, for $n = 1175232$ with probability about 8.25×10^{-280365}.

In the table below we show the bases used by OpenPFGW (Version 3.4.3) to certify the primality of each N (in one case in needed 7), the runtime in an Intel core2 Duo P7450 @ 2.13 GHz with 4Gb of RAM and the estimated runtime for our algorithm. We also show the ranking of the considered primes among the known primes up to date. All of them are among the 1000 bigger known primes, and the biggest one is among the 100 bigger ones and, remarkably, are among the very few big primes not belonging to the most investigated families: Mersenne, generalized Fermat, Cullen, Woodall, Proth, generalized Cullen and generalized Woodall. It seems to us that the families $Kp^n + 1$ have not been deeply investigated except for the case $p = 2$.

$N = 2 \cdot 3^n + 1$, $n=$	529680	1074726	1086112	1175232
Number of digits	252722	512775	518208	560729
Absolute Ranking	895-th	102-th	101-th	87-th
Bases used by OpenPFGW	2,3	2,3,17,23,29,31,41	2	2,3,5
Runtime OpenPFGW (in s.)	1531.	21865.	3220.	14537
Estimated runtime our algorithm	766.	3124.	3220.	4845

We want to stress the importance of take advantage of the structure of Mersenne and Fermat primes in order to reduce the required time for the modular exponentiations in our algorithm. Consider for instance the search for primes of the form $K \cdot 127^n + 1$. Our algorithm requires 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 algorithm. This would be the case of primes of the form $2^s \pm 2^t \pm 1$, for instance.

Acknowledgments

We 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] Leonard M. Adleman, Carl Pomerance, and Robert S. Rumely. On distinguishing prime numbers from composite numbers. *Ann. of Math. (2)*, 117(1):173–206, 1983.

[2] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. PRIMES is in P. *Ann. of Math. (2)*, 160(2):781–793, 2004.

[3] Pedro Berrizbeitia. Sharpening "PRIMES is in P" for a large family of numbers. *Math. Comp.*, 74(252):2043–2059 (electronic), 2005.

[4] 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(7):1923–1925, 1999.

[5] Pedro Berrizbeitia and T. G. Berry. Generalized strong pseudoprime tests and applications. *J. Symbolic Comput.*, 30(2):151–160, 2000.

[6] Pedro Berrizbeitia, T. G. Berry, and Juan Tena-Ayuso. A generalization of Proth's theorem. *Acta Arith.*, 110(2):107–115, 2003.

[7] 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(2):363–365 (electronic), 2002.

[8] Pedro Berrizbeitia and Aurora Olivieri. A generalization of Miller's primality theorem. *Proc. Amer. Math. Soc.*, 136(9):3095–3104, 2008.

[9] Wieb Bosma. Cubic reciprocity and explicit primality tests for $h \cdot 3^k \pm 1$. In *High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams*, volume 41 of *Fields Inst. Commun.*, pages 77–89. Amer. Math. Soc., Providence, RI, 2004.

[10] John Brillhart, D. H. Lehmer, and J. L. Selfridge. New primality criteria and factorizations of $2^m \pm 1$. *Math. Comp.*, 29:620–647, 1975.

[11] H. Cohen and H. W. Lenstra, Jr. Primality testing and Jacobi sums. *Math. Comp.*, 42(165):297–330, 1984.

[12] Richard Crandall and Carl Pomerance. *Prime numbers. A computational perspective.* Springer, New York, second edition, 2005.

[13] José María Grau and Antonio M. Oller-Marcén. An $\widetilde{O}(\log^2 n)$ time primality test for generalized cullen numbers. *Math. Comp.*, to appear.

[14] 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(3):529–534, 1992.

[15] Sergei Konyagin and Carl Pomerance. On primes recognizable in deterministic polynomial time. In *The mathematics of Paul Erdős, I*, volume 13 of *Algorithms Combin.*, pages 176–198. Springer, Berlin, 1997.

[16] Édouard Lucas. Sur la recherche des grands nombres premiers. *Assoc. Francaise p. l'Avanc. des Science. Comptes Rendus*, (5):61–68, 1876.

[17] 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.

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

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

[20] Michael O. Rabin. Probabilistic algorithm for testing primality. *J. Number Theory*, 12(1):128–138, 1980.

[21] A. Schönhage and V. Strassen. Schnelle Multiplikation grosser Zahlen. *Computing (Arch. Elektron. Rechnen)*, 7:281–292, 1971.

[22] H. C. Williams. A note on the primality of $6^{2^n} + 1$ and $10^{2^n} + 1$. *Fibonacci Quart.*, 26(4):296–305, 1988.

[23] H. C. Williams and C. R. Zarnke. Some prime numbers of the forms $2A3^n + 1$ and $2A3^n - 1$. *Math. Comp.*, 26:995–998, 1972.

[24] 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.

Departamento de Matemáticas, Universidad de Oviedo, Avda. Calvo Sotelo, s/n, 33007 Oviedo, Spain

E-mail address: grau@uniovi.es

Departamento de Matemáticas, Universidad de Zaragoza, C/Pedro Cerbuna 12, 50009 Zaragoza (España)

E-mail address: oller@unizar.es