EXPLICIT PRIMALITY CRITERIA FOR $h \cdot 2^k \pm 1$

WIEB BOSMA

Dedicated to the memory of D. H. Lehmer

Abstract. Algorithms are described to obtain explicit primality criteria for integers of the form $h \cdot 2^k \pm 1$ (in particular with $h$ divisible by 3) that generalize classical tests for $2^k \pm 1$ in a well-defined finite sense. Numerical evidence (including all cases with $h < 10^5$) seems to indicate that these finite generalizations exist for every $h$, unless $h = 4^m - 1$ for some $m$, in which case it is proved they cannot exist.

1. INTRODUCTION

In this paper we consider primality tests for integers $n$ of the form $h \cdot 2^k \pm 1$. Since every integer is of that form, we first specify what we mean by this.

Throughout this paper, $h$ will denote an odd positive integer. We shall consider the question of obtaining primality criteria for $n_k = h \cdot 2^k \pm 1$, for all $k$ such that $2^k > h$.

Two classical results express that primality of $2^k \pm 1$ can be decided by a single modular exponentiation; indeed, for $2^k + 1$ one has

$$n = 2^k + 1 \text{ is prime } \iff 3^{(n-1)/2} \equiv -1 \pmod{n},$$

whereas for $2^k - 1$ the formulation is usually in terms of recurrent sequences, as given by Lucas [9] and Lehmer [7] (see also §2):

$$n = 2^k - 1 \text{ is prime } \iff e_{k-2} \equiv 0 \pmod{n},$$

where $e_0 = -4$, and $e_{j+1} = e_j^2 - 2$ for $j \geq 0$. Similar primality criteria exist for $n$ of the form $h \cdot 2^k \pm 1$ with $h$ not divisible by 3.

For fixed $h$ divisible by 3, however, one has to allow a dependency on $k$ in the starting values for the exponentiation (or the recursion, as in (1.2)) in the criterion for $h \cdot 2^k \pm 1$. The generalizations of the above primality criteria described in this paper will be explicit in the sense that for every $k$ with $2^k > h$ an explicit starting value will be given, and finite in the sense that the set of starting values for fixed $h$ will be finite.

It seems that with the exception of $h$ of the form $4^m - 1$, such an explicit, finite generalization always exists. As part of the research for this paper, I

Received by the editor August 3, 1992 and, in revised form, December 9, 1992.
1991 Mathematics Subject Classification. Primary 11Y11, 11A51, 11-04.
This research was supported by the Australian Research Council (ARC Grants A68830699 and A68930041).

©1993 American Mathematical Society
0025-5718/93 $1.00 + .25$ per page

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
constructed such solutions for every \( h \) up to 100000. For \( h \) of the form \( 4^m - 1 \) it is proved that a finite set of starting values will never suffice.

2. Primality criteria

Explicit primality criteria for numbers of the form \( h \cdot 2^k + 1 \) are based on the following theorem. (For proofs of statements in this section, see [2, 10].)

\[ \text{(2.1) Theorem. Let } n = h \cdot 2^k + 1 \text{ with } 0 < h < 2^k \text{ and } h \text{ odd. If } \left( \frac{D}{n} \right) = -1, \text{ then} \]

\[ n \text{ is prime } \iff \left( \frac{D}{n} \right) = -1 \mod n. \]

Thus, finding \( D \) with Jacobi symbol \( \left( \frac{D}{n} \right) = -1 \) suffices to obtain an explicit primality criterion for \( n = h \cdot 2^k + 1 \). In practice, finding such \( D \) for given \( k \) is easily done by picking \( D \) at random, or by searching for the smallest suitable \( D \). The latter strategy was for instance used by Robinson [12] in an early computer search for primes of the form \( h \cdot 2^k + 1 \) with \( h < 100 \) and \( k < 512 \); he found that he never needed \( D \) larger than 47.

However, one wonders whether it would be possible to prescribe \( D \) for fixed \( h \). For that it suffices to solve the following problem.

\[ \text{(2.3) Problem. Given an odd integer } h > 1. \text{ Determine a finite set } \mathcal{D} \text{ and for every positive integer } k > 2 \text{ an integer } D_k \in \mathcal{D} \text{ such that } \left( \frac{D_k}{h \cdot 2^k + 1} \right) \equiv 1 \text{ and } D_k \equiv 0 \mod h \cdot 2^k + 1. \]

\[ \text{(2.4) Remarks. In what follows below, we will often write about a solution } \mathcal{D} \text{ to Problem (2.3), when we mean such a set together with a map } \mathbb{Z}_{\geq 2} \to \mathcal{D}, \text{ which provides the explicit value for every } k. \text{ This map will in our constructions be constant on the residue classes modulo some 'period' } r. \]

Let some odd \( h \) be fixed. Suppose that \( \mathcal{D} \) forms a solution to the problem described in (2.3), and let \( D_k \in \mathcal{D} \) such that \( \left( \frac{D_k}{h \cdot 2^k + 1} \right) \equiv 1 \). If \( \left( \frac{D_k}{h \cdot 2^k + 1} \right) = -1 \), then Theorem (2.1) provides an explicit primality test for \( h \cdot 2^k + 1 \), provided that \( 2^k > h \). If, on the other hand, \( \left( \frac{D_k}{h \cdot 2^k + 1} \right) = 0 \) and \( h \cdot 2^k + 1 \mid D_k \), then both sides of (2.2) are false.

Since \( \left( \frac{-D}{h \cdot 2^k + 1} \right) = \left( \frac{-D}{h \cdot 2^k + 1} \right) \) for \( k > 1 \), we will henceforth assume that \( \mathcal{D} \) consists of positive integers.

\[ \text{(2.5) Remark. Notice that for some } h \text{ it is even possible to solve Problem (2.3) with the stronger requirement that } \left( \frac{D_k}{h \cdot 2^k - 1} \right) = 0. \text{ This is for instance true for } h = 78557: \text{ Selfridge noticed that } 78557 \cdot 2^k + 1 \text{ has a divisor in } \mathcal{D} = \{3, 5, 7, 13, 17, 241\} \text{ for every } k \geq 1 \text{ [6, p. 42].} \]

Next we describe primality criteria for numbers of the form \( h \cdot 2^k - 1 \). Whereas tests for \( h \cdot 2^k + 1 \) all took place within \( \mathbb{Z} \) (or rather \( \mathbb{Z}/n\mathbb{Z} \)), we now pass to quadratic extensions. For a quadratic field \( \mathbb{Q}(\sqrt{D}) \) with ring of integers \( \mathcal{O}_D \) we let \( \sigma \) denote the automorphism of order 2 obtained by sending \( \sqrt{D} \) to \( -\sqrt{D} \). Theorem (2.6) is the analogon of Theorem (2.1).

\[ \text{(2.6) Theorem. Let } n = h \cdot 2^k - 1 \text{ with } 0 < h < 2^k \text{ and } h \text{ odd. Suppose there exist } D \equiv 0, 1 \mod 4, \text{ and } \alpha \in \mathcal{O}_D, \text{ such that } \left( \frac{D}{n} \right) = -1 \text{ and } \left( \frac{N(\alpha)}{n} \right) = -1. \text{ Then} \]

\[ n \text{ is prime } \iff \left( \frac{\alpha}{\sigma(\alpha)} \right)^{(n+1)/2} \equiv -1 \mod n. \]
The way Theorem (2.6) is used for an explicit primality test for $h \cdot 2^k - 1$ will be clear: one looks for a pair $D$ and $\alpha$ such that both $D$ and the norm of $\alpha$ have Jacobi symbol $-1$.

(2.8) **Problem.** Given an odd integer $h > 1$. Determine a finite set $\mathscr{D}$ and for every positive integer $k \geq 2$ a pair $(D, \alpha) \in \mathscr{D} \times O_D$, such that either

$$
\left( \frac{D}{h \cdot 2^k - 1} \right) = -1 = \left( \frac{N(\alpha)}{h \cdot 2^k - 1} \right)
$$

or

$$
\left( \frac{D}{h \cdot 2^k - 1} \right) = 0 \quad \text{and} \quad D \not\equiv 0 \mod h \cdot 2^k - 1.
$$

(2.9) **Remarks.** As in the previous case, for a solution of (2.8) to be explicit we want the finite set $\mathscr{D}$ together with a map telling which pair to choose for each $k \geq 2$. Solving (2.8) again leads to an explicit primality criterion by (2.6), or a factor. Sometimes we will be sloppily using prime $D \equiv 3 \mod 4$ instead of the associated discriminant $4D$.

It remains to be explained how (2.6) relates to the formulation of the Lucas-Lehmer test (1.2) in the introduction. For that, let $\alpha \in O_D$ and let $\beta = \frac{\alpha}{\sigma_\alpha}$. Furthermore, let $e_0 = \beta^h + \beta^{-h}$ and $e_{j+1} = e_j^2 - 2$ for $j \geq 0$. Then, by induction, for $j \geq 0$:

$$
e_j = \beta^{h \cdot 2^j} + \beta^{-h \cdot 2^j}.
$$

Hence,

$$
e_{k-2} \equiv 0 \mod n \iff \beta^{h \cdot 2^{k-2}} + \beta^{-h \cdot 2^{k-2}} \equiv 0 \mod n
$$

$$
\iff \beta^{(n+1)/4} + \beta^{-(n+1)/4} \equiv 0 \mod n
$$

$$
\iff \beta^{(n+1)/2} = -1 \mod n.
$$

Thus, a solution to Problem (2.8) immediately yields a finite generalization of (1.2). Notice that $e_0$ can itself be deduced from $\beta$ by a recurrent sequence: if we put $f_0 = 2$ and $f_i = \beta + \beta^{-1}$, then the relations $f_{j+i} = f_j \cdot f_i - f_{j-i}$ (for $j \geq i$) give $f_j = \beta^j + \beta^{-j}$ for every $j \geq 0$. In particular, $f_{2j} = f_j^2 - 2$ and, importantly, $f_h = \beta^h + \beta^{-h} = e_0$.

Also note that it follows immediately that the starting value $e_0$ is in fact a rational number, and that its denominator is coprime to $n$ (since it is a divisor of the $h$th power of $N(\alpha)$). Thus, one in general obtains a recurrence relation for rational numbers rather than for integers as in the classical Lucas-Lehmer case. Since one is only interested in the values modulo $n$, multiplying with the inverse of the denominator modulo $n$ yields an integer recurrence relation, but this formulation has as a disadvantage that one ends up with recurrence relations for which the starting value depends on $k$ (not just on $\alpha$). For an example, see (3.5) below.

3. **Special cases**

First of all, we deal with the case where $h$ is not divisible by 3.

(3.1) **Theorem.** Let $n = h \cdot 2^k + 1$, with $h \not\equiv 0 \mod 3$ and $k \geq 2$. Then $\mathscr{D} = \{3\}$ and $D_k = 3$ (for $k \geq 2$) solves Problem (2.3). In particular, if $2^k > h$, then

$$
n \text{ is prime } \iff 3^{(n-1)/2} \equiv -1 \mod n.
$$
Proof. Since \( n \equiv 1 \mod 4 \), we have \( \left( \frac{3}{n} \right) = \left( \frac{4}{3} \right) \). Also, \( n = h \cdot 2^k + 1 \equiv 0 \) or \( 2 \mod 3 \), and the first assertion is immediate. The second follows by (2.1). \( \square \)

(3.2) **Theorem.** Let \( n = h \cdot 2^k - 1 \), with \( n \not\equiv 0 \mod 3 \) and \( k \geq 2 \). Then \( \mathcal{D} = \{12\} \) and \((D_k, \alpha_k) = (12, 2 + \sqrt{12})\) solves Problem (2.8). In particular, if \( 2^k > h \), then

\[
\begin{align*}
(3.2) \quad n \text{ is prime} & \iff \left( \frac{2 + \sqrt{12}}{2 - \sqrt{12}} \right)^{(n+1)/2} \equiv -1 \mod n \iff e_{k-2} \equiv 0 \mod n, \\
\text{where } e_0 &= -((2 + \sqrt{3})^h + (2 - \sqrt{3})^h) \text{ and } e_{j+1} = e_j^2 - 2 \text{ for } j \geq 0.
\end{align*}
\]

Proof. \( N(\alpha) = (2 + \sqrt{12})(2 - \sqrt{12}) = -8 \), and therefore, for \( k \geq 2 \),

\[
\left( \frac{12}{n} \right) = -\left( \frac{h \cdot 2^k - 1}{3} \right) = \begin{cases} 
0 & \text{if } h \cdot 2^k \equiv 1 \mod 3, \\
-1 & \text{if } h \cdot 2^k \equiv 2 \mod 3,
\end{cases}
\]

using quadratic reciprocity and the fact that \( n = h \cdot 2^k - 1 \equiv 3 \mod 4 \). Also, if \( k \geq 3 \), then \( n \equiv 7 \mod 8 \), and hence

\[
\left( \frac{N(\alpha)}{n} \right) = \left( \frac{-2}{n} \right) = -1.
\]

This proves the first assertion.

Using the notation of (2.9), we have

\[
e_0 = f_h = \beta^h + \beta^{-h} = \left( \frac{2 + \sqrt{12}}{2 - \sqrt{12}} \right)^h + \left( \frac{2 - \sqrt{12}}{2 + \sqrt{12}} \right)^h
\]

\[
= -(2 + \sqrt{3})^h + (2 - \sqrt{3})^h
\]

and the other assertions follow from (2.6) and (2.9). \( \square \)

Note that (3.1) and (3.2) include the classical case \( h = 1 \) quoted in the introduction. Of course, much more is known for numbers \( 2^k \pm 1 \), but we are not interested in that here.

We would like to know whether we can generalize (3.1) and (3.2) for \( h \) divisible by 3. Not much seems to be known for that case [1, 10, 11]. In general, it will certainly not be possible to use the same \( D \) for every \( k \), but it might be possible to use only \textit{finitely many} different values.

The first observation we make is that a solution to Problem (2.3) for one particular \( h \) will in general lead to a solution for every \( h' \) in the same residue class \( \mod 4 \). In that light, (3.1) is in fact a consequence of (1.1) and the special case \( h = 5 \) and \( \mathcal{D} = \{3\} \).

Similarly, a solution for Problem (2.8) for some \( h \) will lead to solutions for all \( h \) in some residue class with respect to a modulus depending on the \( D \) and the norms \( N(\alpha) \) for the pairs \((D, \alpha)\) used.

Next we show that for \( h = 4^m - 1 \), finite generalizations of (3.1) and (3.2) do not exist.

(3.3) **Theorem.** Let \( m \geq 1 \). For every finite set \( \mathcal{D} \subset \mathbb{Z} \) there exist \( k \geq 2 \) such that

\[
\left( \frac{D}{(4^m - 1) \cdot 2^k + 1} \right) = 1 \quad \text{for every } D \in \mathcal{D}.
\]

In other words, Problem (2.3) does not have a finite solution for \( h = 4^m - 1 \).
Proof. Let $\mathcal{D}$ be a finite set. Let $\mathcal{P}$ be the finite set of prime numbers dividing at least one $D \in \mathcal{D}$:

$$\mathcal{P} = \{p | p \text{ prime, } \exists D \in \mathcal{D} : p | D\}.$$ 

By multiplicativity of the Jacobi symbol, it suffices to prove that there exists $k \geq 2$ such that

$$\left(\frac{p}{(4m - 1) \cdot 2k + 1}\right) = 1$$

for every $p$ in $\mathcal{P}$. To do so, simply choose $k \geq 2$ such that $k$ is a multiple of $\text{ord}_p(2)$ for every odd $p \in \mathcal{P}$, where $\text{ord}_p(2)$ denotes the multiplicative order of 2 modulo $p$. Then

$$\left(\frac{p}{(4m - 1) \cdot 2k + 1}\right) = \left(\frac{(4m - 1) \cdot 1 + 1}{p}\right) = \left(\frac{4m}{p}\right) = 1.$$

If necessary, we also take $k \geq 3$, so that $(4m - 1) \cdot 2k + 1 \equiv +1 \mod 8$ to ensure that

$$\left(\frac{2}{(4m - 1) \cdot 2k + 1}\right) = 1.$$

This proves (3.3). □

(3.4) Theorem. Let $m \geq 1$. For every finite set $\mathcal{D}$ of pairs $(D, \alpha)$, with $D \equiv 0, 1 \mod 4$ and $\alpha \in O_D$, there exist $k \geq 2$ such that for every $(D, \alpha) \in \mathcal{D}$

$$\left(\frac{D}{(4m - 1) \cdot 2k - 1}\right) = 1 \quad \text{or} \quad \left(\frac{N(\alpha)}{(4m - 1) \cdot 2k - 1}\right) = 1.$$

In other words, Problem (2.8) does not have a finite solution for $h = 4m - 1$.

Proof. Let $\mathcal{D}$ be a finite set of pairs as in the statement of the theorem. Note that of the pair of integers $D$ and $N(\alpha)$ at least one is positive. Let $\mathcal{P}$ be the finite set of all prime numbers dividing the positive $D$'s and the positive norms $N(\alpha)$, and $(D, \alpha) \in \mathcal{D}$:

$$\mathcal{P} = \{p | p \text{ prime, } \exists (D, \alpha) \in \mathcal{D} : (D > 0 \text{ and } p | D \text{ or } N(\alpha) > 0 \text{ and } p | N(\alpha))\}.$$ 

By multiplicativity of the Jacobi symbol, it suffices to prove that there exists $k \geq 2$ such that

$$\left(\frac{p}{(4m - 1) \cdot 2k - 1}\right) = 1$$

for every $p$ in $\mathcal{P}$. To do so, simply choose $k \geq 2$ such that $k \equiv -2m \mod \text{ord}_p(2)$ for every odd $p \in \mathcal{P}$, where $\text{ord}_p(2)$ denotes the multiplicative order of 2 modulo $p$. Then

$$\left(\frac{p}{(4m - 1) \cdot 2k - 1}\right) = \left(\frac{-(4m - 1) \cdot 2k - 1}{p}\right) = \left(\frac{-(4m - 1) \cdot 4^{-m} - 1}{p}\right) = \left(\frac{4m}{p}\right) = 1.$$

If necessary, we also take $k \geq 3$ so that $(4m - 1) \cdot 2k - 1 \equiv -1 \mod 8$ to ensure that

$$\left(\frac{2}{(4m - 1) \cdot 2k - 1}\right) = 1.$$

This proves (3.4). □
(3.5) **Remarks.** The best one could hope for in case \( h = 4^m - 1 \) is to find infinite sets as in (2.3) and (2.8), parametrized by \( k \). We easily obtained such results for \( m = 1, 2 \); for example, let \( n_k = 3 \cdot 2^k - 1 \) for \( k \geq 2 \), and define

\[
(D_k, \alpha_k) = \begin{cases} 
(7, 2 + \sqrt{7}) & \text{if } k \equiv 0, 2 \mod 3, \\
(73, 3 + \sqrt{73}) & \text{if } k \equiv 1, 4 \mod 9, \\
(2^{(k-1)/3} + 1 + \sqrt{2^{(k-1)/3} + 1}) & \text{if } k \equiv 7 \mod 9.
\end{cases}
\]

Then \( \left( \frac{D_k}{n_k} \right) = -1 = \left( \frac{N(\alpha_k)}{n_k} \right) \) for every \( k \geq 1 \); furthermore,

\[
n_k \text{ is prime } \iff \left( \frac{\alpha_k}{\sigma \alpha_k} \right)^{(n_k+1)/2} \equiv -1 \mod n_k.
\]

Borho [1] presents a different parametrized infinite solution for (2.8) with \( h = 3 \). He also gives a parametrized solution for \( h = 9 \), but as we will see below, for that case a finite solution exists.

As a final example of an explicit primality test in terms of a recurrent sequence we indicate how the first case of (3.6) translates. So let \( h = 3 \) and \( k \equiv 0, 2 \mod 3 \). In the notation of (2.9), \( \beta = \frac{2 + \sqrt{7}}{2 - \sqrt{7}} \) and \( e_0 = \beta^3 + \beta^{-3} = -\frac{10054}{33} \). We have here a denominator \( 3^3 \) in the starting value for our recurrent sequence; however, since \( n = 3 \cdot 2^k - 1 \), one has \( 3^{-1} \equiv 2^k \mod n \) and (3.6) implies for \( k \equiv 0, 2 \mod 3 \):

\[
n_k \text{ is prime } \iff e_{k-2} \equiv 0 \mod n_k,
\]

where \( e_0 = -10054 \cdot 2^k \) and \( e_{j+1} = e_j^2 - 2 \) for \( j > 1 \).

4. **The general case**

The next question is: what happens for \( h \equiv 3 \mod 6 \) not of the form \( 4^m - 1 \)? Although I have not been able to prove it, all the evidence (including all cases for \( h \) up to 100000) seems to suggest that for such \( h \) there always exists a solution of Problems (2.3) and (2.8)!

A natural but naive first attack to Problem (2.3) consists of finding a suitable \( D_k \) for \( k = 2, 3, \ldots \) in succession, by using the smallest one that works, and by keeping track of the \( k \) for which a given value \( D \) works. What is wrong with this approach is that it uses an ordering of the \( D \)'s according to size, while it is the order of 2 modulo \( D \) that is important, because this determines the modulus for the residue classes of \( k \) for which \( D \) is suitable.

The next attempt, therefore, is to run through the primes \( D \) in order of increasing multiplicative order of 2 in \( (\mathbb{Z}/D\mathbb{Z})^* \). This resulted in the first algorithm that we tried out in practice, by writing a very short program in the Cayley language [4]. We used a table of the complete factorizations of all integers \( 2^u - 1 \) for \( 2 \leq u \leq U = 250 \), obtained from [3] and direct factorization in Cayley.

This worked in fact so well, that we tried it for every \( h \equiv 3 \mod 6 \) up to 10000. Out of the 1667 positive such \( h \) less than 10000, six are of the form \( 4^m - 1 \), and only 36 others were not dealt with by this algorithm.

To deal with the remaining cases, one could try to increase the bound \( U \), but for that we would have to overcome the difficulties of factoring \( 2^u - 1 \) for large
u, which would soon become unfeasible. Instead, we have tried to predict for which values of u we might be successful. It turns out that the main problem lies in the possibility that \( n = h \cdot 2^k + 1 \) is a square.

(4.1) **Example.** Let \( h = 33 \); this is the smallest \( h \) for which our first algorithm failed. We show in this example that squares form a problem.

If we list the factorizations of \( n_k = 33 \cdot 2^k + 1 \) for the first few values of \( k \), one notices that \( n_k \) is the square of an integer for \( k = 4 \) and \( k = 7 \): indeed \( n_4 = 33 \cdot 2^4 + 1 = 23^2 \) and \( n_7 = 33 \cdot 2^7 + 1 = 5^2 \cdot 13^2 \). Therefore, the only \( D > 1 \) for which \( (\frac{D}{n_k}) \neq 1 \) is \( D = 23 \). Since the order of 2 modulo \( D \) is 11, this forces us to consider residue classes modulo 11. For \( n_7 \) we may use \( D = 5 \), so already we need to consider \( k \) modulo 44 because of these squares. In fact, these two are the only squares among \( n_k = 33 \cdot 2^k + 1 \) for \( k \geq 1 \) (this will follow from the proposition below).

However, even if \( n_k \) is not a square, it may be that \( (\frac{D}{n_k}) = 1 \) for every finite set of primes \( D \) not dividing some integer \( b \), for all \( k \) in a residue class with respect to some modulus. This happens in case \( h + 2^k \) is a square. In this example, take for instance \( b = 34 \), and define for any finite set \( \mathcal{D} \) of primes not dividing \( b \) the integer \( k \) by \( k \equiv -8 \mod \text{ord}_2(D) \) for every \( D \in \mathcal{D} \). Then

\[
\left( \frac{D}{33 \cdot 2^k + 1} \right) = \left( \frac{33 \cdot 2^k + 1}{D} \right) = \left( \frac{(2^5 + 1) \cdot 2^{-8} + 1}{D} \right) = \left( \frac{(2^{-4}(1 + 2^4))^2}{D} \right),
\]

which equals 1. As a consequence, for every \( \mathcal{D} \) we will be stuck with the residue class for \( k \equiv -8 \mod u \), for some modulus \( u \), unless we include \( D = 1 + 2^4 = 17 \); that forces \( u \) to be divisible by 8. Similarly, we will need \( D = 7 \) (and hence \( u \) a multiple of 3) to deal with the case \( k \equiv -4 \).

These considerations lead us to consider \( k \) modulo 264 for \( h = 33 \). It turns out that the primes contained in \( \mathcal{P}_{264} \), the set of divisors of \( 2^{264} - 1 \), do indeed solve Problem (2.3) for \( h = 33 \); in fact, we do not need a primitive divisor of \( 2^{264} - 1 \) for this, and hence we were able to solve the problem for \( h = 33 \) without extra factorizations!

The following proposition shows that it is very easy to detect the squares; we will use it to predict what the modulus \( u \) will be. Since for \( h \cdot 2^k - 1 \) we will use basically the same strategy, we deal with that case here at the same time.

(4.2) **Proposition.** (i) Let \( n = h \cdot 2^k + 1 \) for some odd \( h \geq 1 \) and some \( k \geq 2 \). Then \( n \) is a square in \( \mathbb{Z} \) if and only if there exists an odd positive integer \( f \) such that \( h = f \cdot (f \cdot 2^{k-2} + 1) \).

(ii) Let \( n = h + 2^k \) for some odd \( h \geq 1 \) that is divisible by 3, and some \( k \geq 2 \). Then \( n \) is a square in \( \mathbb{Z} \) if and only if \( k \) is even and there exists an odd positive integer \( f \) such that \( h = f \cdot (2^{k/2+1} + f) \).

(iii) Let \( n = h \cdot 2^k - 1 \) for some odd \( h \geq 1 \) and some \( k \geq 2 \). Then \( n \) is never a square in \( \mathbb{Z} \).

(iv) Let \( n = 2^k - h \) for some odd \( h \geq 1 \) that is divisible by 3, and some \( k \geq 2 \). Then \( n \) is a square in \( \mathbb{Z} \) if and only if \( k \) is even and there exists an odd positive integer \( f \) such that \( h = f \cdot (2^{k/2+1} - f) \).

**Proof.** (i) Suppose that \( n = h \cdot 2^k + 1 = d^2 \), with \( d \) some positive odd integer. Then \( d^2 - 1 = h \cdot 2^k \) and \( d = f \cdot 2^{k-1} + 1 \) for some odd \( f \). Thus, \( h \cdot 2^k = (d - 1)(d + 1) = 2^k(f^22^{k-2} + f) \), from which the assertion follows.
Conversely, if \( h = f \cdot (f \cdot 2^{k-2} \pm 1) \), then \( n = f \cdot (f \cdot 2^{k-2} + 1) \cdot 2^k + 1 = (f \cdot 2^{k-1} \pm 1)^2 \).

(ii) Suppose that \( n = h + 2^k = d^2 \), with \( d \) a positive odd integer. Looking modulo 3, we find that \( k \) must be even, say \( k = 2l \). Let \( f \in \mathbb{Z} \) be such that \( d = f + 2^l \); note that \( f \) must be odd and positive. Then

\[
d^2 = f^2 + f \cdot 2^{l+1} + 2^l = h + 2^l,\]

and, therefore, \( h = f^2 + f \cdot 2^{l+1} \), whence the assertion follows.

Conversely, if \( h = f^2 + f \cdot 2^{k/2+1} \), then \( h + 2^k = f^2 + f \cdot 2^{k/2+1} + 2^k = (f + 2^{k/2})^2 \).

(iii) Since \( h \cdot 2^k - 1 \equiv 3 \mod 4 \) for \( k \geq 2 \), it cannot be a square.

(iv) Suppose that \( n = 2^k - h = d^2 \), with \( d \) a positive odd integer. Looking modulo 3, we find that \( k \) must be even, say \( k = 2l \). Let \( f \in \mathbb{Z} \) be such that \( d = f = 2^l \); note that \( f \) must be odd and positive. Then

\[
d^2 = 2^{2l} - f \cdot 2^{l+1} + f^2 = 2^l - h,\]

and, therefore, \( h = f^2 + f \cdot 2^{l+1} - f \).

Conversely, if \( h = f \cdot (2^{k/2+1} - f) \), then \( 2^k - h = 2^k - f \cdot 2^{k/2+1} + f^2 = (2^{k/2} - f)^2 \). This ends the proof of (4.2).

(4.3) Algorithm.

Input. An integer \( h \equiv 3 \mod 6 \), an integer \( U > 1 \), and for all \( 2 \leq u \leq U \) a set \( \mathcal{P}_u \) consisting of divisors of \( 2^u - 1 \).

Output. A positive integer \( r \leq U \) and a sequence of integers \( E = (C_1, C_2, \ldots, C_r) \) of length \( r \) such that

\[
\left( \frac{C_i}{h \cdot 2^k + 1} \right) \neq 1,
\]

for every \( k \equiv i \mod r \), with \( k \geq 3 \).

(1) Find a multiplier \( m \geq 1 \) which is a positive integer with the property that if \( h \cdot 2^k + 1 \) is a square, then \( \gcd(2m - 1, h \cdot 2^k + 1) > 1 \), and if \( h + 2^k \) is a square, then \( \gcd(2m - 1, h + 2^k) > 1 \), for every positive integer \( k \).

(2) Put \( r = 1 \), \( u = m \), \( \mathcal{R} = \emptyset \), and \( E = (0) \). Repeat the following steps until termination.

(a) Let \( k \) be the smallest integer in \( 3 \leq k \leq r + 2 \) such that \( k \notin \mathcal{R} \).

(b) If there does not exist \( D \in \mathcal{P}_u \) such that

\[
\left( \frac{D}{h \cdot 2^k + 1} \right) \neq 1,
\]

proceed to step (c); else let \( D \) be the smallest such value, let \( r' = \text{lcm}(r, u) \), replace \( \mathcal{R} \) by

\[
\{ 3 \leq i \leq r' + 2 | i \equiv k \mod u \text{ or } i \equiv d \mod r \text{ for some } d \in \mathcal{R} \};
\]

replace \( E \) by \( (C_1', \ldots, C_{r'}') \), where

\[
C_i' = \begin{cases} 
C_j & \text{if } C_j \neq 0, \text{ where } j \equiv i \mod r, \\
D & \text{if } j \equiv k \mod r', \\
0 & \text{otherwise};
\end{cases}
\]

next replace \( r \) by \( r' \).

(c) Terminate and return \( E \) if either \( \# \mathcal{R} = r \) or \( u > U - m \). In all other cases: increase \( u \) by \( m \).
(4.4) Remarks. The sequence returned by Algorithm (4.3) represents a solution to Problem (2.3) if it does not contain a zero entry, that is, if it terminated in step (2)(c) with $\#\mathcal{P} = r$.

In the cases I have considered, $h$ was sufficiently small to allow complete factorization without effort, and inspection of all possible factorizations to obtain the multiplier $m$, using the above proposition. Alternatively, one could check all of the finitely many possible $k$ that yield squares.

Of course $2^{m_l} - 1$ is soon too big to be factored completely; if that happened, all known prime factors were used, as well as (very occasionally) composite factors (in particular, divisors of the form $2^d - 1$ of $2^{m_l} - 1$, with $d$ a divisor of $m_l$).

Our strategy for attempting to solve Problem (2.8) for $h \cdot 2^k - 1$ is much the same as that employed in Algorithm (4.3) for $h \cdot 2^k + 1$, except that we have to build in an extra step to find a suitable element. We describe this subalgorithm first.

(4.5) Algorithm.

Input. An integer $h \equiv 3 \mod 6$, positive integers $k$ and $r$, as well as a prime $D$.

Output. Either an element $\alpha \in \mathcal{O}_D$ such that

$$\left(\frac{N(\alpha)}{h \cdot 2^j - 1}\right) \equiv -1 \mod r$$

for every $j \equiv k \mod r$, or 0.

1. If $D \equiv 1 \mod 4$, solve $x^2 + y^2 = D$, and return $\alpha = x + \sqrt{D}$.

2. Choose a suitable bound $b$, and perform step (a) for pairs $x, y$ with $0 < y < b$ and $0 < x < y\sqrt{D}$ (but $x, y$ not both 0) until it is successful, in which case $\alpha$ is returned, or the pairs are exhausted without success, in which case 0 is returned.

(a) Let the integer $g$ coprime to 6 be determined by $x^2 - y^2D = -2^\delta3^\varepsilon g$, with $\delta, \varepsilon \geq 0$. This step is successful if $g$ is a square or

$$\left(\frac{g}{h \cdot 2^k - 1}\right) = 1 \quad \text{and} \quad \text{ord}_2(g) | r;$$

then $\alpha = x + y\sqrt{D}$.

(4.7) Remarks. We briefly comment on Algorithm (4.5) which will be used below to find a suitable element $\alpha$, once $D$ has been found. The search for solutions will be organized in such a way that $D$ will always be positive (recall that either $D$ or $N(\alpha)$ has to be positive) and usually prime (except that it should be replaced by $4D$ if $D \equiv 2, 3 \mod 4$). Since $h \cdot 2^k - 1 \equiv 7 \mod 8$ and $h \cdot 2^k - 1 \equiv 3 \mod 3$,

$$\left(\frac{-1}{h \cdot 2^k - 1}\right) = -1 \quad \text{and} \quad \left(\frac{2}{h \cdot 2^k - 1}\right) = 1 = \left(\frac{3}{h \cdot 2^k - 1}\right).$$

That means not only that $D = 8$ and $D = 12$ will be unsuitable, but also that any factors 2 and 3 in $N(\alpha)$ can be ignored, and that $N(\alpha) = -2^2$ will always be a suitable value. That explains most of step (2) above; the condition given by (4.6) ensures that $N(\alpha)$ not only works for the current value of $k$, but in fact for the whole residue class of $k$ modulo the current modulus $r$. 
It is well known that every prime \( p \equiv 1 \mod 4 \) can be written in the form \( p = x^2 + y^2 \). In step (1) this is used: if \( D = x^2 + y^2 \), then \( N(x + \sqrt{D}) = x^2 - D = -y^2 \), hence suitable! Of course, we should explain how to obtain \( x \) and \( y \) to make everything explicit. There are several methods for solving this problem, some of which work very well in practice, even if \( D \) gets big (in our calculations we used \( D \) of up to 106 decimal digits). One method is to find the square root of \(-1 \) modulo \( D \) and recover \( x \) and \( y \) from such root. We refer the reader to [8, 5] and the references therein for details about these algorithms.

For prime \( D \equiv 3 \mod 4 \) such a general solution does not exist. Still, in step (2) of the above algorithm one will often still find a suitable solution, particularly for small \( D \). We give a few examples in Table 0.

Table 0 contains for certain prime \( D \equiv 3 \mod 4 \) less than 100 an element \( \alpha \) such that \( N(\alpha) = -2^d \cdot 3^e \) as found from Algorithm (4.5) with bound \( b = 25 \) on \( y \). It shows that such a solution (which is suitable for any \( h \) and \( k \)) was found for every such \( D \) with the exception of \( D = 23, 47, 71 \). (It is of course no coincidence that for \( D = 23 \) mod 24 no solution was found: it is easy to see that for these we are trying to solve \( x^2 - Dy^2 = -3^2 \) or \( x^2 - Dy^2 = -2 \cdot 3^2 \), which is impossible.) Note that \( 2^d \cdot 3^e \) may appear in the denominator of the starting value \( e_0 \) as in (2.9) and (3.5).

<table>
<thead>
<tr>
<th>( D )</th>
<th>( \alpha )</th>
<th>( N(\alpha) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>( 2 + \sqrt{7} )</td>
<td>-3</td>
</tr>
<tr>
<td>11</td>
<td>( 3 + \sqrt{11} )</td>
<td>-2</td>
</tr>
<tr>
<td>19</td>
<td>( 4 + \sqrt{19} )</td>
<td>-3</td>
</tr>
<tr>
<td>31</td>
<td>( 2 + \sqrt{31} )</td>
<td>-27</td>
</tr>
<tr>
<td>43</td>
<td>( 4 + \sqrt{43} )</td>
<td>-27</td>
</tr>
<tr>
<td>59</td>
<td>( 23 + 3\sqrt{59} )</td>
<td>-2</td>
</tr>
<tr>
<td>67</td>
<td>( 7 + \sqrt{67} )</td>
<td>-18</td>
</tr>
<tr>
<td>79</td>
<td>( 5 + \sqrt{79} )</td>
<td>-54</td>
</tr>
</tbody>
</table>

Still, \( D = 23 \) (or 47 or 71) may be useful in combination with an element that only works for particular \( h \) and \( k \); such a value is sought after in the last part of the algorithm. For instance, with \( h = 33 \), let \( k = 8 \); then

\[
\left( \frac{23}{33 \cdot 2^8 - 1} \right) = -1 = \left( \frac{-14}{33 \cdot 2^8 - 1} \right) = \left( \frac{N(3 + \sqrt{23})}{33 \cdot 2^8 - 1} \right).
\]

Since the order \( \text{ord}_7(2) = 3 \), the element \( 3 + \sqrt{23} \) is suitable for all \( k \equiv 8 \mod r \) if this current modulus \( r \) is a multiple of 3.

(4.8) Algorithm.

Input. A positive integer \( h \equiv 3 \mod 6 \), an integer \( U > 1 \), and for all \( 2 \leq u \leq U \) a set \( \mathcal{P}_u \) consisting of divisors of \( 2^u - 1 \).

Output. A positive integer \( r \leq U \) and a sequence \( \mathcal{E} = ((D_1, \alpha_1), (D_2, \alpha_2), \ldots, (D_r, \alpha_r)) \) of length \( r \leq U \), with integers \( 0 < D_i \equiv 0 \mod 4 \) and
\[ \alpha_i \in O_{D_i}, \text{ such that} \]
\[
\left( \frac{D_i}{h \cdot 2^k - 1} \right) \not= 1 \quad \text{and} \quad \left( \frac{N(\alpha_i)}{h \cdot 2^k - 1} \right) \not= 1
\]
for every \( k \equiv i \mod r \) (with \( k \geq 2 \)).

1. Find a multiplier \( m \), which is a positive integer with the property that if \( 2^k - h \) is a square, then \( \gcd(2m - 1, 2^k - h) > 1 \) for every positive integer \( k \).

2. Put \( r = 1, \mathcal{R} = \emptyset, u = m, \) and \( \mathcal{E} = ((0,0)) \). Repeat the following steps until termination.

   a. Let \( k \) be the smallest integer in \( 3 < k < r + 2 \) such that \( k \nmid M \).

   b. If there exists no \( D \in \mathcal{R} \) such that
   
   \[
   \left( \frac{D}{h \cdot 2^k + 1} \right) \not= 1
   \]
   then proceed to step (c); else, let \( D \) be the smallest value satisfying this, let \( r' = \text{lcm}(r, u) \), and perform Algorithm (4.5) with \( h, k, r', \) and \( D \) to find an element \( \alpha \). If \( \alpha = 0 \), proceed to step (c); else replace \( \mathcal{R} \) by \( \{3 < i \leq r' + 2 | i \equiv k \mod u \text{ or } i \equiv d \mod r \text{ for some } d \in \mathcal{R} \} \);

   c. Terminate and return the sequence \( \mathcal{E} \) if either \( \#\mathcal{R} = r \) or \( u > U - m \).

   In all other cases: increase \( u \) by \( m \).

The sequence returned by Algorithm (4.8) represents a solution to Problem (2.8) for \( h \) if it does not contain entries of the form \( (0,0) \), that is, if it terminated in step (2)(c) with \( \#\mathcal{R} = r \).

4.9 Numerical results. Six tables (see the Supplement at the end of this issue) summarize the results of running our Cayley implementations of Algorithms (4.3) and (4.8) for \( h \) up to \( 10^5 \). In these tables, \( m \) signifies the multiplier found in step (1) to trap a factor for every possible square, and \( r \) denotes the modulus (‘period’) for the explicit primality test, as returned by the algorithms. Subscripts + and \( - \) indicates tests for \( h \cdot 2^k + 1 \) and \( h \cdot 2^k - 1 \).

In Table 1 multipliers and periods are shown, found using (4.3) for all \( h \equiv 3 \mod 6 \) with \( h < 1000 \). Tables 2 and 3 show the hardest cases for \( h \) up to 100000: in Table 2 all cases for which \( r_+ \) is at least 50 times \( m_+ \) are listed, and Table 3 shows all cases where \( m_+ \geq 500 \). The largest period found was just over 100000.

Tables 4–6 show the corresponding results obtained with Algorithm (4.8), but Table 6 lists all cases with \( m_- \geq 100 \). The largest period encountered is over half a million.

Notice in the tables that the period \( r \) is not always an integral multiple of the multiplier \( m \); the reason for this is that a solution found with \( r \) a multiple of \( m \) sometimes shows an ‘accidental’ periodicity with modulus a divisor of \( r \) that is not a multiple of \( m \).
Finally, we explicitly describe the solutions for $h = 9$ implied by our calculations. According to Table 1, there exists a solution for $9 \cdot 2^k + 1$ with $r = 24$ (and $m = 8$, because the squares $9 + 2^4 = 5^2$ and $9 \cdot 2^5 + 1 = 17^2$ are trapped by $2^8 - 1 = 3 \cdot 5 \cdot 17$), and by Table 4 there is a solution for $9 \cdot 2^k - 1$ with $r = 4$.

(4.10) **Theorem.** Let $n_k = 9 \cdot 2^k + 1$ and define $D_k \in \{5, 7, 17, 241\}$ for $k \geq 2$ as follows:

$$D_k = \begin{cases} 5 & \text{if } k \equiv 0, 2, 3 \mod 4, \\ 7 & \text{if } k \equiv 1, 9, 13, 21 \mod 24, \\ 17 & \text{if } k \equiv 5 \mod 24, \\ 241 & \text{if } k \equiv 17 \mod 24. \end{cases}$$

Then $(\frac{D_k}{n_k}) \neq 1$ for $k \geq 2$. Hence, if $k \geq 4$, then

$$n_k \text{ is prime} \iff D_k^{(n_k-1)/2} \equiv -1 \mod n_k.$$ 

(4.11) **Theorem.** Let $n_k = 9 \cdot 2^k - 1$ and define $D_k, \alpha_k$ for $k \geq 2$ by

$$D_k, \alpha_k = \begin{cases} (5, 1 + \sqrt{5}) & \text{if } k \equiv 0, 1, 2 \mod 4, \\ (17, 1 + \sqrt{17}) & \text{if } k \equiv 3 \mod 4. \end{cases}$$

Then $(\frac{D_k}{n_k}) \neq 1$ and $(\frac{\alpha_k}{\sigma \alpha_k}) = -1$ for every $k \geq 2$. Hence, if $k \geq 4$, then

$$n_k \text{ is prime} \iff (\frac{\alpha_k}{\sigma \alpha_k})^{(n_k+1)/2} \equiv -1 \mod n_k.$$ 

**Bibliography**


License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use


School of Mathematics and Statistics, University of Sydney, Sydney, New South Wales 2006, Australia

E-mail address: wieb@maths.su.oz.au
Supplement to

EXPLICIT PRIMALITY CRITERIA FOR $h \cdot 2^k \pm 1$

WIEB BOSMA

<table>
<thead>
<tr>
<th>$h$</th>
<th>$m_+$</th>
<th>$r_+$</th>
<th>$h$</th>
<th>$m_+$</th>
<th>$r_+$</th>
<th>$h$</th>
<th>$m_+$</th>
<th>$r_+$</th>
<th>$h$</th>
<th>$m_+$</th>
<th>$r_+$</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>†</td>
<td>†</td>
<td>201</td>
<td>4</td>
<td>12</td>
<td>405</td>
<td>3</td>
<td>3</td>
<td>603</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>9</td>
<td>8</td>
<td>24</td>
<td>207</td>
<td>1</td>
<td>5</td>
<td>411</td>
<td>1</td>
<td>12</td>
<td>609</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>15</td>
<td>†</td>
<td>†</td>
<td>213</td>
<td>1</td>
<td>12</td>
<td>417</td>
<td>1</td>
<td>12</td>
<td>615</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>21</td>
<td>12</td>
<td>4</td>
<td>219</td>
<td>1</td>
<td>4</td>
<td>423</td>
<td>1</td>
<td>12</td>
<td>621</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>27</td>
<td>1</td>
<td>4</td>
<td>225</td>
<td>8</td>
<td>16</td>
<td>429</td>
<td>1</td>
<td>15</td>
<td>627</td>
<td>1</td>
<td>12</td>
</tr>
<tr>
<td>33</td>
<td>264</td>
<td>264</td>
<td>231</td>
<td>1</td>
<td>4</td>
<td>435</td>
<td>5</td>
<td>87</td>
<td>633</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>39</td>
<td>4</td>
<td>28</td>
<td>237</td>
<td>1</td>
<td>4</td>
<td>441</td>
<td>1</td>
<td>5</td>
<td>639</td>
<td>10</td>
<td>15</td>
</tr>
<tr>
<td>45</td>
<td>18</td>
<td>18</td>
<td>243</td>
<td>1</td>
<td>5</td>
<td>447</td>
<td>1</td>
<td>12</td>
<td>645</td>
<td>1</td>
<td>18</td>
</tr>
<tr>
<td>51</td>
<td>1</td>
<td>12</td>
<td>249</td>
<td>1</td>
<td>12</td>
<td>453</td>
<td>1</td>
<td>4</td>
<td>651</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>57</td>
<td>10</td>
<td>5</td>
<td>255</td>
<td>†</td>
<td>†</td>
<td>459</td>
<td>1</td>
<td>5</td>
<td>657</td>
<td>20</td>
<td>40</td>
</tr>
<tr>
<td>63</td>
<td>†</td>
<td>†</td>
<td>261</td>
<td>1</td>
<td>12</td>
<td>465</td>
<td>660</td>
<td>660</td>
<td>663</td>
<td>51</td>
<td>102</td>
</tr>
<tr>
<td>69</td>
<td>23</td>
<td>92</td>
<td>267</td>
<td>1</td>
<td>12</td>
<td>471</td>
<td>1</td>
<td>4</td>
<td>669</td>
<td>1</td>
<td>12</td>
</tr>
<tr>
<td>75</td>
<td>3</td>
<td>15</td>
<td>273</td>
<td>88</td>
<td>88</td>
<td>477</td>
<td>1</td>
<td>4</td>
<td>675</td>
<td>12</td>
<td>24</td>
</tr>
<tr>
<td>81</td>
<td>1</td>
<td>12</td>
<td>279</td>
<td>1</td>
<td>12</td>
<td>483</td>
<td>10</td>
<td>5</td>
<td>681</td>
<td>1</td>
<td>15</td>
</tr>
<tr>
<td>87</td>
<td>1</td>
<td>3</td>
<td>285</td>
<td>760</td>
<td>760</td>
<td>489</td>
<td>1</td>
<td>28</td>
<td>687</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>93</td>
<td>1</td>
<td>12</td>
<td>291</td>
<td>96</td>
<td>192</td>
<td>495</td>
<td>11</td>
<td>15</td>
<td>693</td>
<td>1</td>
<td>12</td>
</tr>
<tr>
<td>99</td>
<td>4</td>
<td>4</td>
<td>297</td>
<td>18</td>
<td>18</td>
<td>501</td>
<td>1</td>
<td>4</td>
<td>699</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>105</td>
<td>260</td>
<td>1260</td>
<td>303</td>
<td>1</td>
<td>12</td>
<td>507</td>
<td>1</td>
<td>24</td>
<td>705</td>
<td>5</td>
<td>15</td>
</tr>
<tr>
<td>111</td>
<td>1</td>
<td>4</td>
<td>309</td>
<td>1</td>
<td>4</td>
<td>513</td>
<td>176</td>
<td>176</td>
<td>711</td>
<td>1</td>
<td>11</td>
</tr>
<tr>
<td>117</td>
<td>10</td>
<td>20</td>
<td>315</td>
<td>35</td>
<td>35</td>
<td>519</td>
<td>1</td>
<td>20</td>
<td>717</td>
<td>1</td>
<td>20</td>
</tr>
<tr>
<td>123</td>
<td>1</td>
<td>4</td>
<td>321</td>
<td>1</td>
<td>3</td>
<td>525</td>
<td>11</td>
<td>44</td>
<td>723</td>
<td>1</td>
<td>12</td>
</tr>
<tr>
<td>129</td>
<td>16</td>
<td>48</td>
<td>327</td>
<td>1</td>
<td>12</td>
<td>531</td>
<td>1</td>
<td>12</td>
<td>729</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>135</td>
<td>1</td>
<td>5</td>
<td>333</td>
<td>9</td>
<td>3</td>
<td>537</td>
<td>1</td>
<td>4</td>
<td>735</td>
<td>1</td>
<td>10</td>
</tr>
<tr>
<td>141</td>
<td>4</td>
<td>4</td>
<td>339</td>
<td>1</td>
<td>12</td>
<td>543</td>
<td>1</td>
<td>12</td>
<td>741</td>
<td>3</td>
<td>15</td>
</tr>
<tr>
<td>147</td>
<td>48</td>
<td>48</td>
<td>345</td>
<td>36</td>
<td>36</td>
<td>549</td>
<td>1</td>
<td>8</td>
<td>747</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>153</td>
<td>12</td>
<td>12</td>
<td>351</td>
<td>52</td>
<td>104</td>
<td>555</td>
<td>1</td>
<td>15</td>
<td>753</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>159</td>
<td>1</td>
<td>12</td>
<td>357</td>
<td>18</td>
<td>36</td>
<td>561</td>
<td>132</td>
<td>132</td>
<td>759</td>
<td>1</td>
<td>12</td>
</tr>
<tr>
<td>165</td>
<td>12</td>
<td>24</td>
<td>363</td>
<td>1</td>
<td>4</td>
<td>567</td>
<td>1</td>
<td>5</td>
<td>765</td>
<td>1</td>
<td>18</td>
</tr>
<tr>
<td>171</td>
<td>36</td>
<td>36</td>
<td>369</td>
<td>4</td>
<td>12</td>
<td>573</td>
<td>191</td>
<td>1523</td>
<td>771</td>
<td>1</td>
<td>12</td>
</tr>
<tr>
<td>177</td>
<td>1</td>
<td>4</td>
<td>375</td>
<td>1</td>
<td>3</td>
<td>579</td>
<td>4</td>
<td>12</td>
<td>777</td>
<td>67340</td>
<td>67340</td>
</tr>
<tr>
<td>183</td>
<td>1</td>
<td>4</td>
<td>381</td>
<td>1</td>
<td>12</td>
<td>585</td>
<td>28</td>
<td>84</td>
<td>783</td>
<td>3</td>
<td>12</td>
</tr>
<tr>
<td>189</td>
<td>4</td>
<td>4</td>
<td>387</td>
<td>1</td>
<td>12</td>
<td>591</td>
<td>1</td>
<td>15</td>
<td>789</td>
<td>1</td>
<td>12</td>
</tr>
<tr>
<td>195</td>
<td>39</td>
<td>117</td>
<td>393</td>
<td>66</td>
<td>66</td>
<td>597</td>
<td>1</td>
<td>3</td>
<td>795</td>
<td>10</td>
<td>5</td>
</tr>
</tbody>
</table>

Table 1

Multiplier $m_+$ and period $r_+$ in explicit primality tests
for $h \cdot 2^k + 1$ with $h \equiv 3 \pmod{6}$ and $1 \leq h \leq 1000$. 

© 1993 American Mathematical Society
0025-5718/93 $1.00 + .25 per page

S7

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
Table 2

All cases with \( r_s \geq 50 \cdot m_s \) in the explicit primality tests for \( h \cdot 2^k + 1 \) with \( h < 10^6 \).

<table>
<thead>
<tr>
<th>( h )</th>
<th>( m_s )</th>
<th>( r_s )</th>
<th>( h )</th>
<th>( m_s )</th>
<th>( r_s )</th>
<th>( h )</th>
<th>( m_s )</th>
<th>( r_s )</th>
</tr>
</thead>
<tbody>
<tr>
<td>165</td>
<td>1200</td>
<td>1200</td>
<td>17875</td>
<td>1020</td>
<td>1020</td>
<td>17875</td>
<td>1020</td>
<td>1020</td>
</tr>
<tr>
<td>245</td>
<td>760</td>
<td>760</td>
<td>20605</td>
<td>2952</td>
<td>2952</td>
<td>20605</td>
<td>2952</td>
<td>2952</td>
</tr>
<tr>
<td>465</td>
<td>600</td>
<td>600</td>
<td>21615</td>
<td>1661</td>
<td>1661</td>
<td>21615</td>
<td>1661</td>
<td>1661</td>
</tr>
<tr>
<td>777</td>
<td>67310</td>
<td>67310</td>
<td>21945</td>
<td>9796</td>
<td>9796</td>
<td>21945</td>
<td>9796</td>
<td>9796</td>
</tr>
<tr>
<td>1775</td>
<td>18561</td>
<td>18561</td>
<td>22145</td>
<td>54604</td>
<td>54604</td>
<td>22145</td>
<td>54604</td>
<td>54604</td>
</tr>
<tr>
<td>2113</td>
<td>9070</td>
<td>9070</td>
<td>23073</td>
<td>12782</td>
<td>12782</td>
<td>23073</td>
<td>12782</td>
<td>12782</td>
</tr>
<tr>
<td>2770</td>
<td>2132</td>
<td>2132</td>
<td>24165</td>
<td>106534</td>
<td>106534</td>
<td>24165</td>
<td>106534</td>
<td>106534</td>
</tr>
<tr>
<td>3103</td>
<td>629</td>
<td>1274</td>
<td>26065</td>
<td>37260</td>
<td>37260</td>
<td>26065</td>
<td>37260</td>
<td>37260</td>
</tr>
<tr>
<td>3185</td>
<td>19110</td>
<td>19110</td>
<td>30357</td>
<td>540</td>
<td>540</td>
<td>30357</td>
<td>540</td>
<td>540</td>
</tr>
<tr>
<td>1209</td>
<td>752</td>
<td>752</td>
<td>30915</td>
<td>519</td>
<td>1038</td>
<td>30915</td>
<td>519</td>
<td>1038</td>
</tr>
<tr>
<td>3672</td>
<td>1110</td>
<td>1110</td>
<td>31615</td>
<td>581</td>
<td>581</td>
<td>31615</td>
<td>581</td>
<td>581</td>
</tr>
<tr>
<td>5175</td>
<td>575</td>
<td>575</td>
<td>32165</td>
<td>719</td>
<td>2919</td>
<td>32165</td>
<td>719</td>
<td>2919</td>
</tr>
<tr>
<td>6293</td>
<td>10988</td>
<td>10988</td>
<td>32345</td>
<td>14260</td>
<td>14260</td>
<td>32345</td>
<td>14260</td>
<td>14260</td>
</tr>
<tr>
<td>7755</td>
<td>781</td>
<td>781</td>
<td>33735</td>
<td>519</td>
<td>1038</td>
<td>33735</td>
<td>519</td>
<td>1038</td>
</tr>
<tr>
<td>7905</td>
<td>1115</td>
<td>1115</td>
<td>34191</td>
<td>522</td>
<td>522</td>
<td>34191</td>
<td>522</td>
<td>522</td>
</tr>
<tr>
<td>9213</td>
<td>3071</td>
<td>6112</td>
<td>37173</td>
<td>990</td>
<td>990</td>
<td>37173</td>
<td>990</td>
<td>990</td>
</tr>
<tr>
<td>9521</td>
<td>543</td>
<td>1096</td>
<td>38145</td>
<td>1055</td>
<td>4220</td>
<td>38145</td>
<td>1055</td>
<td>4220</td>
</tr>
<tr>
<td>10183</td>
<td>8100</td>
<td>8100</td>
<td>38153</td>
<td>1540</td>
<td>1540</td>
<td>38153</td>
<td>1540</td>
<td>1540</td>
</tr>
<tr>
<td>10533</td>
<td>510</td>
<td>510</td>
<td>39225</td>
<td>9120</td>
<td>9120</td>
<td>39225</td>
<td>9120</td>
<td>9120</td>
</tr>
<tr>
<td>10515</td>
<td>510</td>
<td>510</td>
<td>39655</td>
<td>510</td>
<td>510</td>
<td>39655</td>
<td>510</td>
<td>510</td>
</tr>
<tr>
<td>10300</td>
<td>831</td>
<td>3321</td>
<td>39706</td>
<td>516</td>
<td>516</td>
<td>39706</td>
<td>516</td>
<td>516</td>
</tr>
<tr>
<td>11393</td>
<td>1857</td>
<td>1857</td>
<td>37510</td>
<td>516</td>
<td>516</td>
<td>37510</td>
<td>516</td>
<td>516</td>
</tr>
<tr>
<td>11388</td>
<td>2566</td>
<td>2566</td>
<td>34367</td>
<td>743</td>
<td>743</td>
<td>34367</td>
<td>743</td>
<td>743</td>
</tr>
<tr>
<td>12337</td>
<td>1791</td>
<td>1791</td>
<td>34781</td>
<td>556</td>
<td>1668</td>
<td>34781</td>
<td>556</td>
<td>1668</td>
</tr>
<tr>
<td>12795</td>
<td>2379</td>
<td>2379</td>
<td>39165</td>
<td>1119</td>
<td>17904</td>
<td>39165</td>
<td>1119</td>
<td>17904</td>
</tr>
<tr>
<td>13045</td>
<td>9270</td>
<td>9270</td>
<td>39545</td>
<td>990</td>
<td>990</td>
<td>39545</td>
<td>990</td>
<td>990</td>
</tr>
<tr>
<td>13222</td>
<td>8084</td>
<td>8084</td>
<td>39921</td>
<td>562</td>
<td>4496</td>
<td>39921</td>
<td>562</td>
<td>4496</td>
</tr>
<tr>
<td>16090</td>
<td>6370</td>
<td>6370</td>
<td>43071</td>
<td>546</td>
<td>2314</td>
<td>43071</td>
<td>546</td>
<td>2314</td>
</tr>
<tr>
<td>17955</td>
<td>4158</td>
<td>4158</td>
<td>41097</td>
<td>818</td>
<td>818</td>
<td>41097</td>
<td>818</td>
<td>818</td>
</tr>
<tr>
<td>18438</td>
<td>6111</td>
<td>6111</td>
<td>66083</td>
<td>576</td>
<td>576</td>
<td>66083</td>
<td>576</td>
<td>576</td>
</tr>
<tr>
<td>18513</td>
<td>8772</td>
<td>8772</td>
<td>69711</td>
<td>612</td>
<td>612</td>
<td>69711</td>
<td>612</td>
<td>612</td>
</tr>
</tbody>
</table>

Table 3

All cases with multiplicity \( m_s \geq 500 \) in the explicit primality test for \( h \cdot 2^k + 1 \) with \( h < 10^6 \).

Table 4

Multiplier \( m_s \) and period \( r_s \) in explicit primality tests for \( h \cdot 2^k + 1 \) with \( h \equiv 3 \mod 6 \) and 1 \( \leq h \leq 1000 \).

<table>
<thead>
<tr>
<th>( h \cdot m_s \cdot r_s )</th>
<th>( h \cdot m_s \cdot r_s )</th>
<th>( h \cdot m_s \cdot r_s )</th>
<th>( h \cdot m_s \cdot r_s )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 1 )</td>
<td>( 1 )</td>
<td>( 201 )</td>
<td>( 1 )</td>
</tr>
<tr>
<td>( 9 )</td>
<td>( 1 )</td>
<td>( 207 )</td>
<td>( 12 )</td>
</tr>
<tr>
<td>( 15 )</td>
<td>( 1 )</td>
<td>( 213 )</td>
<td>( 8 )</td>
</tr>
</tbody>
</table>
### Table 5

All cases with \( r_- \geq 50 \cdot m_- \) in the explicit primality test for \( h \cdot 2^k - 1 \) with \( h < 10^3 \).

<table>
<thead>
<tr>
<th>( h )</th>
<th>( m_- )</th>
<th>( r_- )</th>
<th>( h )</th>
<th>( m_- )</th>
<th>( r_- )</th>
<th>( h )</th>
<th>( m_- )</th>
<th>( r_- )</th>
<th>( h )</th>
<th>( m_- )</th>
<th>( r_- )</th>
</tr>
</thead>
<tbody>
<tr>
<td>3063</td>
<td>108</td>
<td>55</td>
<td>2467</td>
<td>106</td>
<td>50</td>
<td>4975</td>
<td>106</td>
<td>50</td>
<td>4975</td>
<td>106</td>
<td>50</td>
</tr>
<tr>
<td>6135</td>
<td>108</td>
<td>55</td>
<td>2467</td>
<td>106</td>
<td>50</td>
<td>4975</td>
<td>106</td>
<td>50</td>
<td>4975</td>
<td>106</td>
<td>50</td>
</tr>
<tr>
<td>6143</td>
<td>108</td>
<td>55</td>
<td>2467</td>
<td>106</td>
<td>50</td>
<td>4975</td>
<td>106</td>
<td>50</td>
<td>4975</td>
<td>106</td>
<td>50</td>
</tr>
<tr>
<td>4145</td>
<td>108</td>
<td>55</td>
<td>2467</td>
<td>106</td>
<td>50</td>
<td>4975</td>
<td>106</td>
<td>50</td>
<td>4975</td>
<td>106</td>
<td>50</td>
</tr>
<tr>
<td>7135</td>
<td>108</td>
<td>55</td>
<td>2467</td>
<td>106</td>
<td>50</td>
<td>4975</td>
<td>106</td>
<td>50</td>
<td>4975</td>
<td>106</td>
<td>50</td>
</tr>
<tr>
<td>10215</td>
<td>108</td>
<td>55</td>
<td>2467</td>
<td>106</td>
<td>50</td>
<td>4975</td>
<td>106</td>
<td>50</td>
<td>4975</td>
<td>106</td>
<td>50</td>
</tr>
<tr>
<td>13143</td>
<td>108</td>
<td>55</td>
<td>2467</td>
<td>106</td>
<td>50</td>
<td>4975</td>
<td>106</td>
<td>50</td>
<td>4975</td>
<td>106</td>
<td>50</td>
</tr>
<tr>
<td>14007</td>
<td>108</td>
<td>55</td>
<td>2467</td>
<td>106</td>
<td>50</td>
<td>4975</td>
<td>106</td>
<td>50</td>
<td>4975</td>
<td>106</td>
<td>50</td>
</tr>
<tr>
<td>21015</td>
<td>108</td>
<td>55</td>
<td>2467</td>
<td>106</td>
<td>50</td>
<td>4975</td>
<td>106</td>
<td>50</td>
<td>4975</td>
<td>106</td>
<td>50</td>
</tr>
<tr>
<td>21023</td>
<td>108</td>
<td>55</td>
<td>2467</td>
<td>106</td>
<td>50</td>
<td>4975</td>
<td>106</td>
<td>50</td>
<td>4975</td>
<td>106</td>
<td>50</td>
</tr>
</tbody>
</table>

### Table 6

All cases with multiplier \( m_- \geq 100 \) in the explicit primality test for \( h \cdot 2^k - 1 \) with \( h < 10^3 \).

<table>
<thead>
<tr>
<th>( h )</th>
<th>( m_- )</th>
<th>( r_- )</th>
<th>( h )</th>
<th>( m_- )</th>
<th>( r_- )</th>
<th>( h )</th>
<th>( m_- )</th>
<th>( r_- )</th>
<th>( h )</th>
<th>( m_- )</th>
<th>( r_- )</th>
</tr>
</thead>
<tbody>
<tr>
<td>6135</td>
<td>108</td>
<td>55</td>
<td>2467</td>
<td>106</td>
<td>50</td>
<td>4975</td>
<td>106</td>
<td>50</td>
<td>4975</td>
<td>106</td>
<td>50</td>
</tr>
<tr>
<td>6143</td>
<td>108</td>
<td>55</td>
<td>2467</td>
<td>106</td>
<td>50</td>
<td>4975</td>
<td>106</td>
<td>50</td>
<td>4975</td>
<td>106</td>
<td>50</td>
</tr>
<tr>
<td>4145</td>
<td>108</td>
<td>55</td>
<td>2467</td>
<td>106</td>
<td>50</td>
<td>4975</td>
<td>106</td>
<td>50</td>
<td>4975</td>
<td>106</td>
<td>50</td>
</tr>
<tr>
<td>7135</td>
<td>108</td>
<td>55</td>
<td>2467</td>
<td>106</td>
<td>50</td>
<td>4975</td>
<td>106</td>
<td>50</td>
<td>4975</td>
<td>106</td>
<td>50</td>
</tr>
<tr>
<td>10215</td>
<td>108</td>
<td>55</td>
<td>2467</td>
<td>106</td>
<td>50</td>
<td>4975</td>
<td>106</td>
<td>50</td>
<td>4975</td>
<td>106</td>
<td>50</td>
</tr>
<tr>
<td>13143</td>
<td>108</td>
<td>55</td>
<td>2467</td>
<td>106</td>
<td>50</td>
<td>4975</td>
<td>106</td>
<td>50</td>
<td>4975</td>
<td>106</td>
<td>50</td>
</tr>
<tr>
<td>14007</td>
<td>108</td>
<td>55</td>
<td>2467</td>
<td>106</td>
<td>50</td>
<td>4975</td>
<td>106</td>
<td>50</td>
<td>4975</td>
<td>106</td>
<td>50</td>
</tr>
<tr>
<td>21015</td>
<td>108</td>
<td>55</td>
<td>2467</td>
<td>106</td>
<td>50</td>
<td>4975</td>
<td>106</td>
<td>50</td>
<td>4975</td>
<td>106</td>
<td>50</td>
</tr>
<tr>
<td>21023</td>
<td>108</td>
<td>55</td>
<td>2467</td>
<td>106</td>
<td>50</td>
<td>4975</td>
<td>106</td>
<td>50</td>
<td>4975</td>
<td>106</td>
<td>50</td>
</tr>
</tbody>
</table>