ARKIV FÖR MATEMATIK Band 3 nr 20

Communicated 9 February 1955 by OTTO FROSTMAN

A note on the prime numbers of the forms $N=(6a+1)2^{2^{n-1}}-1$ and $M=(6a-1)2^{2^n}-1$

By HANS RIESEL

The purpose of this paper is to give a direct proof of the following two criteria for the primality of the numbers of the above forms. The theorems are, except for a slight modification of the conditions, known by LEHMER [1] and BREWER [2] who proved a more general theorem of this kind. Then we take up to discussion if the third inequality in the theorems could be removed, and show that this is not the case. Finally we give a numerical example and a table of some primes of the discussed forms.

Theorem 1. Let a and n be integers satisfying

$$a \geqq 0,\ n \geqq 2,\ 2^{2^{n-1}} > a. \tag{1}$$

Let a sequence u_i of integers be defined by the recurrence relation

$$u_{i+1} = u_i^2 - 2 \qquad (i = 1, 2, 3, \ldots),$$

with

$$u_1 = (2+\sqrt{3})^{6a+1} + (2-\sqrt{3})^{6a+1}.$$

Then a necessary and sufficient condition that the number $N=(6a+1)2^{2^{n-1}}-1$ should be a prime is that

$$u_{2^{n-2}} \equiv 0 \pmod{N}. \tag{2}$$

Theorem 2. Let a and n be integers satisfying

$$a \geqq 1,\ n \geqq 2,\ 2^{2^n} - 1 \geqq a. \tag{1'}$$

Let a sequence v_i of integers be defined by the recurrence relation

$$v_{i+1} = v_i^2 - 2 \qquad (i = 1, 2, 3, \ldots),$$

with

$$v_1 = (2+\sqrt{3})^{6a-1} + (2-\sqrt{3})^{6a-1}.$$

Then a necessary and sufficient condition that the number $M=(6a-1)2^{2^n}-1$ should be a prime is that

$$v_{2^{n-1}} \equiv 0 \pmod{M}. \tag{2'}$$

Preliminary remarks. The proofs of the two theorems will follow the same lines and are very similar. Here we give the full details of the proof only for Theorem 1, and sketch the proof of Theorem 2. The first part of the proof follows a proof by WESTERN [3] for the special case $a=0$ in Theorem 1.

The proof is based on some results from the theory of the quadratic number field $K(\sqrt{3})$, where K is the field of rational numbers. The field $K(\sqrt{3})$ has the following well-known properties:

The integers x in the field are of the form $x=a+b\sqrt{3}$, where a and b are rational integers. The units are $\pm(2+\sqrt{3})^n$, n a rational integer. The conjugated number $\bar{x}$ of $x=a+b\sqrt{3}$ is $\bar{x}=a-b\sqrt{3}$. The norm $N(x)$ of x is defined by $N(x)=x\bar{x}=a^2-3b^2$.

There are two kinds of primes in the field (excepting the factors of 2 and 3). Firstly, all rational primes q of one of the forms $q=12s\pm5$. Secondly, all primes $\pi=a+b\sqrt{3}$, whose norm $\pi\bar{\pi}=a^2-3b^2$ equals a rational prime p of one of the forms $p=12s\pm1$.

We need the following analogue of Fermat's theorem: Let q be a prime of one of the forms $q=12s\pm5$. Then, if x is an integer in the field, we have

$$x^q\equiv\bar{x} \pmod{q}. \tag{3}$$

Proof: Let $x=a+b\sqrt{3}$. Then we have

$$x^q=(a+b\sqrt{3})^q\equiv a^q+b^q(\sqrt{3})^q\equiv a+b\cdot(3)^{\frac{q-1}{2}}\sqrt{3}\equiv a-b\sqrt{3}=\bar{x} \pmod{q}$$

by the binomial theorem, Fermat's theorem for rational integers and since

$$3^{\frac{q-1}{2}}\equiv\left(\frac{3}{q}\right)=-1 \pmod{q}.$$

$\left(\left(\frac{3}{q}\right)$ is Legendre's symbol, and $\left(\frac{3}{q}\right)=-1$ if $q=12s\pm5\right)$.

We also require the following *lemma:* Let x be an integer of the field $K(\sqrt{3})$. Let d (if it exists) be the smallest positive exponent for which the congruence

$$x^d\equiv-1 \pmod{q} \quad (q \text{ prime}) \tag{4}$$

holds. Then, if ω is any exponent for which one of the congruences

$$x^\omega\equiv-1 \pmod{q} \quad \text{or} \quad x^\omega\equiv1 \pmod{q} \tag{5}$$

holds, ω is an odd or an even multiple of d, respectively.

Since the corresponding lemma for the rational integers is well known and since the proof in the field $K(\sqrt{3})$ is the same, we omit the proof.

Proof of Theorem 1. We find $N=(6a+1)2^{2n-1}-1\equiv-1 \pmod{8}$ (since $n\geqq2$) and $N=(6a+1)4^{n-1}\cdot2-1\equiv(6a+1)\cdot4\cdot2-1\equiv7 \pmod{12}$.

First, we prove the necessity of condition (2). Suppose N is a prime. Then Legendre's symbols $\left(\frac{-1}{N}\right)$, $\left(\frac{2}{N}\right)$ and $\left(\frac{-2}{N}\right)$ have the values

$$\left(\frac{-1}{N}\right)=-1,\ \left(\frac{2}{N}\right)=+1,\ \left(\frac{-2}{N}\right)=-1,$$

and

$$\left(\frac{-2}{N}\right)\equiv(-2)^{\frac{N-1}{2}}=(1+\sqrt{3})^{\frac{N-1}{2}}(1-\sqrt{3})^{\frac{N-1}{2}}\equiv-1 \pmod N$$

or

$$\left(\frac{1+\sqrt{3}}{1-\sqrt{3}}\right)^{\frac{N-1}{2}}(1-\sqrt{3})^{N-1}\equiv-1 \pmod N$$

or

$$\left(\frac{1+\sqrt{3}}{1-\sqrt{3}}\right)^{\frac{N-1}{2}}\frac{2}{1-\sqrt{3}}(1-\sqrt{3})^{N}\equiv-2 \pmod N.$$

Now $(1-\sqrt{3})^N\equiv 1+\sqrt{3} \pmod N$, according to (3), and cancelling the factor 2, we find

$$\left(\frac{1+\sqrt{3}}{1-\sqrt{3}}\right)^{\frac{N+1}{2}}\equiv-1 \pmod N.$$

Since $\frac{1+\sqrt{3}}{1-\sqrt{3}}=\frac{(1+\sqrt{3})^2}{-2}=-(2+\sqrt{3})$, we find

$$(-1)^{\frac{N+1}{2}}(2+\sqrt{3})^{\frac{N+1}{2}}\equiv-1 \pmod N,$$

or since $(-1)^{\frac{N+1}{2}}=1$,

$$(2+\sqrt{3})^{\frac{N+1}{2}}\equiv-1 \pmod N. \tag{6}$$

Adding 1 and multiplying by $(2-\sqrt{3})^{\frac{N+1}{4}}$, we see that congruence (6) implies

$$(2+\sqrt{3})^{\frac{N+1}{4}}+(2-\sqrt{3})^{\frac{N+1}{4}}\equiv 0 \pmod N. \tag{7}$$

This, however, is the same as condition (2), since

$$\begin{aligned}
u_1&=(2+\sqrt{3})^{6a+1}+(2-\sqrt{3})^{6a+1},\\
u_2&=u_1^2-2=(2+\sqrt{3})^{(6a+1)2}+(2-\sqrt{3})^{(6a+1)2},\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
u_{2n-2}&=u_{2n-3}^2-2=(2+\sqrt{3})^{(6a+1)2^{2n-3}}+(2-\sqrt{3})^{(6a+1)2^{2n-3}}\\
&=(2+\sqrt{3})^{\frac{N+1}{4}}+(2-\sqrt{3})^{\frac{N+1}{4}}.
\end{aligned}$$

This shows the necessity of condition (2), if N is a prime.

We now proceed to prove the sufficiency of the conditions given in Theorem 1. Suppose that $u_{2n-2} \equiv 0 \pmod{N}$, or, which is the same thing, that congruence (7) holds. By multiplying this congruence by $(2+\sqrt{3})^{(N+1)/4}$ we obtain congruence (6). Now, since N has the form $12s+7$, and since the product of primes of the forms $12s \pm 1$ yield a number of the same form, N must have a prime factor q of one of the forms $12s \pm 5$. Since congruence (6) holds for the modulus N, it holds, *a fortiori*, for any modulus dividing N, and we obtain

$$(2+\sqrt{3})^{\frac{N+1}{2}} \equiv -1 \pmod{q}.$$

The analogue of Fermat's theorem gives us

$$(2+\sqrt{3})^{q} \equiv 2-\sqrt{3} \pmod{q},$$

or

$$(2+\sqrt{3})^{q+1} \equiv 1 \pmod{q}.$$

Suppose now that d is the smallest positive exponent for which

$$(2+\sqrt{3})^{d} \equiv -1 \pmod{q}.$$

Using the lemma from the preliminary remarks, we conclude that

$$\frac{N+1}{2} = (6a+1)\,2^{2n-2} = kd \qquad (k \text{ an odd number})$$

and that

$$q+1 = jd \ (j \text{ an even number}).$$

Since k is odd, d must contain the factor 2^{2n-2}, and since j is even, $q+1$ contains the factor 2^{2n-1}. Hence we see that if N were not prime we should find a factorisation of the form

$$N = (6a+1)\,2^{2n-1} - 1 = z \cdot q = z\,(m \cdot 2^{2n-1} - 1),$$

with a $z > 1$. If we consider this factorisation (mod 2^{2n-1}), we find that $z \equiv 1 \pmod{2^{2n-1}}$, and that N must have the form

$$N = (6a+1)\,2^{2n-1} - 1 = (l \cdot 2^{2n-1} + 1)\,(m \cdot 2^{2n-1} - 1). \tag{8}$$

The case $l = 0$, $m = 6a+1$ corresponds to the trivial decomposition $N = 1 \cdot N$.

Decomposition (8) implies

$$6a+1 = lm \cdot 2^{2n-1} + m - l = f(l, m) \text{ say.} \tag{9}$$

Considering (9) (mod 2) and (mod 3), we obtain

$$\begin{aligned} 1 &\equiv m - l \pmod{2} \\ \text{and} \qquad 1 + lm &\equiv m - l \pmod{3}. \end{aligned} \tag{10}$$

From these congruences it follows that the values of m and l:

$$\begin{aligned} &m=1,\ l=1,\ 2,\ 3,\ 4,\ 5\\ &m=2,\ l=1,\ 2\\ &m=3,\ l=1\\ &m=4,\ l=1,\ 2\\ &m=5,\ l=1,\ 2,\ 3 \end{aligned} \tag{11}$$

are impossible.

We shall now obtain the smallest possible value of the function $f(l, m)$. Since $f(l, m)$ is an increasing function of l and of m, and since $l>m$ implies $f(l, m)<f(m, l)$, we find:

If $m=1$, l must be $\geqq 6$, and

$$f(l, 1)\geqq f(6, 1)=6\cdot 2^{2n-1}-5.$$

In the same way we find:

$$\begin{aligned} f(l, 2)&\geqq f(3, 2)= 6\cdot 2^{2n-1}-1,\\ f(l, 3)&\geqq f(2, 3)= 6\cdot 2^{2n-1}+1,\\ f(l, 4)&\geqq f(3, 4)=12\cdot 2^{2n-1}+1,\\ f(l, 5)&\geqq f(4, 5)=20\cdot 2^{2n-1}+1, \end{aligned}$$

and finally, if $m\geqq 6$

$$f(l, m)\geqq f(l, 6)\geqq f(1, 6)=6\cdot 2^{2n-1}+5.$$

Since the smallest of these expressions is $6\cdot 2^{2n-1}-5$, this shows that $f(l, m)$ for those values of l and m which are compatible with the congruences (10), satisfies

$$f(l, m)=6a+1\geqq 6\cdot 2^{2n-1}-5.$$

Hence, if the opposite inequality

$$6a+1<6\cdot 2^{2n-1}-5$$

holds, we conclude that the decomposition (8), with any $l>0$, is impossible. The last inequality reduces to

$$a<2^{2n-1}-1,$$

and so we have proved Theorem 1.

For Theorem 2 we find that M satisfies the same congruence relations (mod 8) and (mod 12) as N, and so we have the congruences (6) and (7) in exactly the same manner, but with M instead of N:

$$(2+\sqrt{3})^{\frac{M+1}{4}}+(2-\sqrt{3})^{\frac{M+1}{4}}\equiv 0 \pmod{M}. \tag{7'}$$

Since $M=(6a-1)2^{2^n}-1$, we find that (7′) implies $v_{2^{n-1}}\equiv 0 \pmod{M}$, if $v_{i+1}=v_i^2-2$ $(i=1, 2, 3, \ldots)$, and

$$v_1=(2+\sqrt{3})^{6a-1}+(2-\sqrt{3})^{6a-1}.$$

The proof of the sufficiency leads in the same way as for Theorem 1 to the decomposition

$$M=(6a-1)\,2^{2^n}-1=(l\cdot 2^{2^n}+1)\,(m\cdot 2^{2^n}-1) \tag{8′}$$

and to

$$6a-1=lm\cdot 2^{2^n}+m-l=f'(l, m) \text{ say,} \tag{9′}$$

and to the congruences

$$\begin{aligned} &1\equiv l-m \pmod 2 \\ \text{and} \qquad &\qquad\qquad (10′) \\ &1+lm\equiv l-m \pmod 3. \end{aligned}$$

The impossible values (11) are impossible in this case too, and the smallest value of the function $f'(l, m)$ again occurs for $l=6$, $m=1$, and finally, the inequality

$$6a-1<6\cdot 2^{2^n}-5,$$

which makes (8′) impossible with an $l>0$ leads to

$$a<2^{2^n}-\tfrac{2}{3},$$

that is

$$a\leqq 2^{2^n}-1.$$

Remark 1. If, in Theorem 1, $a=0$, we have the following theorem: The number $N=2^{2^{n-1}}-1$ is a prime, if and only if $u_{2^{n-2}}\equiv 0 \pmod{N}$, where $u_{i+1}=u_i^2-2$ $(i=1, 2, 3, \ldots)$ and $u_1=4$.

This is the well-known Lucas's theorem for the primality of Mersenne's numbers. See WESTERN [3].

Remark 2. It is natural to ask whether Theorem 1 holds if the inequality

$$2^{2^{n-1}}>a$$

is not fulfilled, or whether this inequality is essential.[1] We are going to prove that at least *some* kind of extra condition is needed, if $2^{2^{n-1}}>a$ is not fulfilled.

To prove this, let us in the case $n=2$ try to construct a composed number N for which congruence (6) holds. Then everything in Theorem 1 will be satisfied except, of course, the inequality $2^{2^{n-1}}>a$.

Suppose that $N=(6a+1)\cdot 8-1=48a+7$ is the product of three different primes $q_i=48n_i+7$ $(i=1, 2, 3)$ of the same form as N. Since $7^2\equiv 1 \pmod{48}$

[1] This problem does not seem to have been treated before.

and $7^3 \equiv 7 \pmod{48}$, this is no contradiction. From the proof of the necessity of condition (2) in Theorem 1 it now follows that

$$(2+\sqrt{3})^{\frac{q_i+1}{2}} \equiv -1 \pmod{q_i} \qquad (i=1,2,3).$$

A sufficient condition that

$$(2+\sqrt{3})^{\frac{N+1}{2}} \equiv -1 \pmod{N} \equiv -1 \pmod{q_i} \qquad (i=1,2,3)$$

evidently is that

$$\frac{N+1}{2} \text{ is an odd multiple of } \frac{q_i+1}{2} \qquad (i=1,2,3).$$

Now, suppose that any two of the numbers $(q_i+1)/8$ $(i=1,2,3)$ have the same greatest common divisor d and that

$$\frac{q_i+1}{2} = \frac{48\,n_i+7+1}{2} = 4\,(6\,n_i+1) = 4\,d\,p_i \qquad (i=1,2,3).$$

We conclude that

$$\frac{N+1}{2} = \frac{q_1\,q_2\,q_3+1}{2} = \frac{(8\,d\,p_1-1)\,(8\,d\,p_2-1)\,(8\,d\,p_3-1)+1}{2}$$

should be an odd multiple of $4\,d\,p_1\,p_2\,p_3$, or, which is the same thing, that

$$64\,d^3\,p_1\,p_2\,p_3 - 8\,d^2\,(p_1\,p_2+p_1\,p_3+p_2\,p_3) + d\,(p_1+p_2+p_3) \tag{12}$$

should be an odd multiple of $d\,p_1\,p_2\,p_3$.

Since d and the p_i must be odd numbers, the number (12) is odd, and so this number is an *odd* multiple of $d\,p_1\,p_2\,p_3$ if

$$64\,d^3\,p_1\,p_2\,p_3 - 8\,d^2\,(p_1\,p_2+p_1\,p_3+p_2\,p_3) + d\,(p_1+p_2+p_3) \equiv 0 \pmod{d\,p_1\,p_2\,p_3},$$

or

$$8\,d\,(p_1\,p_2+p_1\,p_3+p_2\,p_3) \equiv p_1+p_2+p_3 \pmod{p_1\,p_2\,p_3}. \tag{13}$$

Since $d\,p_i = 6\,n_i+1$, all the numbers d and p_i must be of one of the forms $6\,s+1$ or $6\,s-1$. Now, for the p_i choose 3 numbers, relatively prime in pairs, and of one of the forms $6\,s \pm 1$, e.g.

$$p_1 = 1, \quad p_2 = 7 \quad \text{and} \quad p_3 = 13.$$

Congruence (13) becomes

$$8\,d \cdot 111 \equiv 21 \pmod{91}$$

with the extra condition

$$d \equiv 1 \pmod{6}.$$

These two last congruences have the solutions

$$d \equiv 301 \pmod{546} = 546x + 301,$$

and we find

$$q_1 = 8dp_1 - 1 = \quad 8d - 1 = \quad 4\,368x + \quad 2\,407,$$

$$q_2 = 8dp_2 - 1 = \quad 56d - 1 = 30\,576x + 16\,855,$$

and

$$q_3 = 8dp_3 - 1 = 104d - 1 = 56\,784x + 31\,303.$$

The only thing that remains is to determine an x for which all q_i are primes; the prime tables show that the values $x = 37$ and $x = 89$ fit, and so we have:

$$N_1 = 164\,023 \cdot 1\,148\,167 \cdot 2\,132\,311$$

and

$$N_2 = 391\,159 \cdot 2\,738\,119 \cdot 5\,085\,079$$

are composed numbers for which congruence (6) holds.

In the same way we can construct an example to show that the inequality

$$2^{2n} - 1 \geqq a$$

in Theorem 2 could not simply be removed. We have found

$$M = 327\,823 \cdot 2\,294\,767 \cdot 4\,261\,711.$$

Numerical example. For the number $M = 5 \cdot 2^{14} - 1 = 81\,919$ the conditions of theorem 2 are fulfilled, and we find

$$v_1 = \quad 724,\ v_2 \equiv 32\,660,\ v_3 \equiv \quad 8\,299,\ v_4 \equiv 61\,439,\ v_5 \equiv \quad 5\,118,$$

$$v_6 \equiv 61\,761,\ v_7 \equiv 26\,722,\ v_8 \equiv 59\,278,\ v_9 \equiv 47\,696,\ v_{10} \equiv 17\,784,$$

$$v_{11} \equiv 63\,314,\ v_{12} \equiv 38\,248 \text{ and } v_{13} \equiv 0, \text{ all congruences taken (mod } 81\,919).$$

The last congruence shows that the number 81 919 is a prime.

Putting $a = 2$, we find $u_1 = 27\,246\,964$ and $v_1 = 1\,956\,244$.

Putting $a = 3$, we find $u_1 = 73\,621\,286\,644$ and $v_1 = 5\,285\,770\,564$.

Theorems 1 and 2 were used to find the prime character of some numbers $(6a \pm 1)\,2^e - 1$. The calculations were made on the Swedish high speed electronic computer BESK for all values of $6a \pm 1 < 56$ and $e \leqq 150$, except for $6a \pm 1 = 5$, 7 and 11, where e takes all values $\leqq 250$.

Those numbers which were found to be primes were tested once more by BESK. The result was that the numbers N and M were prime for the following values of $6a \pm 1$ and e, and composite otherwise (the values of $e = 1, 2, 3$ are taken from the prime tables):

$6a \pm 1$	$e\ (\leqq 250)$
5	2, 4, 8, 10, 12, 14, 18, 32, 48, 54, 72, 148, 184, 248
7	1, 5, 9, 17, 21, 29, 45, 177
11	2, 26, 50, 54, 126, 134, 246
	$e\ (\leqq 150)$
13	3, 7, 23
17	2, 4, 6, 16, 20, 36, 54, 60, 96, 124, 150
19	1, 3, 5, 21, 41, 49, 89, 133, 141
23	4, 6, 12, 46, 72
25	3, 9, 11, 17, 23, 35, 39, 75, 105, 107
29	4, 16, 76, 148
31	1, 5, 7, 11, 13, 23, 33, 35, 37, 47, 115
35	2, 6, 10, 20, 44, 114, 146
37	1
41	2, 10, 14, 18, 50, 114, 122
43	7, 31, 67
47	4, 14, 70, 78
49	1, 5, 7, 9, 13, 15, 29, 33, 39, 55, 81, 95
53	2, 6, 8, 42, 50, 62
55	1, 3, 5, 7, 15, 33, 41, 57, 69, 75, 77, 131, 133

BESK also verified that the known Mersenne numbers up to $2^{607}-1$ are primes.

REFERENCES

1. D. H. LEHMER, Annals of Math. (2), *31*, 446 (1930).
2. B. W. BREWER, Duke Math. Journ. *18*, 757 (1951).
3. A. E. WESTERN, Journ. of the London Math. Soc. *7*, 130 (1932).

Tryckt den 7 maj 1955

Uppsala 1955. Almqvist & Wiksells Boktryckeri AB