PRIMALITY TESTS FOR NUMBERS OF THE FORM $k \cdot 2^m \pm 1$

Zhi-Hong Sun

Department of Mathematics, Huaiyin Teachers College, Huaian, Jiangsu 223001, P.R. China
e-mail: zhsun@hytc.edu.cn

(Submitted January 2004-Final Revision December 2004)

ABSTRACT

Let $k, m \in \mathbb{Z}$, $m \geq 2$, $0 < k < 2^m$ and $2 \not| k$. In the paper we give a general primality criterion for numbers of the form $k \cdot 2^m \pm 1$, which can be viewed as a generalization of the Lucas-Lehmer test for Mersenne primes. In particular, for $k = 3, 9$ we obtain explicit primality tests, which are simpler than current known results. We also give a new primality test for Fermat numbers and criteria for $9 \cdot 2^{4n+3} \pm 1$, $3 \cdot 2^{20n+6} \pm 1$ or $3 \cdot 2^{36n+6} \pm 1$ to be twin primes.

1. INTRODUCTION

For nonnegative integers n, the numbers $F_n = 2^{2^n} + 1$ are called the Fermat numbers. In 1878 Pepin showed that $F_n (n \geq 1)$ is prime if and only if $3^{(F_n - 1)/2} \equiv -1 \pmod{F_n}$. For primes p, let $M_p = 2^p - 1$. The famous Lucas-Lehmer test states that M_p is a Mersenne prime if and only if $M_p \mid S_{p-2}$, where $\{S_n\}$ is given by $S_0 = 4$ and $S_{k+1} = S_k^2 - 2$ $(k = 0, 1, 2, \dots)$.

In [1], [2], [6] and [9], W. Borho, W. Bosma, H. Riesel and H.C. Williams extended the above two tests to numbers of the form $k \cdot 2^m \pm 1$, where $0 < k < 2^m$ and k is odd. For example, we have the following known results.

Theorem 1.1: Let $p = k \cdot 2^m + 1$ with $m \geq 2$, $0 < k < 2^m$, $2 \not| k$ and $D \in \mathbb{Z}$ with the Jacobi symbol $\left(\frac{D}{p}\right) = -1$. Then p is prime if and only if $D^{(p-1)/2} \equiv -1 \pmod{p}$. In particular, if $3 \not| k$ we may take $D = 3$.

Let $\{S_n(x)\}$ be given by $S_0(x) = x$ and $S_{k+1}(x) = (S_k(x))^2 - 2$ $(k \geq 0)$. Then we have

Theorem 1.2: Let $p = k \cdot 2^m - 1$ with $m \geq 3$, $0 < k < 2^m$ and $k \equiv \pm 1 \pmod{6}$, and let $x = (2 + \sqrt{3})^k + (2 - \sqrt{3})^k$. Then p is prime if and only if $p \mid S_{m-2}(x)$.

Here we point out that the x in Theorem 1.2 is also given by $x = \sum_{r=0}^{(k-1)/2} \frac{k}{k-r} \binom{k-r}{r} (-1)^r 4^{k-2r}$.

In this paper we prove the following main result

(1.1) For $m \geq 2$ let $p = k \cdot 2^m \pm 1$ with $0 < k < 2^m$ and k odd. If b is an integer such that $(\frac{2+b}{p}) = (\frac{2-b}{p}) = -1$, then p is prime if and only if $p \mid S_{m-2}(\sum_{r=0}^{(k-1)/2} \frac{k}{k-r} \binom{k-r}{r} (-1)^r b^{k-2r})$.

As applications of (1.1) we have many new simple primality criteria for numbers of the form $k \cdot 2^m \pm 1 (k = 1, 3, 9)$. Here are some typical results.

(1.2) For $n \geq 1$ the Fermat number F_n is prime if and only if $F_n \mid S_{2^n - 2}(5)$.

(1.3) Let $m \geq 3$ be a positive integer. If $m \equiv 0 \pmod 2$ or $m \equiv 5, 11 \pmod{12}$, then $9 \cdot 2^m - 1$ is composite. If $m \equiv 1, 3, 7, 9 \pmod{12}$, then $9 \cdot 2^m - 1$ is prime if and only if $9 \cdot 2^m - 1 \mid S_{m-2}(x)$, where

$$x = \begin{cases} 5778 & \text{if } m \equiv 1, 9 \pmod{12}, \\ 1330670 & \text{if } m \equiv 3 \pmod{12}, \\ 2186871698 & \text{if } m \equiv 7 \pmod{12}. \end{cases}$$

(1.4) Let n be a nonnegative integer. Then $9 \cdot 2^{4n+3} - 1$ and $9 \cdot 2^{4n+3} + 1$ are twin primes if and only if $(9 \cdot 2^{4n+3})^2 - 1 \mid S_{4n+1}(32672 \cdot 1067459581)$.

Throughout this paper we use the following notations: $\mathbb{Z}$−the set of integers, $\mathbb{N}$−the set of positive integers, $(\frac{d}{p})$−the Jacobi symbol, (m, n)−the greatest common divisor of m and n, $S_n(x)$− the sequence defined by $S_0(x) = x$ and $S_{k+1}(x) = (S_k(x))^2 - 2 (k \geq 0)$.

2. BASIC LEMMAS

For $P, Q \in \mathbb{Z}$ the Lucas sequences $\{U_n(P, Q)\}$ and $\{V_n(P, Q)\}$ are defined by

$$U_0(P, Q) = 0,\ U_1(P, Q) = 1,\ \ U_{n+1}(P, Q) = PU_n(P, Q) - QU_{n-1}(P, Q)\ (n \geq 1)$$

and

$$V_0(P, Q) = 2,\ V_1(P, Q) = P,\ \ V_{n+1}(P, Q) = PV_n(P, Q) - QV_{n-1}(P, Q)\ (n \geq 1).$$

Let $D = P^2 - 4Q$. It is well known that

$$U_n(P, Q) = \frac{1}{\sqrt{D}} \Big\{ \Big(\frac{P + \sqrt{D}}{2} \Big)^n - \Big(\frac{P - \sqrt{D}}{2} \Big)^n \Big\} (D \neq 0) \tag{2.1}$$

and

$$V_n(P, Q) = \Big(\frac{P + \sqrt{D}}{2} \Big)^n + \Big(\frac{P - \sqrt{D}}{2} \Big)^n. \tag{2.2}$$

Set $U_n = U_n(P, Q)$ and $V_n = V_n(P, Q)$. From the above one can easily check that

$$V_n = PU_n - 2QU_{n-1} = 2U_{n+1} - PU_n. \tag{2.3}$$

¿From [5] we also have

$$U_{2n} = U_n V_n,\ V_{2n} = V_n^2 - 2Q^n \quad \textit{and} \quad V_n^2 - DU_n^2 = 4Q^n. \tag{2.4}$$

If p is an odd prime not dividing Q, it is well known that ([5])

$$U_{p-(\frac{D}{p})}(P, Q) \equiv 0 \pmod p \quad \text{and} \quad U_p(P, Q) \equiv \left(\frac{D}{p} \right) \pmod p. \tag{2.5}$$

Let p be an odd prime such that $\left(\frac{Q}{p}\right) = 1$ and $p \not| D$. D. H. Lehmer proved the following stronger congruence (see [4] or [9, p.85]):

$$U_{(p-(\frac{D}{p}))/2}(P,Q) \equiv 0 \pmod p. \tag{2.6}$$

Definition 2.1: Let $P, Q \in \mathbb{Z}$, and p be an odd prime such that $p \not| Q$. Define $r_p(P,Q)$ to be the smallest positive integer n such that $p \mid U_n(P,Q)$.

¿From [5, IV.17] or [9, p.87] we know that $p \mid U_m(P,Q)$ if and only if $r_p(P,Q) \mid m$. This can also be deduced from [9, (4.2.59), p.81]. Using (2.5) and (2.6) we have

Lemma 2.1: *Let P and Q be integers, $D = P^2 - 4Q$, and let p be an odd prime such that $p \not| Q$. Then $r_p(P,Q) \mid p - \left(\frac{D}{p}\right)$. Moreover, if $\left(\frac{Q}{p}\right) = 1$ and $p \not| D$, then $r_p(P,Q) \mid \frac{p-(\frac{D}{p})}{2}$.*

¿From (2.4) and induction we have

Lemma 2.2: *Let $P, Q \in \mathbb{Z}$, $Q \neq 0$ and $n \in \mathbb{N}$. Then $S_n(\frac{P}{\sqrt{Q}}) = Q^{-2^{n-1}} V_{2^n}(P,Q)$.*

Lemma 2.3: *Let $P, Q \in \mathbb{Z}$ and $n \in \mathbb{N}$. Let p be an odd prime such that $p \not| Q(P^2 - 4Q)$ and $S_n(P/\sqrt{Q}) \equiv 0 \pmod p$. Then $p \equiv (\frac{P^2-4Q}{p}) \pmod{2^{n+(3+(\frac{Q}{p}))/2}}$.*

Proof: In view of Lemma 2.2 we have $p \mid V_{2^n}(P,Q)$ and so $p \mid U_{2^{n+1}}(P,Q)$ by (2.4). From (2.4) we see that $p \not| U_{2^n}(P,Q)$. Thus, $r_p(P,Q) = 2^{n+1}$. This together with Lemma 2.1 gives the result.

Lemma 2.4: *Let $P, Q \in \mathbb{Z}$ and $n \in \mathbb{N}$, and let $p > 1$ be an odd integer such that $(p, Q(P^2 - 4Q)) = 1$ and $S_n(P/\sqrt{Q}) \equiv 0 \pmod p$. Let $\alpha = n+2$ or $n+1$ according as Q is a square or not. If $p < (2^\alpha - 1)^2$, then p is prime.*

Proof: If p is composite, then p has a prime divisor q such that $q \leq \sqrt{p}$. Since $q \mid p$ and $S_n(P/\sqrt{Q}) \equiv 0 \pmod p$ we see that $S_n(P/\sqrt{Q}) \equiv 0 \pmod q$. It follows from Lemma 2.3 that $q \equiv (\frac{P^2-4Q}{q}) \pmod{2^{n+(3+(\frac{Q}{q}))/2}}$ and so $q \geq 2^{n+(3+(\frac{Q}{q}))/2} - 1$. Thus, $p \geq q^2 \geq (2^{n+(3+(\frac{Q}{q}))/2} - 1)^2$. This contradicts the assumption. So p must be prime.

Let $[x]$ denote the greatest integer not exceeding x. Using induction one can easily prove

Lemma 2.5 ([9, (4.2.36)]): *Let $P, Q \in \mathbb{Z}$ and $n \in \mathbb{N}$. Then*

$$V_n(P,Q) = \sum_{r=0}^{[n/2]} \frac{n}{n-r} \binom{n-r}{r} P^{n-2r}(-Q)^r.$$

3. THE GENERAL PRIMALITY TEST FOR NUMBERS OF THE FORM $k \cdot 2^m \pm 1$

Lemma 3.1: *Let $P, Q \in \mathbb{Z}$ and $D = P^2 - 4Q$. Let p be an odd prime such that $p \not| QD$. Suppose $(\frac{Q}{p}) = 1$ and so $c^2 \equiv Q \pmod p$ for some integer c. Then*

(i) $V_{\frac{p-(\frac{D}{p})}{2}}(P,Q) \equiv 2\left(\frac{P+2c}{p}\right) c^{\frac{1-(\frac{D}{p})}{2}} \pmod p$,

(ii) $V_{\frac{p+(\frac{D}{p})}{2}}(P,Q) \equiv P\left(\frac{P+2c}{p}\right) c^{\frac{(\frac{D}{p})-1}{2}} \pmod p$.

Proof: For $b, c \in \mathbb{Z}$ it is clear that

$$\left(\frac{b \pm \sqrt{b^2-4bc}}{2}\right)^2 = b \cdot \frac{b-2c \pm \sqrt{(b-2c)^2-4c^2}}{2}.$$

Thus, applying (2.2) we see that

$$V_{2n}(b, bc) = b^n V_n(b-2c, c^2). \tag{3.1}$$

Hence, if p is an odd prime such that $p \not| b^2-4bc$ and $\varepsilon = (\frac{b^2-4bc}{p})$, by [9, (4.3.4)] we obtain

$$V_{\frac{p-\varepsilon}{2}}(b-2c, c^2) = b^{-\frac{p-\varepsilon}{2}} V_{p-\varepsilon}(b, bc) \equiv b^{-\frac{p-\varepsilon}{2}} \cdot 2(bc)^{\frac{1-\varepsilon}{2}} = 2b^{-\frac{p-1}{2}} c^{\frac{1-\varepsilon}{2}} \equiv 2\left(\frac{b}{p}\right) c^{\frac{1-\varepsilon}{2}} \pmod p.$$

Now suppose $b = P+2c$ and $c^2 \equiv Q \pmod p$. Then $b^2-4bc = P^2-4c^2 \equiv P^2-4Q \pmod p$ and so $\varepsilon = (\frac{D}{p})$. From the above we see that

$$V_{\frac{p-\varepsilon}{2}}(P,Q) \equiv V_{\frac{p-\varepsilon}{2}}(b-2c, c^2) \equiv 2\left(\frac{P+2c}{p}\right) c^{\frac{1-\varepsilon}{2}} \pmod p.$$

This proves (i).

¿From (2.1) and (2.2) we see that

$$V_{(p+(\frac{D}{p}))/2}(P,Q) = \frac{1}{2Q^{(1-(\frac{D}{p}))/2}} \Big\{ P V_{(p-(\frac{D}{p}))/2}(P,Q) + \left(\frac{D}{p}\right) D U_{(p-(\frac{D}{p}))/2}(P,Q) \Big\}.$$

Thus, by (i) and (2.6) we obtain

$$V_{(p+(\frac{D}{p}))/2}(P,Q) \equiv \frac{1}{2Q^{(1-(\frac{D}{p}))/2}} \cdot 2P\left(\frac{P+2c}{p}\right) c^{\frac{1-(\frac{D}{p})}{2}} \equiv P\left(\frac{P+2c}{p}\right) c^{\frac{(\frac{D}{p})-1}{2}} \pmod p.$$

This proves (ii) and hence the proof is complete.

Remark 3.1: Lemma 3.1 can also be easily deduced from [7, Lemma 3.4] or [8, Lemma 3.1].

Lemma 3.2: *Let $P, Q \in \mathbb{Z}$ and p be an odd prime with $p \not| Q(P^2 - 4Q)$. Suppose $(\frac{Q}{p}) = 1$ and so $c^2 \equiv Q \pmod p$ for some integer c. Then*

$$V_{\frac{p-(\frac{-1}{p})}{4}}(P, Q) \equiv 0 \pmod p \quad \textit{if and only if} \quad \left(\frac{2Q + cP}{p}\right) = \left(\frac{2Q - cP}{p}\right) = -1.$$

Proof: From Lemma 3.1 we have

$$V_{\frac{p-(\frac{-1}{p})}{2}}(P, Q) \equiv \begin{cases} 2\left(\frac{P+2c}{p}\right) c^{\frac{1-(\frac{-1}{p})}{2}} \pmod p & \text{if } \left(\frac{4Q-P^2}{p}\right) = 1, \\ P\left(\frac{P+2c}{p}\right) c^{-\frac{1+(\frac{-1}{p})}{2}} \pmod p & \text{if } \left(\frac{4Q-P^2}{p}\right) = -1. \end{cases}$$

Thus, applying (2.4) we obtain

$$V^2_{\frac{p-(\frac{-1}{p})}{4}}(P, Q) = V_{\frac{p-(\frac{-1}{p})}{2}}(P, Q) + 2Q^{\frac{p-(\frac{-1}{p})}{4}} \equiv V_{\frac{p-(\frac{-1}{p})}{2}}(P, Q) + 2c^{\frac{1-(\frac{-1}{p})}{2}} \left(\frac{c}{p}\right)$$

$$\equiv \begin{cases} 2c^{\frac{1-(\frac{-1}{p})}{2}} \left\{\left(\frac{P+2c}{p}\right) + \left(\frac{c}{p}\right)\right\} \pmod p & \text{if } \left(\frac{4Q-P^2}{p}\right) = 1, \\ c^{-\frac{1+(\frac{-1}{p})}{2}} \left\{P\left(\frac{P+2c}{p}\right) + 2c\left(\frac{c}{p}\right)\right\} \pmod p & \text{if } \left(\frac{4Q-P^2}{p}\right) = -1. \end{cases}$$

Since $p \not| P^2 - 4Q$ and $c^2 \equiv Q \pmod p$ we see that $P(\frac{P+2c}{p}) \not\equiv -2c(\frac{c}{p}) \pmod p$. Hence,

$$p \,\Big|\, V_{\frac{p-(\frac{-1}{p})}{4}}(P, Q) \iff \left(\frac{4Q - P^2}{p}\right) = 1 \quad \text{and} \quad \left(\frac{P + 2c}{p}\right) = -\left(\frac{c}{p}\right)$$

$$\iff \left(\frac{2Q + cP}{p}\right) = \left(\frac{2Q - cP}{p}\right) = -1.$$

This proves the lemma.

Lemma 3.3: *Suppose $P, Q, k, n \in \mathbb{Z}$ with $k, n \geq 0$. Then*

$$V_{kn}(P, Q) = V_n(V_k(P, Q), Q^k).$$

Proof: Set $V_m = V_m(P, Q)$. From [9, (4.2.8)] we know that

$$V_{r+k} = V_k V_r - Q^k V_{r-k} \quad \text{and so} \quad V_{k(m+1)} = V_k V_{km} - Q^k V_{k(m-1)}.$$

Now we prove the result by induction on n. Clearly the result is true for $n = 0, 1$. Suppose the result holds for $1 \leq n \leq m$. By the above and the inductive hypothesis we have

$$V_{k(m+1)} = V_k V_m(V_k, Q^k) - Q^k V_{m-1}(V_k, Q^k) = V_{m+1}(V_k, Q^k).$$

So the result holds for $n = m + 1$. Hence, the lemma is proved by induction.

Theorem 3.1: *For* $m \in \{2, 3, 4, \dots\}$ *let* $p = k \cdot 2^m \pm 1$ *with* $0 < k < 2^m$ *and* k *odd. If* $b, c \in \mathbb{Z}$, $(p, c) = 1$ *and* $(\frac{2c+b}{p}) = (\frac{2c-b}{p}) = -(\frac{c}{p})$, *then* p *is prime if and only if* $p \mid S_{m-2}(x)$, *where* $x = c^{-k} V_k(b, c^2) = \sum_{r=0}^{(k-1)/2} \frac{k}{k-r} \binom{k-r}{r} (-1)^r (b/c)^{k-2r}$.

Proof: Set $U_n = U_n(b, c^2)$ and $V_n = V_n(b, c^2)$. From Lemmas 3.3, 2.2 and 2.5 we have

$$V_{(p-(\frac{-1}{p}))/4} = V_{k \cdot 2^{m-2}} = V_{2^{m-2}}(V_k, c^{2k}) = c^{k \cdot 2^{m-2}} S_{m-2}(V_k/c^k) = c^{k \cdot 2^{m-2}} S_{m-2}(x).$$

If p is prime, it follows from Lemma 3.2 that $p \mid V_{(p-(\frac{-1}{p}))/4}$. So $S_{m-2}(x) \equiv 0 \pmod p$.

Now suppose $S_{m-2}(x) = S_{m-2}(V_k/c^k) \equiv 0 \pmod p$. From (2.4) we have $V_n^2 - (b^2 - 4c^2)U_n^2 = 4c^{2n}$. Thus, $(U_n, V_n) \mid 4c^{2n}$. As $(p, 2c) = 1$ and $p \mid V_{k \cdot 2^{m-2}}$ we find $(p, U_{k \cdot 2^{m-2}}) = 1$. It is well known that (see [5] and [9]) $U_r \mid U_{rn}$ for any positive integers r and n. Thus, $U_k \mid U_{k \cdot 2^{m-2}}$ and so $(p, U_k) = 1$. Hence, $(p, V_k^2 - 4c^{2k}) = 1$ by (2.4). Set $P = V_k, Q = c^{2k}$ and $n = m - 2$. If $0 < k < 2^m - 2$, then clearly $p = k \cdot 2^m \pm 1 < (2^m - 1)^2$. By Lemma 2.4, p is prime. If $p = (2^m - 1)2^m \pm 1$ is composite, by Lemma 2.3 we know that any prime divisor q of p satisfying $q \equiv \pm 1 \pmod{2^m}$. It is easy to check that $p \neq (2^m \pm 1)^2$. Thus $p \geq (2^m - 1)(2^m + 1)$. This is impossible. So p is prime. This completes the proof.

Taking $b = 4$ and $c = 1$ in Theorem 3.1 we obtain the Lucas-Lehmer test for Mersenne primes and Theorem 1.2.

¿From Theorem 3.1 we also have the following criterion for Fermat primes, which is similar to the Lucas-Lehmer test.

Corollary 3.1: *For* $n \in \mathbb{N}$ *the Fermat number* F_n *is prime if and only if* $F_n \mid S_{2^n-2}(5)$.

Proof: Since $F_n \equiv 2 \pmod 3$ and $F_n \equiv 3, 5 \pmod 7$ we see that

$$\left(\frac{-3}{F_n}\right) = \left(\frac{F_n}{3}\right) = -1 \quad \text{and} \quad \left(\frac{7}{F_n}\right) = \left(\frac{F_n}{7}\right) = -1.$$

Thus putting $p = F_n$, $k = 1$, $b = 5$ and $c = 1$ in Theorem 3.1 we obtain the result.

Remark 3.2: In 1960 K. Inkeri[3] showed that the Fermat number F_n $(n \geq 2)$ is prime if and only if $F_n \mid S_{2^n-2}(8)$.

4. THE PRIMALITY CRITERION FOR NUMBERS OF THE FORM $9 \cdot 2^m \pm 1$

In the section we use Theorem 3.1 to obtain explicit primality criterion for numbers of the form $9 \cdot 2^m \pm 1$.

Theorem 4.1: *Let* $m \geq 3$ *be a positive integer. If* $m \equiv 0 \pmod 2$ *or* $m \equiv 5, 11 \pmod{12}$, *then* $9 \cdot 2^m - 1$ *is composite. If* $m \equiv 1, 3, 7, 9 \pmod{12}$, *then* $9 \cdot 2^m - 1$ *is prime if and only if* $9 \cdot 2^m - 1 \mid S_{m-2}(x)$, *where*

$$x = \begin{cases} 5778 & \text{if } m \equiv 1, 9 \pmod{12}, \\ 1330670 & \text{if } m \equiv 3 \pmod{12}, \\ 2186871698 & \text{if } m \equiv 7 \pmod{12}. \end{cases}$$

Proof: Clearly the result is true for $m = 3$. Now assume $m \geq 4$. If $m = 2n$ for some integer n, then $9 \cdot 2^m - 1 = (3 \cdot 2^n + 1)(3 \cdot 2^n - 1)$ and so $9 \cdot 2^m - 1$ is composite. If $m \equiv 5, 11 \pmod{12}$, then $7 \mid 9 \cdot 2^m - 1$ since $2^3 \equiv 1 \pmod 7$. If $m \equiv 1, 3, 7, 9 \pmod{12}$, once setting

$$b = \begin{cases} 3 & \text{if } m \equiv 1, 9 \pmod{12}, \\ 5 & \text{if } m \equiv 3 \pmod{12}, \\ 11 & \text{if } m \equiv 7 \pmod{12} \end{cases}$$

one can easily check that

$$\left(\frac{2+b}{9 \cdot 2^m - 1}\right) = \left(\frac{2-b}{9 \cdot 2^m - 1}\right) = -1.$$

From Lemma 2.5 we know that

$$V_9(b, 1) = b^9 - 9b^7 + 27b^5 - 30b^3 + 9b = (b^3 - 3b)((b^3 - 3b)^2 - 3) = x.$$

Applying Theorem 3.1 in the case $c = 1$ we get the result.

In a similar way, applying Theorem 3.1 we have

Theorem 4.2: *Let $m \geq 3$ be a positive integer. If $m \equiv 0 \pmod 4$, then $5 \mid 9 \cdot 2^m + 1$. If $m \equiv 10 \pmod{12}$, then $13 \mid 9 \cdot 2^m + 1$. If $m \equiv 5 \pmod 8$, then $17 \mid 9 \cdot 2^m + 1$. If $m \not\equiv 0 \pmod 4$, $m \not\equiv 10 \pmod{12}$ and $m \not\equiv 5 \pmod 8$, then $9 \cdot 2^m + 1$ is prime if and only if $9 \cdot 2^m + 1 \mid S_{m-2}(x)$, where x is given by Table* 4.1.

m	b	$x = V_9(b,1) = (b^3 - 3b)((b^3 - 3b)^2 - 3)$
$m \equiv 1, 9 \pmod{24}$	37	$50542 \cdot 2554493761$
$m \equiv 2 \pmod{12}$	28	$21868 \cdot 478209421$
$m \equiv 3, 6, 7 \pmod{12}$	12	$1692 \cdot 2862861$
$m \equiv 11 \pmod{12}$	32	$32672 \cdot 1067459581$
$m \equiv 17, 65 \pmod{72}$	150	$3374550 \cdot (3374550^2 - 3)$
$m \equiv 41 \pmod{72}$	2167	$(2167^3 - 6501) \cdot ((2167^3 - 6501)^2 - 3)$

Table 4.1

Remark 4.1: For $m \geq 4$ let $p = 9 \cdot 2^m + 1$ and

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

In [2] W. Bosma showed that p is prime if and only if $D^{(p-1)/2} \equiv -1 \pmod p$.

Theorem 4.3: *Let n be a positive integer. Then $9 \cdot 2^{4n+3} - 1$ and $9 \cdot 2^{4n+3} + 1$ are twin primes if and only if $(9 \cdot 2^{4n+3})^2 - 1 \mid S_{4n+1}(32672 \cdot 1067459581)$.*

Proof: Let $b = 32$. Then $2 + b = 2 \cdot 17$ and $2 - b = -2 \cdot 3 \cdot 5$. Since $\left(\frac{2}{9 \cdot 2^{4n+3} \pm 1}\right) = \left(\frac{3}{9 \cdot 2^{4n+3} \pm 1}\right) = 1$ and $2^4 \equiv -1 \pmod{17}$ we find

$$\left(\frac{2+b}{9 \cdot 2^{4n+3} \pm 1}\right) = \left(\frac{17}{9 \cdot 2^{4n+3} \pm 1}\right) = \left(\frac{9 \cdot 2^{4n+3} \pm 1}{17}\right) = \left(\frac{4(-1)^n \pm 1}{17}\right) = -1,$$

$$\left(\frac{2-b}{9 \cdot 2^{4n+3} \pm 1}\right) = \left(\frac{-5}{9 \cdot 2^{4n+3} \pm 1}\right) = \pm\left(\frac{9 \cdot 2^{4n+3} \pm 1}{5}\right) = \pm\left(\frac{72 \pm 1}{5}\right) = -1.$$

Thus, applying Theorem 3.1 we see that $9 \cdot 2^{4n+3} \pm 1$ is prime if and only if $9 \cdot 2^{4n+3} \pm 1 \mid S_{4n+1}(V_9(b,1))$. To see the result, we note that $(9 \cdot 2^{4n+3} + 1, 9 \cdot 2^{4n+3} - 1) = 1$ and that

$$V_9(b,1) = b^9 - 9b^7 + 27b^5 - 30b^3 + 9b = (b^3 - 3b)((b^3 - 3b)^2 - 3) = 32672 \cdot 1067459581.$$

Remark 4.2: If $9 \cdot 2^m \pm 1 (m > 1)$ are twin primes, then $m \equiv 3 \pmod 4$. If $m \equiv 11 \pmod{12}$, then $7 \mid 9 \cdot 2^m - 1$ and so $9 \cdot 2^m \pm 1$ cannot be twin primes. If $m \equiv 3 \pmod{12}$, by taking $b = 12$ and $c = 1$ in Theorem 3.1 we can prove that $9 \cdot 2^m - 1$ and $9 \cdot 2^m + 1$ are twin primes if and only if $(9 \cdot 2^m)^2 - 1 \mid S_{m-2}(4843960812)$. It is known that $9 \cdot 2^m - 1$ and $9 \cdot 2^m + 1$ are twin primes when $m = 1, 3, 7, 43, 63, 211$. Do there exist only finitely many such twin primes?

5. THE PRIMALITY CRITERION FOR NUMBERS OF THE FORM $3 \cdot 2^m \pm 1$

Theorem 5.1: *Let $m \geq 3$ be a positive integer such that $m \not\equiv -2 \pmod{10080}$. If $m \equiv 1 \pmod 4$, $m \equiv 46 \pmod{72}$ or $m \equiv 862 \pmod{1440}$, then $3 \cdot 2^m - 1$ is composite. If $m \not\equiv 1 \pmod 4$, $m \not\equiv 46 \pmod{72}$ and $m \not\equiv 862 \pmod{1440}$, then $3 \cdot 2^m - 1$ is prime if and only if $3 \cdot 2^m - 1 \mid S_{m-2}(x)$, where x is given by Table 5.1.*

m	b	$x = V_3(b,1) = b^3 - 3b$
$m \equiv 0, 3 \pmod 4$	3	18
$m \equiv 2, 6 \pmod{12}$	5	110
$m \equiv 10p \pmod{24}$	15	3330
$m \equiv 22 \pmod{72}$	17	4862
$m \equiv 70 \pmod{144}$	192	7077312
$m \equiv 142 \pmod{288}$	65535	$65535^3 - 3 \cdot 65535$
$m \equiv 286, 574 \pmod{1440}$	9	702
$m \equiv 1150 \pmod{1440}$	29	24302
$m \equiv 1438, 2878, 4318, 7198 \pmod{10080}$	27	19602
$m \equiv 5758 \pmod{10080}$	41	68798
$m \equiv 8638 \pmod{10080}$	125	1952750

Table 5.1

Proof: If $m \equiv 1 \pmod 4$, then $5 \mid 3 \cdot 2^m - 1$; if $m \equiv 46 \pmod{72}$, then $37 \mid 3 \cdot 2^m - 1$; if $m \equiv 862 \pmod{1440}$, then $11 \mid 3 \cdot 2^m - 1$. Now suppose $m \not\equiv 1 \pmod 4$, $m \not\equiv 46 \pmod{72}$ and $m \not\equiv 862 \pmod{1440}$. Let b be given by Table 5.1. One can easily check that

$$\left(\frac{2+b}{3 \cdot 2^m - 1}\right) = \left(\frac{2-b}{3 \cdot 2^m - 1}\right) = -1.$$

Thus the result follows from Theorem 3.1 by taking $c = 1$ and $p = 3 \cdot 2^m - 1$.

Remark 5.1: If $m \in \mathbb{N}$ and $m \equiv 0, 2 \pmod 3$, in 1993 W. Bosma[2] showed that $3 \cdot 2^m - 1$ is prime if and only if $3 \cdot 2^m - 1 \mid S_{m-2}(10054 \cdot 2^{3m})$.

In a similar way, using Theorem 3.1 we can prove

Theorem 5.2: *Let $m \geq 3$ be a positive integer such that $180 \not| m$. If $m \equiv 1 \pmod 3$, then $7 \mid 3 \cdot 2^m + 1$; if $m \equiv 3 \pmod 4$, then $5 \mid 3 \cdot 2^m + 1$; if $m \equiv 2 \pmod{12}$, then $13 \mid 3 \cdot 2^m + 1$; if $m \equiv 144 \pmod{180}$, then $61 \mid 3 \cdot 2^m + 1$. If $m \not\equiv 1 \pmod 3$, $m \not\equiv 3 \pmod 4$, $m \not\equiv 2 \pmod{12}$ and $m \not\equiv 144 \pmod{180}$, then $3 \cdot 2^m + 1$ is prime if and only if $3 \cdot 2^m + 1 \mid S_{m-2}(x)$, where x is given by Table 5.2.*

m	b	$x = V_3(b,1) = b^3 - 3b$
$m \equiv 5 \pmod{12}$	12	1692
$m \equiv 6 \pmod{12}$	28	21868
$m \equiv 8 \pmod{12}$	37	50542
$m \equiv 9 \pmod{12}$	32	32672
$m \equiv 12, 24 \pmod{36}$	150	3374550
$m \equiv 36 \pmod{180}$	207	8869122
$m \equiv 72 \pmod{180}$	64	261952
$m \equiv 108 \pmod{180}$	5282	$5282 \cdot 27899521$

Table 5.2

Theorem 5.3: *Let n be a nonnegative integer. Then $3 \cdot 2^{20n+6} - 1$ and $3 \cdot 2^{20n+6} + 1$ are twin primes if and only if $(3 \cdot 2^{20n+6})^2 - 1 \mid S_{20n+4}(73962)$.*

Proof: Let $b = 42$. Then $2 + b = 44$ and $2 - b = -40$. Since $(\frac{2}{3 \cdot 2^{20n+6} \pm 1}) = 1$, and $2^5 \equiv -1 \pmod{11}$ we find

$$\left(\frac{2+b}{3 \cdot 2^{20n+6} \pm 1}\right) = \left(\frac{11}{3 \cdot 2^{20n+6} \pm 1}\right) = \pm\left(\frac{3 \cdot 2^{20n+6} \pm 1}{11}\right) = \pm\left(\frac{-6 \pm 1}{11}\right) = -1,$$

$$\left(\frac{2-b}{3 \cdot 2^{20n+6} \pm 1}\right) = \pm\left(\frac{5}{3 \cdot 2^{20n+6} \pm 1}\right) = \pm\left(\frac{3 \cdot 2^{20n+6} \pm 1}{5}\right) = \pm\left(\frac{12 \pm 1}{5}\right) = -1.$$

Thus, applying Theorem 3.1 in the case $b = 42$ and $c = 1$ we see that $3 \cdot 2^{20n+6} \pm 1$ is prime if and only if $3 \cdot 2^{20n+6} \pm 1 \mid S_{20n+4}(V_3(b,1))$. To see the result, we note that $(3 \cdot 2^{20n+6} + 1, 3 \cdot 2^{20n+6} - 1) = 1$ and that $V_3(b,1) = b^3 - 3b = 42^3 - 3 \cdot 42 = 73962$.

In the same way, putting $b = 17$ and $c = 1$ in Theorem 3.1 we get

Theorem 5.4: *Let n be a nonnegative integer. Then $3 \cdot 2^{36n+6} - 1$ and $3 \cdot 2^{36n+6} + 1$ are twin primes if and only if $(3 \cdot 2^{36n+6})^2 - 1 \mid S_{36n+4}(4862)$.*

REFERENCES

[1] W. Borho. "Grosse Primzahlen und befreundete Zahlen: *ü*ber den Lucas-test und Thabit Regeln." *Mitt. Math. Ges. Hamburg* (1983): 232-256.
[2] W. Bosma. "Explicit Primality Criteria for $h \cdot 2^k \pm 1$." *Math. Comp.* **61** (1993): 97-109, MR94c:11005.
[3] K. Inkeri. "Tests for Primality." *Ann. Acad. Sci. Fenn.* (Ser. A) **1** (1960): 1-19, MR22#7984.
[4] D. H. Lehmer. "An Extended Theory of Lucas' Functions." *Ann. Math.* **31** (1930): 419-448.
[5] P. Ribenboim. *The Book of Prime Number Records*, 2nd ed., Springer, Berlin, 1989, 44-50.
[6] H. Riesel. "Lucasian Criteria for the Primality of $N = h \cdot 2^n - 1$." *Math. Comp.* **23** (1969): 869-875.
[7] Z.-H. Sun. "Combinatorial Sum $\sum_{k \equiv r \pmod{m}} \binom{n}{k}$ and Its Applications in Number Theory III." *J. Nanjing Univ. Math. Biquarterly* **12** (1995): 90-102, MR96g:11017.
[8] Z.-H. Sun. "Values of Lucas Sequences Modulo Primes." *Rocky Moun. J. Math.* **33** (2003): 1123-1145.
[9] H.C. Williams. *Édouard Lucas and Primality Testing, Canadian Mathematical Society Series of Monographs and Advanced Texts*, Vol. 22, Wiley, New York, 1998, 74-92.

AMS Classification Numbers: 11Y11, 11B39, 11B50

✠ ✠ ✠