

CHEBYSHEV POLYNOMIALS AND HIGHER ORDER LUCAS LEHMER ALGORITHM

KOK SENG CHUA

ABSTRACT. We extend the necessity part of Lucas Lehmer iteration for testing Mersenne prime to all base and uniformly for both generalized Mersenne and Wagstaff numbers (the later correspond to negative base). The role of the quadratic iteration $x \rightarrow x^2 - 2$ is extended by Chebyshev polynomial $T_n(x)$ with an implied iteration algorithm because of the compositional identity $T_n(T_m(x)) = T_{nm}(x)$. This results from a Chebyshev polynomial primality test based essentially on the Lucas pair $(\omega_a, \bar{\omega}_a)$, $\omega_a = a + \sqrt{a^2 - 1}$, where $a \neq 0 \pm 1$. It seems interesting that the arithmetic are all coded in the Chebyshev polynomials $T_n(x)$.

1. MAIN RESULTS AND PROOF

The Chebyshev polynomial of the first kind, which is explicitly defined [8] for $|x| \geq 1$, by

$$T_n(x) = \frac{(x + \sqrt{x^2 - 1})^n + (x - \sqrt{x^2 - 1})^n}{2} = \frac{\omega^n + \bar{\omega}^n}{2},$$

where $\omega_x := x + \sqrt{x^2 - 1}$, has a natural extension to negative value of n , with $T_{-n}(x) = T_n(x)$ since $\omega\bar{\omega} = 1$ and this is in agreement with its hyperbolic (since we are interested in $|x| \geq 1$) characterization $T_n(\cosh \theta) = \cosh(n\theta)$ or equivalently $T_n(a) = \cosh(n \log(\omega_a))$. It also says that $T_n(a)$ is just (half) the trace of the n th power of the unit ω_a in $\mathbb{Q}(\sqrt{a^2 - 1})$.

Lucas-Lehmer [2] states that if p is an odd prime, and if we let

$$(1.1) \quad s_0 = 4, \quad s_{n+1} = s_n^2 - 2,$$

then $M_p = 2^p - 1$ is prime if and only if M_p divides s_{p-2} . The iteration map $x \rightarrow x^2 - 2$ is essentially the Chebyshev polynomial $T_2(x) = 2x^2 - 1$. If we let $s_n = 2T_{2^n}(2)$, then s_n satisfies the recurrence (1.1) because of the very special compositional identity $T_m(T_n(x)) = T_{mn}(x)$ so that $T_{2^n}(x) = T_2^n(x)$ where the power n on the right means iterated composition n times.

But there is no reason for the base 2 to be special for Chebyshev and the implied algorithm $T_{q^n}(a) = T_q^n(a)$ lead us to look at the residues $T_q^n(a) \pmod{q^n - 1}$. In this note we extend the necessity part of Lucas-Lehmer to all base $q \neq 0, \pm 1$ and all starting values $a \neq 0, \pm 1$ where the quadratic iteration (1.1) is replaced by the order q Chebyshev map $x \rightarrow T_q(x)$. In addition, an unexpected surprise is that we can also allow negative q which actually means testing for Wagstaff primes by the same algorithm. Let $\Phi_p(x) = \frac{x^p - 1}{x - 1}$ be the p th cyclotomic polynomial. Note $\Phi_p(q) = \frac{q^p - 1}{q - 1}$ and $\Phi_p(-q) = \frac{q^p + 1}{q + 1}$ are the generalized Mersenne and Wagstaff

2000 *Mathematics Subject Classification.* Primary : 11A51, Secondary : 11A15.

Key words and phrases. Lucas-Lehmer, Chebyshev, Primality.

numbers. Let $U_n(x)$ be the Chebyshev polynomials of the second kind. We note that $U_{-n}(x) = -U_{n-2}(x)$ and $U_n(x) = \frac{\omega^{n+1} - \bar{\omega}^{n+1}}{\omega - \bar{\omega}}$.

Theorem 1.1. *Let q, a be integers both not $0, \pm 1$ and p be an odd prime and let $\epsilon = \left(\frac{a^2-1}{\Phi_p(q)}\right)$, if $\Phi_p(q)$ is a prime not dividing $a^2 - 1$, then*

$$(1.2) \quad T_{q^\epsilon}(a) = T_{q+\epsilon-1}(a), \quad U_{q^{p-\epsilon(q-1)-2}}(a) = 0 \pmod{\Phi_p(q)}.$$

Remark 1.2. This works also for $-q$, for example for $q = -2, a = 2, \epsilon = \left(\frac{2}{3}\right)$, it says $N_p = (2^p + 1)/3$ prime implies $T_{2^p}(2) = T_{3-\left(\frac{2}{3}\right)}(2) \pmod{N_p}$, which in term of (1.1) is equivalent to N_p divides $s_p - 104 - 90\left(\frac{2}{3}\right)$. This is a weakened form and we can derive a stronger version later, namely N_p divides $s_{p-1} - 5 - 9\left(\frac{2}{3}\right)$. Note also we only need to code one program which will work for both $\pm q$ provided $T_{-n}(x)$ and $U_{-n}(x)$ are implemented as $T_n(x), -U_{n-2}(x)$ as was the case with PARI-GP which we used.

Remark 1.3. One can compute $T_{q^p}(a)$ efficiently as $T_q^p(a)$ but $U_n(x)$ does not satisfies the compositional identity and in general they don't commute, $U_n(U_m(x)) \neq U_m(U_n(x))$. For large n of no special form, U_n and also T_n can be computed in $O(\log n)$ steps by the usual method of writing a linear recurrence as a matrix power and applied the binary exponentiation as was observed in [3]. We give the formula to compute $T_{n+1}(a), U_n(a) \pmod{Q}$ together via a coupled recurrence, which follows from $\omega^{n+1} = \omega^n \omega$ and (2.2) below,

$$(1.3) \quad \begin{pmatrix} T_{n+1}(a) \\ U_n(a) \end{pmatrix} = \begin{pmatrix} a & a^2 - 1 \\ 1 & a \end{pmatrix}^n \begin{pmatrix} a \\ 1 \end{pmatrix} \pmod{Q}.$$

If $n = q^p \pm \delta$ for small δ , one should use q -nary expansion of n .

Remark 1.4. One can express (1.2) in a simple Lucas-Lehmer form similar to (1.1), let

$$s_0 = a, \quad s_{n+1} = T_q(s_n),$$

if $\Phi_p(q)$ is prime, it divides $s_p - 2T_{q+\left(\frac{a^2-1}{\Phi_p(q)}\right)-1}(a)$. This is weaker than what is provable but have a simple uniform form. Sufficiency actually failed in this weak form for some small p for some choices of a . eg.

$$q = 11, p = 3, a = 2, M_{11} = (11^3 - 1)/10 = 133 = 7.19$$

$$q = -5, p = 3, a = 3, N = (5^3 + 1)/6 = 21 = 3.7$$

but this can be ruled out if we choose other starting point eg. use $a = q$. They also failed the stronger Chebyshev test.

Remark 1.5. Theorem (1.1) can be "seen" visually if we compute a list of values of $T_{q^p}(a) \pmod{\Phi_p(q)}$ for primes p up to say 200. There is clearly a dip in the number of digits of the residues when $\Phi_p(q)$ is prime, and this is how we first saw them.

Theorem 1 follows immediately from the following lemma.

Lemma 1.6. *Let Q be an odd prime and $a \neq 0, \pm 1$, $\omega = a + \sqrt{a^2 - 1}$, as before, and let $\epsilon = \left(\frac{a^2-1}{Q}\right), \delta = \left(\frac{2(a+1)}{Q}\right)$, then*

$$(1.4) \quad \omega^{\frac{Q-\epsilon}{2}} = \delta \pmod{Q},$$

or equivalently,

$$(1.5) \quad T_{\frac{Q-\epsilon}{2}}(a) = \delta, \quad U_{\frac{Q-\epsilon}{2}-1}(a) = 0 \pmod{Q},$$

and this implies

$$T_{\frac{Q-\epsilon}{2}}(a) = \delta \pmod{Q^2}.$$

Proof. We have computing mod Q ,

$$(a - 1 + \sqrt{a^2 - 1})^Q = a - 1 + \epsilon \sqrt{a^2 - 1}.$$

Multiplying by $(a - 1 - \epsilon \sqrt{a^2 - 1})$ gives

$$(2 - 2a)^{(1-\epsilon)/2} = (a - 1 + \sqrt{a^2 - 1})^{(Q-\epsilon)},$$

and using $(a - 1 + \sqrt{a^2 - 1})^2 = 2(a - 1)\omega$ gives us, (note $(-1)^{\frac{1-\epsilon}{2}} = \epsilon$)

$$\omega^{\frac{Q-\epsilon}{2}} = \left(\frac{2(a+1)}{Q} \right) \pmod{Q}.$$

But we have (without mod Q)

$$\omega^{\frac{Q-\epsilon}{2}} = T_{\frac{Q-\epsilon}{2}}(a) + U_{\frac{Q-\epsilon}{2}-1}(a)\sqrt{a^2 - 1},$$

by (2.2) below, which give the equivalent (1.5). \square

Remark 1.7. Writing $n = \frac{Q-\epsilon}{2}$, since ω is a unit, so is ω^n , we must have the Pell's equation $\omega^n \bar{\omega}^n = T_n(a)^2 - (a^2 - 1)U_{n-1}(a)^2 = 1$. So we have Q^2 divides $T_n(a)^2 - 1 = (T_n(a) - \delta)(T_n(a) + \delta)$. Since Q divides $T_n(a) - \delta$, its prime divisor cannot divide $T_n(a) + \delta$, so we always have $T_n(a) = \delta \pmod{Q^2}$.

Proof. (Proof of theorem) Specialize to $Q = \Phi_p(q) = \frac{q^p-1}{q-1}$ (q may be negative) in (1.4) gives

$$\omega^{\frac{q^p-1-\epsilon(q-1)}{2(q-1)}} = \delta,$$

and raising to the $2(q-1)$ power (this lose information) gives $\omega^{q^p-1-\epsilon(q-1)} = 1$, which is the same as

$$T_{q^p}(a) = T_{\epsilon(q-1)+1}(a) = T_{q+\epsilon-1}(a), \quad U_{q^p-\epsilon(q-1)-2}(a) = 0 \pmod{Q}.$$

\square

Remark 1.8. Using (1.4), one can find similar divisibility criteria of the same sequence for many class of primes, eg $q = \pm 2$, $a = 2$ and s_n the usual Lucas-Lehmer sequence (1.1), we have

$M_p = 2^p - 1$ prime implies M_p divides s_{p-2} .

$N_p = (2^p + 1)/3$ prime implies N_p divides $s_{p-1} - 5 - 9\left(\frac{p}{3}\right)$

$n > 2$, $M_n = 3 \cdot 2^n - 1$, prime implies M_n divides $(s_{n-1}^3 - 3s_{n-1} - 4)$

$n > 2$, $N_n = 3 \cdot 2^n + 1$, prime implies N_n divides $(s_{n-1} + 1)(s_{n-1} - 2)$, etc...

The last two follows from setting $a = 2$, $T_{3 \cdot 2^{n-1}}(2) = T_1(2)$ and $T_{3 \cdot 2^{n-1}}(2) = 1$.

Remark 1.9. For a cubic example, let $q = \pm 3$, $a = 2$, and $s_0 = 2$, $s_{n+1} = s_n(4s_n^2 - 3)$, then $M_p = (3^p - 1)/2$ prime implies it divides $s_p - 26$ and $N_p = (3^p + 1)/4$ prime implies it divides $s_p - 194 + (-1)^{(p-1)/2}168$.

2. CHEBYSHEV PRIMALITY TEST

If Q is a prime and a an integer with $\gcd(a^2 - 1, Q) = 1$, by (1.5), we have

$$(2.1) \quad T_{\frac{Q-\epsilon}{2}}(a) = \left(\frac{2(a+1)}{Q} \right), \quad U_{\frac{Q-\epsilon}{2}-1}(a) = 0 \pmod{Q}.$$

Clearly all odd primes Q pass this test to every base a . We shall call an odd non-prime integer Q , with $\gcd(Q, a^2 - 1) = 1$, which pass this test a Chebyshev pseudoprime to the base a . It depends only on $a \pmod{Q}$ but there is no subgroup structure. Chebyshev pseudoprimes are always squarefree except for some prime squared. They are rare and seems rarer than Fermat pseudoprimes. There are only seven of them to the base 2 upto 20000,

$$23.43, \quad 37.73, \quad 103^2, \quad 61.181, \quad 5.7.443, \quad 97.193, \quad 31.607.$$

Is there a Chebyshev pseudoprime to every base mod Q ? A Sierpiński number [9] is a positive odd integer k such that $N_n = k2^n + 1$ is composite for every $n \geq 1$. $k_0 = 78557$ is the smallest known Sierpiński number, because every $N_n = k_02^n + 1$ is divisible by one of $\{3, 5, 7, 13, 19, 37, 73\}$. It may be possible that N_n fail a Chebyshev test for every n for some a . Since $N_n \equiv 1 \pmod{8}$ for $n \geq 3$. We get $\epsilon = \delta = 1$ if we pick $a = 3$. So if $s_0 = 3, s_{k+1} = 2s_k^2 - 1$, and $N_n^2 = (k2^n + 1)^2$ does not divide $T_k(s_{n-1}) - 1$ for every $n \geq 3$, then k is Sierpiński. Note $N_{n+1} = 2N_n - 1$. It is open if any of the following five numbers 21181, 22699, 24737, 55459, 67607 is Sierpiński.

A Chebyshev pseudoprime for the base a is also a weak Chebyshev pseudoprime as defined in [7] ie. $T_Q(a) = a \pmod{Q}$ since the condition on U means $\omega^{Q-\epsilon} = 1$ or $\omega^Q = \omega^\epsilon$ and taking trace gives $T_Q(a) = T_1(a) = a \pmod{Q}$. There are composites which pass the weak test for all base a OEIS A175530, but all of them fail the strong Chebyshev test for all base from 2 to 10.

A square-free Q which pass the T test will also pass the U test. [Proof: We have $T_{Q-\epsilon}(a) = 1$ so that $(\omega^{(Q-\epsilon)/2} - \bar{\omega}^{(Q-\epsilon)/2})^2 = 0$ and squarefreeness of Q implies $U_{(Q-\epsilon)/2-1}(a) = 0$.] There are many non square-free integers which pass the T test but the only non squarefree integer which can pass both tests are square of prime (Proof?). So the second part only serve to rule out non squarefree integer and this is relevant since there is no known efficient algorithm to detect squarefreeness. However we can always rule out perfect square as input

If $(Q-\epsilon)/2 = 2^t Q_1$ is even, we can look at the profile $[T_{Q_1}(a), T_{2Q_1}(a), \dots, T_{(Q-\epsilon)/2}(a)]$ as in the strong pseudoprime test. Since $T_2(x) = 2x^2 - 1$, if there is a 1 not preceded by ± 1 or a -1 not preceded by 0, Q cannot be prime. For the seven pseudoprimes above, the profiles are

$$[1], [0, -1], [9083, 0, -1, 1], [0, -1, 1, 1, 1], [8416, 4431, 8861, 1], \\ [14063, 17370, 18527, 387, 1], [18791, 1301, 18720, 0, -1, 1],$$

so the strong test rule out 5.7.443 and 97.193 as primes. For square free Q , -1 is always preceded by 0, since $(\omega^m + \bar{\omega}^m)/2 = -1$ implies $(\omega^{m/2} + \bar{\omega}^{m/2})^2 = 0 \pmod{Q}$.

We note that for $a \neq 0 \pm 1$, $(\omega_a, \bar{\omega}_a)$ forms a Lucas pair in the sense of [1], since $\frac{\omega_a}{\bar{\omega}_a}$ is not a root of unity. The associated Lucas number $u_n(\omega_a, \bar{\omega}_a) = U_{n-1}(a)$. It seems to follow from [1] that for every $n > 1$, $U_n(a)$ has a primitive divisor, ie. there is a prime p which divides $U_n(a)$ but not $a(a^2 - 1)U_0(a) \dots U_{n-1}(a)$.

2.1. Multiplicative order and sufficiency test. Many of the necessity criteria seems to be sufficient in the range we can compute. It could be that when Q is composite, the residue behave randomly and the chance they give divisibility is $1/Q$ which is very small so we never see them.

Let $\omega = a + \sqrt{a^2 - 1}$ be the canonical unit. For an integer power n , we must have $\omega^n = P(a) + Q(a)\sqrt{a^2 - 1}$ for some $P(x), Q(x) \in \mathbb{Z}[x]$ but for ω , they are just Chebyshev polynomials [8], or just by induction,

$$(2.2) \quad \omega^n = T_n(a) + U_{n-1}(a)\sqrt{a^2 - 1},$$

and n may be negative. Writing $\omega^{n+1} = \omega^n \omega$ gives the recurrence formula in (1.3).

For an odd integer Q , let $O_Q(\omega)$ be the multiplicative order of $\omega_a \bmod Q$, ie. the smallest integer m such that $\omega^m = 1 \bmod Q$. This is thus the same as the smallest integer m such that $T_m(a) = 1$ and $U_{m-1}(a) = 0 \bmod Q$. Note that for a prime Q or a Chebyshev pseudoprime Q , we have $\omega_a^{Q-\epsilon} = \delta^2 = 1$ so that $O_Q(\omega_a)$ divides one of $Q \pm 1$, in particular it divides $Q^2 - 1$ and $O_Q(\omega) \leq Q + 1$.

There seems to be only one argument to prove primality of Q . One shows that ω has multiplicative order $Q \pm 1$ and hence Q cannot have any non trivial divisor, since it will have the same order in $\mathbb{F}_p[\sqrt{a^2 - 1}]$ for the smallest prime p dividing Q of size $t^2 < Q \pm 1$. We can determine the order if we know the complete factorization of $Q \pm 1$.

Lemma 2.1. *Let Q be an odd integer and $a \neq 0, \pm 1$, and assume $\left(\frac{2(a+1)}{Q}\right) = -1$.*

Let $\epsilon = \left(\frac{a^2-1}{Q}\right)$. If Q is prime, then $T_{(Q-\epsilon)/2}(a) = -1$ and $U_{(Q-\epsilon)/2-1}(a) = 0$.

Conversely if we know the complete factorization $Q - \epsilon = \prod_{j=0}^k q_j^{n_j}, j = 0, \dots, k$ where $q_0 = 2$, and we have $T_{(Q-\epsilon)/2}(a) = -1$ and $U_{(Q-\epsilon)/2-1}(a) = 0$, and also $T_{(Q-\epsilon)/q_j}(a) \neq 1$ or $U_{(Q-\epsilon)/2-1}(a) \neq 0$, for $j = 1, \dots, k$, then Q is prime.

For $Q = 2^p - 1$, and $a = 2$, we get $\omega^{2^p-1} = -1$ so that $O_Q(\omega_2) = 2^p = Q + 1$. So $2^p - 1$ is prime if and only if $O_2(\omega_2) = Q + 1$ if and only if $T_{2^p-1}(2) = -1$ and this is equivalent to $T_{2^p-2}(2) = 0 \bmod Q$. Instead of starting with $a = 2$, we can choose any a of the form $a = 1 + x^2$ so that $a + 1 = 3y^2$ or $a + 1 = 6y^2$, we then have $\epsilon = -1 = \delta$ we still have $2^p - 1$ is prime if and only if $T_{2^p-2}(a) = 0 \bmod Q$. This condition turns out to be necessary and sufficient and is given in OEIS A18844.

Lemma 2.1 is just the analogue of the usual computational definition of the existence of a primitive root in the case of \mathbb{Z}/Q^* but there is one basic difference here, since changing base a means changing the group $\mathbb{Z}[\sqrt{a^2 - 1}]^*$ also. We can change a until we get the correct order.

Example 2.2. Let $a = 2$ and $r = r_1, \dots, r_k$ be an odd square free integer not divisible by 3 and let $\delta = 2 - r \in \{0, 1\} \bmod 3$, $N = 2n + \delta$ and $Q = r2^N - 1$. Let $s_0 = 2, s_{n+1} = s_n^2 - 2$. Then Q is prime implies Q divides $T_r(s_{N-2}/2)$. Conversely if Q is odd integer of the form $r2^N - 1$, and divides $T_r(s_{N-2}/2)$ and in addition, $T_{(r/r_j)}(s_N/2) \neq 1 \bmod Q$, for $j = 1, \dots, k$, then Q is prime.

Proof. The value of δ were chosen such that $Q = 1 \bmod 3$, so for $a = 2, \epsilon = -1$ and $\left(\frac{2(a+1)}{Q}\right) = -1$ and we have $\omega^{(Q-\epsilon)/2} = \omega^{r2^{N-1}} = -1$, so that $T_{r2^{N-2}}(2) = 0$. It also implies the order $O_Q(\omega) = t_1 \dots t_k 2^N$ where t_j divides r_j . If $T_{(r/r_j)}(s_N/2) \neq 1, \omega^{(r/r_j)2^N} \neq 1$, we must have $t_j = r_j$ and $O_M(\omega) = M + 1$. \square

If we let $r = 5$, then for n up to 3000, there are 29 primes and 5 of them at $n = 2, 18, 32, 1638, 2622$, fail the sufficiency tests.

We also have an order q version

Example 2.3. Let $Q = 12q^n + 1$ be prime where q is an odd prime, then $T_{3q^n}(2) = 0 \pmod{Q}$. Conversely if an odd integer Q is of the form $12q^n + 1$ satisfies $T_{3q^n}(2) = 0$, and in addition $T_{4q^n}(2), T_{12q^{n-1}}(2)$ are all not 1 mod Q , then Q is prime.

Proof. We have $Q = 1 \pmod{3}$ and $5 \pmod{8}$. So if $a = 2$, $\epsilon = 1$, $\delta = -1$ so that we have $\omega^{6q^n} = -1$. So $T_{3q^n}(2) = 0$ and $O_Q(\omega) = 4.3^{t_1}q^{t_2}$, $t_1 \leq 1, t_2 \leq n$. It is $12q^n = Q - 1$ iff $T_{12q^{n-1}}(2) \neq 1$ and $T_{4q^n}(2) \neq 1$. \square

For $q = 5$, Q is prime when

$$n = 1[1, 1], 5, 7, 18, 19, 23, 46, 51, 55, 69[1, *], 126[*], 469, 1835[*], 3079, 3249, 4599, 4789$$

but the primality proof failed for 1, 69, 126, 1835, but we get a proof when we change base.

Recall that a Proth's number $N = k2^n + 1$, where k is odd and $k < 2^n$, is prime if and only if there is an integer a such that $a^{(N-1)/2} = 1 \pmod{N}$.

We have an exact analogue

Lemma 2.4. Let $N = k2^n + 1$ where k is odd and $k < 2^n$. Let a be such that $\epsilon = -\delta = 1$, then N is prime if and only if it pass the Chebyshev test, ie. $\omega_a^{(N-1)/2} = -1$ or equivalently $T_{k2^{n-1}}(a) = -1, U_{k2^{n-1}-1}(a) = 0 \pmod{N}$.

Proof. The necessity is just Chebyshev test. Conversely $\omega^{(N-\epsilon)/2} = \omega^{k2^{n-1}} = -1 \pmod{N}$ implies the same mod any prime p dividing N , which implies $p + 1 \geq O_p(\omega) \geq 2^n$, which means every prime divisor of N is greater than \sqrt{N} . \square

A special case of this is a question in MathOverflow [5], where we set $a = 4$ (see also answer by Ian Algol). The requirement $\epsilon = -\delta = 1$ translate to $\left(\frac{5}{N}\right) = -1$ and $\left(\frac{N}{3}\right) (-1)^{(N-1)/2} = -1$ since $N = 1 \pmod{8}$ for $n > 2$, and note that $P_n(x) = 2T_n(x/2)$.

For any fixed k and n , there is always some choice of a to give a necessary and sufficient condition. What we want is for a fixed k to find an a which works for all n but for $k = 3$, this does not seem to be possible.

Example 2.5. In the same way if $n > 1$ and $F_n = 2^{2^n} + 1$ and set $a = 4$, we have $\epsilon = 1 = -\delta$, so $\omega_4^{2^{2^n-1}} = -1$ so that $O_{F_n}(\omega_4) = 2^{2^n} = F_n - 1$ and also $\omega_4^{2^{2^n-2}} + \bar{\omega}_4^{2^{2^n-2}} = 0$. So F_n is prime if and only if $T_{2^{2^n-2}}(4) = 0 \pmod{F_n}$. In Lucas-Lehmer term if $s_0 = 8, s_{n+1} = s_n^2 - 2$, then F_n is prime if and only if F_n divides s_{2^n-2} .

ACKNOWLEDGEMENTS

This works started when we read some posting on MathOverflow of user Pedja Terzić and realized that the function he defined is essentially Chebyshev polynomial $T_n(x)$ and that the compositional identity $T_n(T_m(x)) = T_{nm}(x)$ means there is an implied q -nary Lucas-Lehmer iteration algorithm. Numerical experimentation then lead us to the statement of theorem 1.1. The q -nary Lucas Lehmer is essentially known in many posting by Pedja Terzić [5, 6] and these can all be derived from our main Lemma 1.6.

REFERENCES

1. Y. Bilu, G. Hanrot, P. Voutier, Existence of primitive divisors of Lucas and Lehmer numbers, Journal für die reine und angewandte Mathematik (Crelles Journal) 539:75-122 · January 2001.
2. D. H. Lehmer, On Lucas test for the primality of Mersenne numbers, J. Londo Math. Soc, 10 (1935), 162-165.
3. Lucia, MathOverflow, Is there an explicit formula for Chebyshev polynomials mod $x^r - 1$.
4. R. S. Melham, Probable prime tests for generalized Mersenne numbers, Bol Soc Mat Mexicana, 14, (2008), 7-14.
5. Pedja Terzić, MathOverflow, Primality test for specific class of Proth numbers.
6. Pedja Terzić, Project Primus.
7. M. O. Rayes, V. Trevisan and P. S.Wang, Chebyshev Polynomials and Primality tests,ICM Technical Report, ICM-199901-0002.
8. Wikipedia, Chebyshev polynomials.
9. Wikipedia, Sierpiński numbers.

Email address: chuakks52@outlook.com