Generalizing the Lucas-Lehmer Primality Test

Alyson Deines *

May 8, 2007

1 Lucas-Lehmer Test for Mersenne Primes

1.1 Background

Take \( P, Q \in \mathbb{Z} \setminus 0 \). Consider the quadratic polynomial \( x^2 - Px + Q \). Then take the discriminant \( D \) to be the square-free part of \( c^2 D = P^2 - Q \). The roots of the polynomial are \( a, \bar{a} = \frac{P \pm \sqrt{D}}{2} \). So we have the following identities:

\[
\begin{align*}
a + \bar{a} &= P \\
a\bar{a} &= Q \\
a - \bar{a} &= c^2 D.
\end{align*}
\]

Define the Lucas sequences \( U, V \) to be

\[
U_n(P, Q) = \frac{a^n - \bar{a}^n}{a - \bar{a}}
\]

and

\[
V_n(P, Q) = a^n + \bar{a}^n
\]

*the author was advised by Dr. Todd Cochrane and supported by the Goldwater and Clare Booth Luce scholarships
for $n \geq 0$. For simplicity, $P, Q$ will be assumed and the Lucas sequences will be denoted by $U_n$ and $V_n$. Note $U_0 = 0, U_1 = 1, V_0 = 2, \text{ and } V_1 = P$.

The following identities will be used in the paper. Their proofs are in the appendix.

1. $U_{p^n-1(p-(\frac{P}{P^n}) \equiv 0 (\text{mod } p^n)}$ if $GDC(2QcD, p) = 1$.

2. $V_{2n} = V_n^2 - 2Q^n$

3. $2V_{m+n} = V_m V_n + c^2 DU_m V_n$

4. $V_P \equiv P (\text{mod } p)$

5. $U_P \equiv (\frac{P}{p} (\text{mod } p)$

6. $V_n^2 - c^2 DU_n^2 \equiv 4Q^n$

(7) $U_n = U_{\frac{n}{2}} V_{\frac{n}{2}}$

(8) If $n, k \geq 1$ then $U_n \mid U_{kn}$

1.2 Theorem 1

Theorem 1. [2, Riesel] Suppose $N + 1 = \Pi_{j=1}^{n} q_j^\alpha_j$ with all $q_j$'s distinct primes. If a Lucas sequence $U_m$ satisfying $GDC(2QcD, N) = 1$ can be found such that $GDC(U_{N+1}, N) = 1$ for any $j = 1, 2, ..., n$ and $N$ divides $U_{N+1}$, then $N$ is prime.

Proof: Consider any prime factor $p$ of $N$. Then $GDC(U_{N+1}, p) = 1$ for all $j = 1, 2, ..., n$. Additionally $p$ divides $U_{N+1}$. Then $U_{N+1} = \frac{a^{N+1} - a^{-N+1}}{a - \bar{a}} \equiv 0 (\text{mod } p)$. This implies $a^{N+1} - \bar{a}^{N+1} \equiv 0 (\text{mod } p)$, or, as $a\bar{a} = Q$ then $a$ and $\bar{a}$ are coprime to $N$ and thus coprime to $p$. Then we have
\(a^{N+1} \equiv (a^{N+1})^{N+1} \equiv 1 \pmod{p}\). Now, take \(d\) to be the smallest integer such that \(U_d \equiv 0 \pmod{N}\). Then \(U_d \equiv 0 \pmod{p}\) and as above \((a^{N+1})^d \equiv 1 \pmod{p}\). As \(d\) is the smallest such integer, \(d \mid N + 1\). However, since \(p\) does not divide \(U_j \forall j = 1, 2, \ldots, n\), then \(a^{q_j} \equiv (a^{N+1})^{q_j} \equiv 1 \pmod{p}\), which implies that \(d\) does not divide \(N+1\), thus \(d \mid N + 1\) but \(d\) does not divide \((N + 1)q_j\) for all \(j = 1, 2, \ldots, n\), hence \(q_j \mid d\) so \(N + 1 \mid d\) and we have \(N + 1 = d\).

Suppose \(N = \prod p_i^{\alpha_i}\) and \(\text{GCD}(2QcD, N) = 1\). Then by (1) we have \(U_{p_i^{\alpha_i}} = (p_i - D) \equiv 0 \pmod{p_i^{\alpha_i}}\). Using the fact that all the subscripts satisfying precisely one of the congruences \(U_n \equiv 0 \pmod{p_i^{\alpha_i}}\) constitute the nonnegative part of a module, the subscripts satisfying all the congruencies also form the nonnegative part of a module. This module has a generator, which is the least common multiple of the generators of all the individual modules. Thus \(U_m \equiv 0 \pmod{N}\) where \(m = \text{LCM} [p_i^{\alpha_i} (p_i - D) / p_i]\).

Since \(\text{GCD}(2QcD, N) = 1\), we have that all \(p_i\)'s are odd and thus all \(p_i - D / p_i\) are even. This in turn leads to the inequality \(m = 2\text{LCM} [p_i^{\alpha_i} (p_i - D / p_i)] \leq 2\prod p_i^{1 - 1 / p_i} p_i^{\alpha_i} \leq 2N \prod p_i^{1 / 2} (1 + \frac{1}{p_i})\). Define \(T = 2N \prod p_i^{1 / 2} (1 + \frac{1}{p_i})\). Now there are two cases to consider, first, where \(N\) is a prime power and second, \(N\) contains at least two distinct prime factors.

Case 1. Suppose \(N\) is a prime power, then \(N = p_1^{\alpha_1}\), where \(\alpha_1 \geq 2\). In this case we can calculate the exact value of \(m\), \(m = N(1 + \frac{1}{p_1}) = p_1^{\alpha_1} \pm p_1^{\alpha_1 - 1}\). Then we have \(p_1^{\alpha_1} \pm p_1^{\alpha_1 - 1} \neq N + 1\).

Case 2. If \(N\) contains at least two distinct prime factors, \(p_1\) and \(p_2\), we have \(T = N(1 + \frac{1}{p_1})(1 + \frac{1}{p_2}) \prod p_i^{1 / 2} (1 + \frac{1}{p_i}) \leq N(1 + \frac{1}{3})(1 + \frac{1}{3}) = 0.8N < N + 1\). Thus, if \(N\) is a composite number, \(d \neq N + 1\). However, as the value for \(d\) was previously seen to be \(d = N + 1\), \(N\) must be prime.

1.3 Primality Test for Mersenne Numbers

Theorem [1, Ribenboim] Let \(P = 2\) and \(Q = 4\). Consider the associate Lucas sequences \((U_m)_{m \geq 0}\), \((V_m)_{m \geq 0}\) which have discriminant \(D = 3\) (as \(c^2D = 12\)). Then for \(N = M_q\), where \(M_q = 2^q - 1\), \(N\) is prime if and only if \(N\) divides \(V_{N+1}^{N+1}\).

Proof: Let \(N\) be a prime. By (2)
\[V_{N+1}^{2} = V_{N+1}^{N+1} + 2Q_{N+1}^{N+1} \]
\[ V_{N+1} = 2(-2)(-2)^{N-1} \]
\[ \equiv V_{N+1} + 4 - \frac{2}{N} \]
\[ \equiv V_{N+1} + 4 \pmod{N}. \]

Note that \( -\frac{2}{N} = 1 \) as \( N \equiv 3 \pmod{4} \) and \( N \equiv 7 \pmod{8} \), thus \( -\frac{2}{N} = -1 \). Thus to show \( N \) divides \( V_{N+1} \) we need to show \( V_{N+1} \equiv -4 \pmod{N} \). By (3),

\[ 2V_{N+1} = V_NV_1 + c^2DU_NU_1 = 2V_N + 12U_N \]

By (4)

\[ V_N \equiv P \pmod{N} \]

and by (5)

\[ U_N \equiv \frac{D}{N} \pmod{N} \]

Thus we arrive at \( V_{N+1} \equiv V_N + 6U_N \equiv 2 + 6\frac{3}{N} \equiv 2 - 6 \equiv -4 \pmod{N} \).

Now, showing the other direction, assume \( N \) divides \( V_{N+1} \). By (7) \( U_{N+1} = U_{\frac{N+1}{2}}V_{\frac{N+1}{2}} \) which implies that \( N \) divides \( U_{N+1} \). By (6) \( V_{\frac{N+1}{2}}^2 - 12U_{\frac{N+1}{2}} = 4(-2)^{\frac{N+1}{2}} \). As \( N \) does not divide \( 4(-2)^{\frac{N+1}{2}} \), \( N \) does not divide \( 12U_{\frac{N+1}{2}} \), thus \( \gcd(N, U_{\frac{N+1}{2}}) = 1 \). Since \( \gcd(2QcD, N) = 1 \) all criteria are met for Theorem 1 and hence \( N \) is a prime.

### 1.4 Actual Test

Theorem [1, Ribenboim] The number \( M_n = 2^n - 1 \) is prime if and only if \( M_n \) divides \( S_{n-2} \) where \( S_0 = 4 \) and \( S_{k+1} = S_k^2 - 2 \).

Proof: First notice that \( \frac{V_2}{2} = 4 = S_0 \). Now use induction. Assume \( S_{k-1} = \frac{V_{2k}}{2^{2k-1}} \). Then

\[ S_k = S_{k-1}^2 - 2 = \frac{V_{2k}^2}{2^{2k}} - 2 = \frac{V_{2k+1} + 2Q^{2k}}{2^{2k}} - \frac{2^{2k+1}}{2^{2k}} = \frac{V_{2k+1}}{2^{2k}}. \]

Thus from the Primality Test for Mersenne Numbers, the above statement holds.

Notice that Theorem 1 does not work well if you wish to generalize this primality test. To use Theorem 1 for \( N = h2^n - 1 \) the Lucas sequence \( U_{\frac{N+1}{q_i}} \) must be examined for all \( q_i \) where \( q_i \) are factors of \( h \). This leads to the necessity of the following theorem for the generalization of the Lucas-Lehmer primality test.
2 Generalized Lucas-Lehmer Primality Test

2.1 Theorem 2

Theorem 2: [2, Riesel] Suppose \( N + 1 = RF = R \prod q_i^{e_i} \) with all \( q_i \)'s distinct primes, \( R < F \), and \( \text{GCD}(R, F) = 1 \). If a Lucas sequence \( U_m \) with \( \text{GCD}(2QcD, N) = 1 \) exists satisfying \( \text{GCD}(U_{N+1}, N) = 1 \) and \( U_{N+1} \equiv 0 \pmod N \), then \( N \) is prime.

Proof: Consider a possible prime factor of \( N \), \( p \). If we can find a Lucas sequence \( U_m \) with \( \text{GCD}(2QcD, N) = 1 \) such that \( \text{GCD}(U_{N+1}, N) = 1 \), then \( \text{GCD}(U_{N+1}, p) = 1 \) for all \( i \). Further, if \( U_{N+1} \equiv 0 \pmod N \) then \( U_{N+1} \equiv 0 \pmod p \). Take \( d \) to be the smallest subscript such that \( U_d \equiv 0 \pmod p \). From \( U_{N+1} \equiv 0 \pmod p \) we have \( a^{N+1} \equiv a^{N+1} \pmod p \), which in turn yields \( (a \bar{a})^{N+1} \equiv 1 \pmod p \). Similarly, \( (a \bar{a})^d \equiv 1 \pmod p \). Then \( d \) divides \( N+1 \). As \( p \) does not divide \( U_{N+1} \) for all \( i \), \( (a \bar{a})^{N+1} \) is not congruent to \( 1 \pmod p \). Hence \( d \) does not divide \( \frac{N+1}{q_i} \) for any \( q_i \), so \( F \) divides \( d \). However, by (1) \( d \) divides \( p - \frac{D}{p} \), namely, \( d \) divides \( p + 1 \), so \( F \) divides \( p + 1 \) and we can say \( p \geq F + 1 \). If \( p \geq F + 1 \), then \( F + 1 > \sqrt{N} \) and \( N \) is prime. If \( p = F - 1 \) this is not the case, so consider \( N = RF - 1 = R(p + 1) - 1 = Rp + R - 1 \equiv 0 \pmod p \). This implies that \( R \equiv 1 \pmod p \). However, since \( 0 < R < F = p + 1 \), if \( R \equiv 1 \pmod p \), then \( R = 1 \), which implies that \( N = p \), i.e. \( N \) is a prime.

Notice with this test, it is easy to test numbers of the form \( h = R \), and \( 2^n = F \), where \( h < 2^n \). However, when \( h > 2^n \), it becomes difficult to calculate the necessary Lucas sequences. Another problem with this test, is that in many cases, such as \( Q = 1 \), \( \left( \frac{D}{p} \right) = -1 \), then \( U_{N+1} \equiv 0 \pmod p \). So one solution is to insert new elements into the sequence to double the index.

2.2 Generalized Primality Test (O. Körner, Ulm, Germany)

Theorem: [2, Riesel] If \( h \) is odd and \( 2^n > 4h \), then \( N = h2^n - 1 \) is prime if there exists a Lucas sequence \( V_m \) with \( \text{GCD}(QcD, N) = 1 \) such that \( V_{N+1} \equiv 0 \pmod N \).

Proof: Suppose \( N \) is composite and \( p \) is the smallest prime factor of \( N \). Then \( p \leq \sqrt{N} \). If \( U_d \equiv 0 \pmod N \) for \( d \), where \( d \) is defined to be the smallest subscript such that \( U_d \equiv 0 \pmod N \). Then
from (8), all \( m \) with \( U_m \equiv 0 \pmod{N} \) are multiples of \( d \). Since \( U_{N+1}^{2} = V_{N+1}^{2} U_{N+1} \equiv 0 \pmod{N} \), \( d \) divides \( \frac{N+1}{2} \).

Notice that \( U_{N+1}^{2} \) is not congruent to 0 \( \pmod{N} \). If for some \( m \) \( U_m \) and \( V_m \) are both congruent to 0 \( \pmod{N} \), then \((a - \overline{a})U_m \equiv V_m \equiv 0 \pmod{N}\). This implies that \( a^m - \overline{a}^m = (a^m + \overline{a}^m) \equiv 2a^m \) and \(-2\pi^m \equiv 0 \pmod{N}\), thus \( a^m, \overline{a}^m \equiv 0 \pmod{N}\), and moreover, there exists a prime \( p \), \( p \) a factor of \( N \) such that \( p \) divides \((a - \overline{a})^2 = c^2D\). This is a contradiction as \( \gcd(QcD, N) = 1\).

Applying the previous reasoning to \( m = \frac{N+1}{4} \), we find that \( d \) does not divide \( \frac{N+1}{4} = h2^n \). Thus \( 2^{n-1} \) divides \( d \). Now, notice that \( U_{p^2}^2 \equiv 0 \pmod{p} \) by (1), so \( d \) divides \( p - \frac{p}{p} \), which implies \( 2^{n-1} \) divides \( p - \frac{p}{p} \). In particular \( p \equiv \frac{p}{p} \pmod{2^{n-1}} \) and \( p \geq 2^{n-1} - 1 \).

The case \( p = 2^{n-1} - 1 \) can be excluded as this implies that \( N = h2^n - 1 = 2h(p+1) - 1 \equiv 2h - 1 \pmod{p} \) and \( 2h - 1 = p \). As \( p^2 \geq (2^{n-1})^2 = 2^{n(2n-2)} > h2^n = N + 1 \), this contradicts the assumption that \( p \) is the smallest prime factor of \( N \). Thus \( N \) is prime.

### 2.3 Lucas’ Generalized Primality Test when 3 does not divide \( h \)

Theorem: [2, Riesel] Suppose that \( h \) is an odd integer, \( 2^n > h \) and neither \( N = h2^n - 1 \) nor \( h \) is divisible by \( 3 \). Then \( N \) is a prime if and only if \( v_{n-2} \equiv 0 \pmod{N} \), where \( v_k = v_{k-1}^2 - 2 \) and \( v_0 = (2 + \sqrt{3})^h + (2 - \sqrt{3})^h \).

Proof: Take \( a = 2 + \sqrt{3} \) and \( \overline{a} = 2 - \sqrt{3} \). Then \( P = 4, Q = 1, c^2D = 12, D = 3, \) and \( \frac{P}{D} = -1 \). Take \( \sqrt{a} = \frac{\sqrt{3}+1}{2}, \overline{\sqrt{a}} = \frac{\sqrt{3}-1}{2} \) and create the sequence \( V_k' = (\frac{\sqrt{3}+1}{2})^k + (\frac{\sqrt{3}-1}{2})^k \). Then \( P' = \sqrt{6} \) and \( Q' = 1 \). Then for the Lucas sequence \( V_k \) defined by \( a \) and \( \overline{a} \), \( V_k = V_{2k} = V_k^2 - 2Q^k = V_k^2 - 2 \). Then for \( v_k = V_{h2^k}, v_k = v_{k-1}^2 - 2 \) holds. Thus \( v_{n-2} \equiv 0 \pmod{N} \) if and only if \( V_{2^{n-1}} \equiv V_{h2^{n-2}} \equiv V_{N+1} \equiv 0 \pmod{N} \). Hence, by the Generalized Primality Test of Korner, \( N \) is prime.

Notice that the above test can be used for Mersenne numbers when \( h = 1 \), but it utilizes a different sequence. Even in the case of the first test, the Test for Mersenne primes, the sequence is not unique, other sequences, i.e. other \( P \) and \( Q \) can be found that satisfy the conditions required.
3 Testing Numbers of the Form $2^n3^m - 1$

The problem with testing numbers where $3 \mid h$ is that there is no one recursive sequence $(v)_n$ that we can use to check all cases. Further complicating issues $(\frac{D}{N})$ now depends on both $h$ and $n$. Thus there is no consistent $D$ such that $(\frac{D}{N}) = -1$ for all $N$ which means that it is difficult and computationally tedious to find an appropriate Lucas sequence in the first place. However, Riesel there is a test in [2, Riesel] specifically for when $3 \mid h$.

3.1 Theorem 3, $3 \mid h$

Theorem: [2, Riesel] Suppose $h$ is an odd integer and that $2^n > 4h$. Then $N = h2^n - 1$ is prime if and only if $v_{n-2} \equiv 0 \pmod{N}$, where $v_s = v_{s-1}^2 - 2$ with $v_0 = a^h + a^{-h}$, and $\text{GCD}(N, (a-a^{-1})^2) = 1$, where $a$ is a unit of $\mathbb{Q}(\sqrt{D})$ of the form

$$a = \frac{(k + l\sqrt{D})^2}{r}$$

where

$$\left(\frac{D}{N}\right) = -1$$

and

$$\frac{k^2 - l^2D}{r} \left(\frac{r}{N}\right) = -1.$$ 

For $n \equiv m + 1 \pmod{4}$ this test can be used for numbers of the from $N = 2^n3^m - 1$ with one consistent sequences and discriminant $D$. Additionally, examining many of the other cases for $n$ not congruent to $m + 1 \pmod{4}$ shows that $N$ cannot be prime.

3.2 Primality Test for $N = 2^n3^m - 1$

Theorem: Take $h = 3^m$ to get $N = 2^n3^m - 1$. Then when $D = 5$, $Q = 1$ and $n \equiv m + 1 \pmod{4}$, the previous theorem, Theorem 3, is satisfied.

Proof: If $D = 5$, $Q = 1$ we find that $P = 3$ as $P^2 - 4Q = D$. Then $a, \bar{a} = \frac{-3 \pm \sqrt{5}}{2}$. Notice $\bar{a} = \frac{-3 - \sqrt{5}}{2} = a^{-1}$. We additionally find that for $k = -1, l = 1, r = -4$ the following equations are satisfied:

$$a = \frac{(k + l\sqrt{D})^2}{r}$$

and

$$\frac{k^2 - l^2D}{r} \left(\frac{r}{N}\right) = -1.$$
Notice that \( \left( \frac{n!}{N!} \right) = (-1)^{\frac{2^n(n-1)}{2}} = (-1)^{2^n-1} = -1. \) This implies that \( \left( \frac{a}{N} \right) \left( \frac{b}{N} \right) = (-1)(-1) = -1. \)

Now the only item left to check is that \( \left( \frac{a}{N} \right) = -1, \) when this occurs all the criteria for the test are satisfied. As \( 5 \equiv 1 \pmod{4} \) we have \( \left( \frac{5}{N} \right) = \left( \frac{N}{5} \right). \) This simplifies the problem to finding which values \( \pmod{5} \) give \( \left( \frac{N}{5} \right) = -1, \) namely, for what values is \( N^2 \equiv -1 \pmod{5} \). Thus we want \( N \equiv 2, 3 \pmod{5} \), which implies we need to find \( n, m \) such that \( 2^n 3^m \equiv 3, 4 \pmod{5} \). Examining \( 2^n \) and \( 3^m \) individually \( \pmod{5} \), the following relation appears \( 2^{1+4k} \equiv 2, 2^{2+4k} \equiv 4, 2^{3+4k} \equiv 3, 2^{4k} \equiv 1 \) and \( 3^{1+4k} \equiv 3, 3^{2+4k} \equiv 4, 3^{3+4k} \equiv 2, 3^{4k} \equiv 1 \) for some integer \( k \). Thus \( 2^n 3^m \equiv 3 \pmod{5} \) when \( n \equiv m + 1 \pmod{4} \) and \( 2^n 3^m \equiv 4 \pmod{5} \) when \( n \equiv m + 2 \pmod{4} \).

This allows us to use Theorem 3 to test \( N = 2^n 3^m - 1 \) with \( v_0 = \frac{-3+\sqrt{5}}{2}h + \frac{-3-\sqrt{5}}{2}h. \) Notice that \( v_0 \) can be calculated \( \pmod{N} \) as above but with a different relation \( V_{m+1} = (a+n)V_m - aV_{m-1} = PV_m - QV_{m-1} = 3V_m - V_{m-1}. \)

Now examining the cases where \( 2^n 3^m \equiv 0, 1, 2 \pmod{5} \). If \( 2^n 3^m \equiv 1, \) then \( 5 \mid N, \) so \( N \) is not prime. This case occurs when \( n \equiv m \pmod{4} \). As \( \mathbb{F}_5 \) is a field, and thus has no zero divisors, \( 2^n 3^m \equiv 0 \) never occurs. This leaves only the case \( 2^n 3^m \equiv 2 \pmod{5} \), which occurs when \( n \equiv m - 1 \pmod{4} \). Future work could be finding a test for this situation.

Notice however, that this test does not allow us to test primes where \( 4h > 2^n \). With the case of \( N = 2^n 3^m - 1 \) we can accomplish testing of \( N \) when \( 3^m > 2^n \) by reversing the rolls of \( R \) and \( F \) in Theorem 2. Here we need to test that \( N \mid U_{N+1} \) and that \( N \) does not divide \( U_{N+1}. \) This is equivalent to the condition \( N \mid V_{N+1}^2 - Q_{N+1}^{N+1}. \) First note that \( U_{N+1} = U_{N+1}^2 (V_{N+1}^2 - Q_{N+1}^{N+1}). \) If \( N \mid V_{N+1}^2 - Q_{N+1}^{N+1}, \) then as \( V_{N+1}^2 - DU_{N+1} = 4Q_{N+1}^{N+1}, \) this simplifies to \( DU_{N+1} = -3Q_{N+1}^{N+1} \pmod{N}. \) As \( \text{GCD}(2QcD, N) = 1, \) \( N \) does not divide \( U_{N+1} \) but \( N \mid U_{N+1}. \) As \( V_{2k} = V_{2k-1}^2 - 2Q_{2k-1}^{2k-1}, \) we can easily calculate \( V_{2n}. \) From here note that \( V_{3k+2n} = V_{3k+2n}^2 (V_{3k+2n}^2 - 3Q_{3k+2n}^{2k+1}). \) So we can easily calculate \( V_{3m-12n} = V_{3m-12n}^2. \) Also note that this test is not restricted to the previous cases of \( n \equiv m + 1, n \equiv m + 2 \pmod{4} \) and though slower, could be used to test all numbers \( N \) where \( 2^n > 3^m \) as well, however, as noted above, we wouldn't be able to use \( Q = 1 \) and \( \left( \frac{b}{N} \right) = -1 \) as that results in \( U_{N+1} \equiv 0 \pmod{N}. \)
4 Appendix

Here are the proofs of the following:

(1) $U_{p^{n-1}(p-(\frac{p}{p^r}))} \equiv 0 \pmod{p^n}$ if $GDC(2QcD, p) = 1$.

(2) $V_{2n} = V_n^2 - 2Q^n$

(3) $2V_{m+n} = V_mV_n + c^2DU_mU_n$

(4) $V_p \equiv P \pmod{p}$

(5) $U_p \equiv (\frac{D}{p}) \pmod{p}$

(6) $V_n^2 - c^2DU_n^2 = 4Q^n$

(7) $U_{2n} = U_nV_n$

(8) If $n, k \geq 1$ then $U_k \mid U_{kn}$

Proof of (1)

By definition $U_n = \frac{a^n - \overline{a}^n}{a - \overline{a}}$. As $a$ is in $\mathbb{Q}(\sqrt{D})$, we can write $a$ as $a = r + s\sqrt{D}$ for some $r, s \in \mathbb{Q}(\sqrt{D})$. Note that as $GDC(2QcD, p) = 1$ and $Q = a\overline{a}$, $GDC(a, p) = 1$. Thus $a^n = (r + s\sqrt{D})^n = r^n + s^nD^n \equiv r^n + s^n(\frac{D}{p})\sqrt{D} \equiv r^n + s^n(\frac{D}{p})\sqrt{D} \pmod{p}$. This implies that $a^n \equiv a \pmod{p}$ if $(\frac{D}{p}) = 1$ and $a^n \equiv \overline{a} \pmod{p}$ if $(\frac{D}{p}) = -1$.

Then for $(\frac{D}{p}) = -1$ we have that $a^{p+1} \equiv a^pa \equiv a\overline{a} \pmod{p}$. Therefore $a^{p^{n-1}(p+1)} = (a^{p+1})^{p^{n-1}} = (a\overline{a} + kp)^{p^{n-1}} \equiv (a\overline{a})^{p^{n-1}} \pmod{p^n}$ as $p^n$ divides every coefficient of $(a\overline{a} + kp)^{p^{n-1}}$ except the first coefficient, i.e. the coefficient of $a\overline{a}$. Thus $U_{p^{n-1}(p-(\frac{p}{p^r}))} \equiv a^{p^{n-1}(p-(\frac{p}{p^r}))} - a^{p^{n-1}(p-(\frac{p}{p^r}))} \equiv a\overline{a} - a\overline{a} \equiv 0 \pmod{p^n}$. 

9
For \( \frac{\binom{a}{p}}{p} = 1 \) and \( n > 2 \), \( a^{p^n} = (a^p)^{p^{n-1}} = (a + kp)^{p^{n-1}} \equiv a^{p^{n-1}} \pmod{p^n} \) thus \( a^{p^n} = ap^{n-1} \equiv a^{p^{n-1}}(p-1) \equiv 1 \pmod{p} \) and \( a^{p^{n-1}}(p-\binom{a}{p}) - a^{p^{n-1}}(p-\binom{a}{p}) \equiv 0 \pmod{p} \).

Proof of (2)

\[ V_{2n} = a^{2n} + \bar{a}^{2n} = a^{2n} + 2(a\bar{a})^n + \bar{a}^{2n} - 2(a\bar{a})^n = (a^n + \bar{a}^n)^2 - 2(a\bar{a})^n = V_n^2 - 2Q^n. \]

Proof of (3)

\[ 2V_{m+n} = 2(a^{m+n} + \bar{a}^{m+n}) = 2a^m a^n + 2\bar{a}^m \bar{a}^n = (a^m + \bar{a}^m)(a^n + \bar{a}^n) + (a - \bar{a}) \frac{(a^n - \bar{a}^n)(a^n - \bar{a}^n)}{(a - \bar{a})(a - \bar{a})} = V_m V_n + DU_m U_n. \]

Proof of (4)

\[ V_p = a^p + \bar{a}^p \equiv (a + \bar{a})^p \equiv P^p \equiv P \pmod{p}. \]

Proof of (5)

\[ U_p = \frac{a^p - \bar{a}^p}{a - \bar{a}} \equiv \frac{(a - \bar{a})^p}{a - \bar{a}} \equiv (a - \bar{a})^{p-1} \equiv (e^2D)^{\frac{p-1}{2}} \equiv \binom{a}{p} \pmod{p}. \]

Proof of (6)

\[ V_n^2 - e^2DU_n^2 = (a^n + \bar{a}^n)^2 - (a - \bar{a})^2 \frac{(a^n - \bar{a}^n)^2}{(a - \bar{a})^2} = 4a^n \bar{a}^n = 4Q^n. \]

Proof of (7)

\[ U_{2n} = \frac{a^{2n} - \bar{a}^{2n}}{a - \bar{a}} = \frac{(a^n - \bar{a}^n)(a^n + \bar{a}^n)}{a - \bar{a}} = U_n V_n. \]

Proof of (8)
First the following identity must be shown:

\[ U_{m+n} = U_m U_n - Q^n U_{m-n} \]

\[ U_{m+n} = \frac{a^{m+n} - \overline{a}^{m+n}}{a - \overline{a}} = \frac{(a^m - \overline{a}^m)(a^n + \overline{a}^n)}{a - \overline{a}} - \frac{a^n \overline{a}^n (a^{m-n} - \overline{a}^{m-n})}{a - \overline{a}} = U_m U_n - Q^n U_{m-n}. \]

By (7) \( U_k \mid U_{2k} \). Now, assume \( U_k \mid U_{k(n-1)} \) for all integers up to and including \( n - 1 \). Then from the above identity \( U_{kn} = U_{k+k(n-1)} = U_{k(n-1)} U_k - Q^k U_{k(n-2)} \). As \( U_k \mid U_{k(n-2)} \) and \( U_k \mid U_k \), then \( U_k \mid U_{kn} \).

References

