1. Introduction. Let $R$ and $Q$ be relatively prime integers, and $\alpha$ and $\beta$ denote the zeros of $x^2 - \sqrt{Rx + Q}$.

In 1930, D. H. Lehmer [4] extended the arithmetic theory of Lucas sequences by defining $u_n = (\alpha^n - \beta^n)/(\alpha - \beta)$ and $v_n = \alpha^n + \beta^n$ for $n \geq 0$. If $R$ is a perfect square, $\{u_n\}$ and $\{v_n\}$ are Lucas sequences and “associated” Lucas sequences, respectively. If $R$ is not a square, then $u_{2n+1}$ and $v_{2n}$ are integers, while $u_{2n}$ and $v_{2n+1}$ are integral multiples of $\sqrt{R}$. If one defines

\begin{align*}
U_n &= U_n(\sqrt{R}, Q) = \begin{cases} 
(\alpha^n - \beta^n)/(\alpha - \beta) & \text{if } n \text{ is odd}, \\
(\alpha^n - \beta^n)/(\alpha^2 - \beta^2) & \text{if } n \text{ is even},
\end{cases} \\
V_n &= V_n(\sqrt{R}, Q) = \begin{cases} 
(\alpha^n + \beta^n)/(\alpha + \beta) & \text{if } n \text{ is odd}, \\
\alpha^n + \beta^n & \text{if } n \text{ is even},
\end{cases}
\end{align*}

then $\{U_n\}$ and $\{V_n\}$ are seen to be the sequences $\{u_n\}$ and $\{v_n\}$ with the $\sqrt{R}$ factor in $u_{2n}$ and $v_{2n+1}$ suppressed, and are therefore integer sequences. The sequences $\{U_n\}$ and $\{V_n\}$ are known as Lehmer and “associated” Lehmer sequences, respectively.

In this paper, we examine these sequences for the existence of perfect square terms and terms which are twice a perfect square. Using congruences, with extensive reliance upon the Jacobi symbol, we determine that the square terms of those Lehmer sequences $\{U_n(\sqrt{R}, Q)\}$ for which $R$ is odd and $Q \equiv 3 \pmod{4}$, and for which $Q \equiv R \equiv 5 \pmod{8}$, may occur only for $n = 0, 1, 2, 3, 4$ or $6$. We obtain a similar result for the associated Lehmer sequences $\{V_n(\sqrt{R}, Q)\}$, and corresponding results for the sequences $\{2U_n(\sqrt{R}, Q)\}$ and $\{2V_n(\sqrt{R}, Q)\}$.

Interest in the factors of $U_n$ and $V_n$ began with Lehmer [4] who described the divisors of $U_n$ and $V_n$ and gave their forms in terms of $n$. In 1983, Rotkiewicz [7] used the Jacobi symbol to show that certain terms of the Lehmer sequence $\{U_n(\sqrt{R}, Q)\}$ cannot be squares when certain conditions on $R$ and $Q$ are satisfied. Each of Rotkiewicz’s results involves $R \equiv 3 \pmod{4}$, $Q \equiv 0 \pmod{4}$, or $R \equiv 0 \pmod{4}$, $Q \equiv 1 \pmod{4}$, and in either
case it is shown that the term $U_n$ is not a square if $n$ is odd and not a square, or $n$ is an even integer, not a power of 2, whose greatest odd prime factor does not divide $\Delta = R - 4Q^2$.

The problem of determining the square terms when $R$ is a perfect square, i.e., in Lucas sequences and associated Lucas sequences, has been solved in certain cases: When $Q = \pm 1$, and $\sqrt{R} = P$ is odd or has certain even values [1], [2], [3], and recently [6] for all Lucas sequences for which $P$ and $Q$ are odd. The previously mentioned paper by Rotkiewicz contains a partial solution for the Lucas sequence with $P$ even and $Q \equiv 1 \pmod{4}$.

2. Preliminary results. From the definition of $\alpha$ and $\beta$, we have $Q = \alpha \beta$, $R = (\alpha + \beta)^2$ and we define $\Delta = R - 4Q = (\alpha - \beta)^2$. It follows readily from (1) that $U_0 = 0$, $U_1 = 1$, $V_0 = 2$, $V_1 = 1$, and these recurrence relations hold for $n \geq 2$:

$$U_{n+2} = \begin{cases} RU_{n+1} - QU_n & \text{if } n \text{ is odd,} \\ U_{n+1} - QU_n & \text{if } n \text{ is even,} \end{cases}$$

$$V_{n+2} = \begin{cases} V_{n+1} - QV_n & \text{if } n \text{ is odd,} \\ RV_{n+1} - QV_n & \text{if } n \text{ is even.} \end{cases}$$

The definitions of $U_n$ and $V_n$ can be extended to $n$ negative: (1) and (2) immediately imply that $U_{-n} = -U_n/Q^n$ and $V_{-n} = V_n/Q^n$; we see easily that if $n \neq 0$, $\gcd(U_n, Q) = \gcd(V_n, Q) = 1$, so $U_{-n}$ and $V_{-n}$ are integers only when $Q = \pm 1$. We shall require the following properties which hold for all $n$ and all integers $R$ and $Q$, except as noted:

5. If $R$ and $Q$ are odd and $n \geq 0$, then $U_n$ is even iff $3 \mid n$ and $V_n$ is even iff $3 \nmid n$.

6. $U_{2n} = U_n V_n$ and $V_{2n} = \begin{cases} RV_n^2 - 2Q^n & \text{if } n \text{ is odd,} \\ V_n^2 - 2Q^n & \text{if } n \text{ is even.} \end{cases}$

7. $U_{3n} = \begin{cases} U_n(RV_n^2 - Q^n) = U_n(\Delta U_n^2 + 3Q^n) & \text{if } n \text{ is odd,} \\ U_n(V_n^2 - Q^n) = U_n(R\Delta U_n^2 + 3Q^n) & \text{if } n \text{ is even.} \end{cases}$

8. $V_{3n} = \begin{cases} V_n(RV_n^2 - 3Q^n) & \text{if } n \text{ is odd,} \\ V_n(V_n^2 - 3Q^n) & \text{if } n \text{ is even.} \end{cases}$

9. $2U_{m \pm n} = \begin{cases} RU_m V_{m \pm n} + U_{m \pm n} V_m & \text{if } m \text{ is even and } n \text{ is odd,} \\ U_m V_{m \pm n} + RU_{m \pm n} V_m & \text{if } m \text{ and } n \text{ have the same parity,} \\ U_m V_{m \pm n} + RU_{m \pm n} V_m & \text{if } m \text{ is odd and } n \text{ is even.} \end{cases}$

10. $2V_{m \pm n} = \begin{cases} RV_m V_{m \pm n} + \Delta U_m U_{m \pm n} & \text{if } m \text{ and } n \text{ have opposite parity,} \\ RV_m V_{m \pm n} + \Delta U_m U_{m \pm n} & \text{if } m \text{ and } n \text{ are odd,} \\ U_m V_{m \pm n} + R\Delta U_m U_{m \pm n} & \text{if } m \text{ and } n \text{ are even.} \end{cases}$

11. If $j = 2^u k$, $u \geq 1$, $k$ odd, $k > 0$, and $m > 0$, then

(a) $U_{2j+m} \equiv -Q^j U_m \pmod{V_{2^u}}$,}
(b) $U_{2j-m} \equiv Q^{j-m}U_m \pmod{V_{2^k}}$ if $j \geq m$,
(c) $V_{2j+m} \equiv -Q^jV_m \pmod{V_{2^k}}$,
(d) $V_{2j-m} \equiv -Q^{j-m}V_m \pmod{V_{2^k}}$ if $j \geq m$.

(12) If $d = \gcd(m, n)$, then $\gcd(U_m, U_n) = U_d$.
(13) If $d = \gcd(m, n)$, then $\gcd(V_m, V_n) = V_d$ if $m/d$ and $n/d$ are odd, and 1 or 2 otherwise.
(14) If $d = \gcd(m, n)$, then $\gcd(U_m, V_n) = V_d$ if $m/d$ is even, and 1 or 2 otherwise.

Properties (5) through (10) are proven precisely as for the Lucas sequences ((6) through (10) are immediately verifiable using (1) and (2)), and (12) is well-known. Property (11) follows readily from (6), (9), (10), (13) and (14). Properties (13) and (14) are proven in [5].

We list, for reference purposes, the first few values of $U_n$ and $V_n$:

$U_0 = 0$,
$U_1 = 1$,
$U_2 = 1$,
$U_3 = R - Q$;
$V_0 = 2$,
$V_1 = 1$,
$V_2 = R - 2Q$,
$V_3 = R - 3Q$.

3. Some preliminary lemmas. For the remainder of the paper, it is assumed that $R$ and $Q$ are relatively prime odd integers, $R$ is positive and not a square, and that $\Delta = R - 4Q > 0$. (The latter condition assures that $U_n > 0$ and $V_n > 0$ for $n > 0$.)

**Lemma 1.** Let $m$ be an odd positive integer and $u \geq 1$.

(a) If $3 \mid m$, then $V_{2^u m} \equiv \pm 2 \pmod{8}$.
(b) If $3 \nmid m$, then $V_{2^u m} \equiv \begin{cases} -1 \pmod{8} & \text{if } u > 1, \\ R - 2Q \pmod{8} & \text{if } u = 1. \end{cases}$

**Proof.** (a) If $3 \mid m$, then by (5) and (6), $V_{2m} = RV_m^2 - 2Q^m \equiv -2Q$ or $4R - 2Q \equiv \pm 2 \pmod{8}$, and the result is immediate by induction.
(b) If $3 \nmid m$, then $V_{2m} = RV_m^2 - 2Q^m \equiv R - 2Q \pmod{8}$ is odd, so $V_{4m} = V_{2m}^2 - 2Q^{2m} \equiv -1 \pmod{8}$, and the result for $V_{2^u m}$ follows by induction.

It is also readily shown by induction on $u$ that

(15) $V_{2^u} \equiv -Q^{2^{u-1}} \pmod{V_3}$ if $u > 1$, and
(16) $V_{2^u} \equiv -Q^{2^{u-1}} \pmod{U_3}$ if $u \geq 1$.

**Lemma 2.** Let $t > 0$, $m \geq 0$, and $12t - m > 0$. Then

(i) $V_{12t+m} \equiv V_m \pmod{8}$ and $V_{12t-m} \equiv Q^mV_m \pmod{8}$, and
(ii) $U_{12t+m} \equiv U_m \pmod{8}$ and $U_{12t-m} \equiv -Q^mU_m \pmod{8}$.

**Proof.** (i) By repeatedly using (4), we obtain

$V_{6+m} = a_0V_{1+m} + a_1V_m$,
where \( a_0 = (R - Q)(R - 3Q) \) if \( m \) is odd, \( a_0 = R(R - Q)(R - 3Q) \) if \( m \) is even, and \( a_1 = -Q(R^2 - 3QR + Q^2) \). For all odd \( R \) and \( Q \), \( a_0 \equiv 0 \) (mod 8), so \( V_{6r+m} \equiv a_1 V_m \) (mod 8), and it readily follows by induction that \( V_{6r+m} \equiv a_1^r V_m \) (mod 8), for \( r \geq 1 \). Upon letting \( r = 2t \), we have the first congruence of (i), since \( a_1 \) is odd, and the second congruence of (i) is readily established using \( V_n = V_n/Q^n \).

(ii) The proof of (ii) is similar to that of (i).

**Lemma 3.** If \( u > 1 \), the Jacobi symbol \( J = (V_3 | V_{2^u}) \) equals +1.

**Proof.** Since \( V_{2^u} \) is odd, \( \gcd(V_3, V_{2^u}) = 1 \) so \( (V_3 | V_{2^u}) \) is defined. Let \( V_3 = 2^e N, e \geq 1 \) and \( N \) odd. Then \( J = (2^e | V_{2^u})(N | V_{2^u}) \). Since \( V_{2^u} \equiv -1 \) (mod 8) for \( u > 1 \), \( (2^e | V_{2^u}) = +1 \), for all \( e \). Hence, \( J = (-1)^{(N-1)/2}(V_{2^u} | N) \). By (15), \( V_{2^u} \equiv -Q^{2^u-1} \) (mod \( N \), so \( J = (-1)^{(N-1)/2}(-Q^{2^u-1} | N) = (-1)^{(N-1)/2}(-1)^{(N-1)/2} = +1 \).

**Lemma 4.** If \( u > 1 \), then \( (U_3 | V_{2^u}) \) equals +1.

**Proof.** By (5) and (14), \( \gcd(U_3, V_{2^u}) = 1 \), so \( (U_3 | V_{2^u}) \) is defined. We let \( U_3 = 2^e N, e \geq 1 \), \( N \) odd, and proceed as in Lemma 3, using (16), to find that \( (U_3 | V_{2^u}) = +1 \).

**Lemma 5.** If \( n \) is a positive integer, then

(i) \( 3 | U_n \) if and only if \( 3 | n \) and \( R \equiv Q \not\equiv 0 \) (mod 3), or \( 4 | n \) and \( R \equiv 2Q \) (mod 3), and

(ii) \( 3 | V_n \) if and only if \( n \) is odd, \( 3 | n \) and \( R \equiv 0 \) (mod 3), or \( n \equiv 2 \) (mod 4) and \( R \equiv 2Q \) (mod 3).

**Proof.** Assume \( n > 0 \) is odd. We note first that if \( 3 | Q \), then \( 3 | U_n \) and \( 3 | V_n \), since \( \gcd(U_n, Q) = \gcd(V_n, Q) = 1 \). Assume \( 3 \nmid Q \). Then either \( R \equiv 0 \) (mod 3), \( R \equiv Q \) (mod 3), or \( R \equiv 2Q \) (mod 3).

(i) If \( R \equiv 0 \) (mod 3), then \( U_n = RU_{n-1} - QU_{n-2} = -QU_{n-2} \equiv (-Q)^2 U_{n-4} \equiv \ldots \equiv (-Q)^{(n-1)/2} U_1 \not\equiv 0 \) (mod 3).

If \( R \equiv Q \) (mod 3), then \( 3 \) divides \( U_3 = R - Q \), and it follows from (12) that \( 3 | U_n \) if \( 3 | n \). And, if \( R \equiv 2Q \) (mod 3), then \( 3 \) divides \( U_4 = U_2V_2 = R - 2Q \) and, since by (12), \( \gcd(U_4, U_n) = U_1, U_2 \) or \( U_4, 3 | U_n \) iff \( 4 | n \).

(ii) If \( R \equiv 0 \) (mod 3), then \( V_1 = V_1(RV_1^2 - 3Q) \equiv 0 \) (mod 3) and by (13), \( \gcd(V_3, V_n) \) is divisible by 3 iff \( n \) is an odd multiple of 3. If \( R \equiv Q \) (mod 3), then \( 3 | U_3 \); however, by (14), \( \gcd(U_3, V_n) \) is 1 or 2 for all \( n \), so \( 3 \nmid V_n \). If \( R \equiv 2Q \) (mod 3), then \( 3 \) divides \( V_2 = R - 2Q \) and again, by (13), \( \gcd(V_3, V_n) \) is divisible by 3 iff \( n \) is an odd multiple of 2.
4. Squares in \( \{ U_n \} \) and \( \{ V_n \} \). In this section, we use \( \square \) for the words “a square”.

**Lemma 6.** Let \( n \) be a positive odd integer.

(i) If \( Q \equiv 3 \pmod{4} \), then \( U_n = \square \) if and only if \( n = 1 \), or \( n = 3 \) and \( R - Q = \square \), and \( U_n = 2\square \) if and only if \( n = 3 \) and \( R - Q = 2\square \).

(ii) If \( Q \equiv 1 \pmod{4} \), then \( V_n = \square \) if and only if \( n = 1 \), or \( n = 3 \) and \( R - 3Q = \square \), and \( V_n = 2\square \) if and only if \( n = 3 \) and \( R - 3Q = 2\square \).

**Proof.** (i) Assume \( Q \equiv 3 \pmod{4} \) and \( n > 0 \) is odd. We note that \( U_1 = 1 = \square \neq 2\square \) and clearly, \( U_3 = \square \) or \( 2\square \) if \( R - Q = \square \) or \( 2\square \). Assume \( n > 3 \) and let \( n = 2j + m, j = 2^u k, u \geq 1, k \) odd, \( k > 0 \), and \( m = 1 \) or \( 3 \). We define \( \lambda = 1 \) or \( 2 \) and observe that if \( u > 1 \), then, using Lemma 1, we have \( (\lambda | V_{2^u}) = +1 \).

By (11a),
\[
\lambda U_{2j+m} \equiv -\lambda Q^j U_m \pmod{V_{2^u}}.
\]
Now, \( \lambda U_n = \square \) only if the Jacobi symbol \( -\lambda Q^j U_m \pmod{V_{2^u}} \) is +1. However, if \( u > 1 \), then \( -\lambda Q^j U_m \pmod{V_{2^u}} = (\lambda | V_{2^u})(-U_m \pmod{V_{2^u}}) \) is clearly -1 if \( m = 1 \), and, by Lemma 4, is -1 if \( m = 3 \). If \( u = 1 \), then \( n = 4k + m, k \) odd, implies that \( n \equiv -1 \) or \(-3 \pmod{8} \); let \( n = 2i - t, i = 2^w r, w \geq 2, r \) odd and \( t = 1 \) or \( 3 \). By (11b),
\[
\lambda U_n = \lambda U_{2i-t} \equiv \lambda Q^{i-1} U_1 \text{ or } \lambda Q^{i-3} U_3 \pmod{V_{2^u}}.
\]
Since \( Q \equiv 3 \pmod{4} \),
\[
(\lambda Q^{i-1} U_1 \pmod{V_{2^u}}) = (+1)(Q | V_{2^u}) = (-1)(V_{2^u} | Q)
\]
\[
= -(V_{2^w-1} - 2Q^{2^{w-1}} | Q) = -1,
\]
and, using Lemma 4,
\[
(\lambda Q^{i-3} U_3 \pmod{V_{2^u}}) = (\lambda Q^{i-3} \pmod{V_{2^u}})(U_3 \pmod{V_{2^u}}) = -1.
\]
This proves that \( \lambda U_n \neq \square \) and therefore that \( U_n \neq \lambda \square \).

(ii) Assume \( Q \equiv 1 \pmod{4} \) and \( n \) is a positive odd integer. If \( n = 1 \), then \( V_n = 1 = \square \neq 2\square \), and if \( n = 3 \), then \( V_n = R - 3Q \) could be \( \square \) or \( 2\square \). If \( n > 3 \), let \( n = 2j + m, j = 2^u k, u \geq 1, k \) odd, \( k > 0 \), and \( m = 1 \) or \( 3 \). As in (i), let \( \lambda = 1 \) or \( 2 \). By (11c),
\[
\lambda V_{2j+m} \equiv -\lambda Q^j V_m \pmod{V_{2^u}}.
\]
We see from Lemma 1 that if \( u > 1 \), then \( V_{2^u} \equiv -1 \pmod{8} \); hence, in this case, if \( m = 1 \), then \( J = (-\lambda Q^j V_m \pmod{V_{2^u}}) = -1 \), and if \( m = 3 \), then, by Lemma 3, \( J = -1 \). If \( u = 1 \), then \( n = 4k + m \) with \( k \) odd, so \( n \equiv -1 \) or \(-3 \pmod{8} \); let \( n = 2i - t, i = 2^w r, w \geq 2, r \) odd and \( t = 1 \) or \( 3 \). By (11d),
\[
\lambda V_n = \lambda V_{2i-t} \equiv -\lambda Q^{i-1} V_t \equiv -\lambda Q^{i-3} V_1 \text{ or } -\lambda Q^{i-3} V_3 \pmod{V_{2^u}}.
\]
Since $Q \equiv 1 \pmod{4}$,

\[-\lambda Q^{-1}v | V_{2w} = - (\lambda | V_{2w})(Q | V_{2w}) = -(V_{2w} | Q) = -1,

and, using Lemma 3,

\[-\lambda Q^{-1}v | V_{3w} = - (Q | V_{3w})(V_{3w} | V_{2w}) = -1(1+1) = -1,

so $\lambda \nu \neq \square$, and therefore $V_n \neq \lambda \square$.

**Theorem 1.** Let $n \geq 0$. If $Q \equiv 1 \pmod{4}$ and $R \equiv 1, 5,$ or $7 \pmod{8}$, or $Q \equiv 3 \pmod{4}$ and $R \equiv 1 \pmod{8}$, then $V_n \neq \square$ if $n = 1$, or $n = 3$ and $R - 3Q = \square$.

**Proof.** If $n$ is even, then $V_n = \square$ only if $V_n \equiv 0, 1, 4 \pmod{8}$, and by Lemma 1 this is possible for $Q$ and $R$ odd only if $R - 2Q \equiv 1 \pmod{8}$. Hence, for $Q \equiv 1 \pmod{4}$ and $R \equiv 1, 5,$ or $7 \pmod{8}$, or for $Q \equiv 3 \pmod{4}$ and $R \equiv 1, 3,$ or $5 \pmod{8}$, $V_n \neq \square$.

Assume $n$ is odd. If $Q \equiv 1 \pmod{4}$ and $R \equiv 1, 5,$ or $7 \pmod{8}$, the theorem is true by Lemma 6.

Assume $Q \equiv 3 \pmod{4}$ and $R \equiv 1 \pmod{8}$. If $n = 1$, then $V_n = V_1 = 1 = \square$, and if $n = 3$, then $V_n = V_3 = R - 3Q$ is a square iff $R - 3Q$ is a square. Let $n = 2j + m$, $j \geq 1$, $k$ odd, $k > 0$, and $m = 1$ or $3$. Then

$V_{2j+m} \equiv -Q^jV_m \equiv -Q^jV_1 \text{ or } -Q^jV_3 \pmod{V_{2w}}.$

By Lemma 1, $V_{2w} \equiv -1 \pmod{8}$ for $u > 1$ and $V_2 = R - 2Q \equiv 3 \pmod{4}$. Hence, $(-Q^jV_1 | V_{2w}) = -1$ if $u \geq 1$ and by Lemma 3, $(-Q^jV_3 | V_{2w}) = -1$ if $u > 1$. That is, $V_n \neq \square$ if $n = 2 \cdot 2^k + 1$ for $u \geq 1$, $m = 1$, or $u > 1$, $m = 3$.

It remains to show that $V_n \neq \square$ if $n = 4k + 3$, $k$ odd. In this case, $n \equiv -5, -1$ or $3 \pmod{12}$. By Lemma 2,

$V_{12l-5} \equiv Q^3V_5 \equiv Q(R^2 - 5Q + 5Q^2) \equiv 5 \pmod{8}$

and

$V_{12l-1} \equiv QV_1 \equiv 3 \text{ or } 7 \pmod{8}$,

and it is clear that $V_n \neq \square$ in each case. If $n \equiv 3 \pmod{12}$, we write $n = 3r \cdot h$, $r \geq 1$, $h$ odd, $3 \nmid h$. By using (8) repeatedly, we have

$V_{3r} = V_{3r} \cdot \prod_{i=j}^{c-1}(RV_{3r}^2 - 3Q^{3r})$.

for $0 \leq j \leq c - 1$. Since $V_{3r} \cdot | V_{3r} \cdot h$ for $j \leq i$, and $\gcd(V_{3r} \cdot h, Q) = 1$, we have $\gcd(V_{3r} \cdot h, RV_{3r}^2 - 3Q^{3r}) = 1$ or $3$. Therefore, $\gcd(V_{3r} \cdot h, \prod_{i=j}^{c-1}(RV_{3r}^2 - 3Q^{3r}))$ is $1$ or a power of $3$. Hence, $V_{3r} = \square$ only if $V_{3r} = \square$ or $3\square$ for $0 \leq j \leq c - 1$, and, in particular, $V_h = \square$ or $3\square$. However, we have just shown that, for $h$ not divisible by $3$, $V_h = \square$ only if $h = 1$, and, by Lemma 5, $V_h \neq 3\square$. 

Taking \( h = 1 \), we have \( V_n = V_{3^e} = \square \) only if \( V_{3^e} = \square \) or \( 3\square \), for \( j = 1, \ldots, u - 1 \). Now, since \( \gcd(R, R^2 - 3Q) = 1 \) or \( 3 \), \( \square = V_3 = R(R^2 - 3Q) \) is possible only if \( R = \square \) or \( 3\square \). However, \( R \) is not a square, by assumption, and \( R \neq 3\square \) since \( R \equiv 1 \pmod{8} \). It follows that \( V_3 = \square \) for \( e \geq 1 \), proving that \( V_n = \square \) if and only if \( n = 3 \).

**Theorem 2.** Let \( n \geq 0 \) and \( Q \equiv 3 \pmod{4} \), or \( Q \equiv 5 \pmod{8} \) and \( R \equiv 5 \pmod{8} \). Then \( U_n = \square \) if and only if \( n \equiv 3 \pmod{4} \).

(i) \( n = 0, 1, 2, \) or \( n = 3 \) and \( R - Q = \square \), or \( n = 4 \) and \( R - 2Q = \square \), or 
(ii) \( n = 6 \), \( R - Q = 2\square \) and \( R - 3Q = 2\square \) (this implies \( Q \equiv 3 \pmod{4} \), \( R \equiv Q \pmod{8} \)).

**Proof.** That \( U_n = \square \) if (i) holds is obvious. Suppose \( n > 4 \).

**Case 1:** \( n \) odd and \( n \geq 5 \). Assume that \( U_n = \square \). If \( Q \equiv 3 \pmod{4} \), then \( U_n \neq \square \) by Lemma 6. Assume that \( Q \equiv R \equiv 5 \pmod{8} \) and let \( n = 2j + m \), where \( j \) and \( m \) are defined as in the proof of Theorem 1. Then

\[
U_{2j+m} = -Q^j U_m \equiv -Q^j U_1 \text{ or } -Q^j U_3 \pmod{v_2},
\]

and exactly as in the proof of Theorem 1 (and using Lemma 4), we have \( U_n \neq \square \) except possibly if \( n = 4k + 3 \), \( k \) odd.

If \( n = 4k + 3 \), \( k \) odd, then \( n \equiv -5 \), or \( 3 \) \( \pmod{12} \), and by Lemma 2,

\[
U_{12t-5} \equiv -Q^5 U_5 \equiv -Q(R^2 - 3RQ + Q^2) \equiv 5 \pmod{8}
\]

and

\[
U_{12t-1} \equiv -QU_1 \equiv 3 \pmod{8}.
\]

It is clear that \( U_n \neq \square \) in each case. If \( n = 12t + 3 \), we write \( n = 3^e h, e \geq 1 \), \( h \) odd, \( 3 \nmid h \). By using (7) repeatedly, we have

\[
U_{3^eh} = U_{3^eh} \cdot \prod_{i=j}^{e-1} (\Delta U_{3^ih}^2 + 3Q^{3^ih}),
\]

for \( 0 \leq j \leq e - 1 \). By an argument essentially identical to that in Theorem 1, we see that \( U_{3^eh} = \square \) only if \( U_{3^eh} = \square \) or \( 3\square \) for \( 0 \leq j \leq e - 1 \), and, in particular, \( U_h = \square \) or \( 3\square \). We just showed above that for \( h \) not divisible by 3, \( U_h = \square \) only if \( h = 1 \), and \( U_h = 3\square \) is not possible by Lemma 5.

Taking \( h = 1 \), we have \( U_n = U_{3^e} = \square \) only if \( U_{3^e} = \square \) or \( 3\square \) for \( j = 1, 2, \ldots, e - 1 \). We have noted that \( U_3 \) may be a square and have shown above that \( U_3^{2} = U_{24+1} \neq \square \). If \( 3\square = U_3 = U_3(\Delta U_3^2 + 3Q^3) \), then \( \Delta U_3^2 + 3Q^3 = \square \) or \( 3\square \). However, since \( U_3 = R - Q \equiv 0 \pmod{8} \), \( \Delta U_3^2 + 3Q^3 \equiv 0 + 3 \cdot 5 \equiv -1 \pmod{8} \) implies that \( \Delta U_3^2 + 3Q^3 \neq \square \) or \( 3\square \). Hence, \( U_n = U_{3^e} = \square \) only if \( e = 1 \), i.e., only if \( n = 3 \).
Case 2: $n$ even. Assume $n > 4$ and $U_n = \Box$, and let $n = 2^m u$, $u \geq 1$, $m$ odd. By repeated application of (6), we have
\[ U_{2^m} = U_{2^{m-1}} V_{2^{m-1}} V_{2^{m-1}} \ldots V_{2^{m-1}}, \quad \text{for } 0 \leq j \leq u - 1. \]

Now, by (13) and (14), $\gcd(U_{2^m}, V_{2^m}) = 1$ or 2, and $\gcd(V_{2^{m-1}}, V_{2^{m}}) = 1$ or 2 for $i \neq j$. Hence, $\gcd(U_{2^m}, V_{2^m})$ is equal to 1 or a power of 2, and $\gcd(V_{2^{m-1}}, V_{2^{m-1}} \ldots V_{2^{m-1}}) = 1$ or a power of 2. It follows that $U_{2^m} = \Box$ or $2\Box$ and $V_{2^m} = \Box$ or $2\Box$ for $0 \leq j \leq u - 1$. In particular, $U_m = \Box$ or $2\Box$ and $V_m = \Box$ or $2\Box$.

If $Q \equiv 3$ (mod 4), then, by Lemma 6 and Case 1 above, $U_m = \Box$ or $2\Box$ only if $m = 1$ or $m = 3$, and if $Q \equiv 1$ (mod 4) then, by Theorem 1 and Lemma 6, $V_m = \Box$ or $2\Box$ only if $m = 1$ or $m = 3$.

We assume now that $Q \equiv 3$ (mod 4) or $Q \equiv R \equiv 5$ (mod 8). If $m = 1$, $U_{2^m} = U_2$ is odd, so $U_2 \neq 2\Box$. If $j = 1$, then $U_2 = U_1 = \Box$, and, if $j = 2$, then $U_4 = R - 2Q$ could be a square if $R \equiv 3$ (mod 4). If $j = 3$, then $U_2 = U_8 = U_4 V_4$ is not a square since $\gcd(U_4, V_4) = 1$ and $V_4 \neq \Box$ by Lemma 1. Hence, if $m = 1$, then $U_n = \Box$ if and only if $n = 2$ or $n = 4$ and $R - 2Q = \Box$.

If $m = 3$, we show first that $U_{24} \neq \Box$ or $2\Box$, implying that $u \leq 2$. Now, by (7), $U_{24} = U_8 (R DU_8^2 + 3Q^8)$. Since $\gcd(U_8, Q) = 1$, $\gcd(U_8, R DU_8^2 + 3Q^8) = 1$ or 3. If $U_{24} = \Box$ or $2\Box$, then since by (5), $U_8$ is odd, we have $U_8 = \Box$ or $3\Box$; however, $U_8 \neq \Box$, as seen above, and $3\Box = U_8 = U_4 V_4$ implies that $V_4 = \Box$ or $3\Box$, which is impossible by Lemma 1.

It follows that $n = 2^u \cdot 3$, with $u = 1$ or 2. If $u = 1$, then $U_n = U_6 = \Box$ if $U_3 = R - Q = 2\Box$ and $V_3 = R - 3Q = 2\Box$. This is possible for $Q \equiv R \equiv 3$ or 7 (mod 8). Conversely, if $R - Q = 2\Box$ and $R - 3Q = 2\Box$, then $U_6 = \Box$.

If $u = 2$, then $U_n = U_{12} = U_6 V_6 = \Box$ is possible only if $U_6 = 2\Box$ and $V_6 = 2\Box$ ($U_6 = \Box$, $V_6 = \Box$ is not possible since $V_6 \equiv \pm 2$ (mod 8)). This implies that $U_3 = \Box$, $V_3 = 2\Box$, $V_2 = 3\Box$ and $V_2^2 - 3Q^2 = 6\Box$. Hence, there exist integers $x$, $y$ and $z$ such that $U_3 = R - Q = x^2$, $V_3 = R - 3Q = 2y^2$ and $V_2 = R - 2Q = 3z^2$. Since $Q$ and $R$ are odd, $x$ is even, $z$ is odd, and $(3U_3 - V_3)/2 = R - 3x^2/2 - y^2$ implies $y$ is odd. We see now, however, that $Q = V_2 - V_3 = 3z^2 - 2y^2 \equiv 1$ (mod 8), contrary to our assumption that $Q \equiv 3, 5$ or 7 (mod 8). Thus, $n = 2^u \cdot 3$ only if $u = 1$.

**Theorem 3.** Let $n \geq 0$. If $Q \equiv 1$ (mod 4) and $R \equiv 1$ or 7 (mod 8), then $V_n = 2\Box$ if $n = 0$, or $n = 3$ and $R - 3Q = 2\Box$.

**Proof.** We note that $V_0 = 2 = 2\Box$ and $V_3 = R - 3Q$. Assume $n \neq 0, 3$ and that $V_n = 2\Box$. Since $V_n$ is even, $3 \mid n$, by (5). Let $n = 3^c h$, $c \geq 1$ and $3 \nmid h$. By Lemma 6, we may assume $h$ is even. We have, from (8),
\[ V_{3^c h} = V_h \cdot \prod_{i=0}^{c-1} (V_{3^i h}^2 - 3Q^{3^i h}). \]
It follows that $V_{3h} = 2\varnothing$ only if $V_h = \varnothing$ or $3\varnothing$; however, $V_h = \varnothing$ is impossible for $h$ even by Theorem 1 and $3\varnothing = V_h \equiv R - 2Q \pmod{8}$, by Lemma 1, and this is not possible for $Q \equiv 1 \pmod{4}$ and $R \equiv 1$ or $7 \pmod{8}$.

Theorem 4. Let $n \geq 0$ and $Q \equiv 3 \pmod{4}$. Then $U_n = 2\varnothing$ iff

(i) $n = 0$,
(ii) $n = 3$ and $R - Q = 2\varnothing$, or
(iii) $n = 6$, and $R - Q = \varnothing$ or $2\varnothing$ and $R - 3Q = 2\varnothing$ or $\varnothing$, respectively.

We omit the proof, since the argument is similar to those of the preceding theorems.

We remark, in closing, that it appears likely that a different approach may be required to prove the theorems of this paper for additional values of $Q$ and $R$. The difficulty in obtaining the result for the remaining values is related, primarily, to the failure of Lemma 1 to hold for those additional values, and this lemma played a key role in our proofs.

REFERENCES