Primes and Lucas Sequences Draft 30

Mark Broderius

August 23, 2019

1 Introduction

Prime numbers have been studied since ancient times and are considered to be the building blocks of the integers. The Fundamental Theorem of Arithmetic, which can be found on page 2 of [4], states that every integer greater than 1 is either a prime number or can be uniquely expressed as a product of prime numbers. It has been known since the time of the Greeks that there are infinitely many primes. The Prime Number Theorem even gives a formula for approximating the number of primes up to any given integer. If $\pi(x)$ denotes the number of primes less than or equal to x, then $\pi(x)$ is approximately $\frac{x}{ln(x)}$ for large x. More information on this theorem can be found in [1]. Another interesting question is whether different kinds of sequences have a finite or an infinite number of primes. For example, page 57 of [4] states that for fixed integers a and b, there are infinitely primes in the sequence $an + b$, as $n = 0, 1, 2, ...$, if and only if the greatest common divisor of a and b is 1. However, an unsolved problem that dates back to the Greeks is whether the sequence $2^n - 1$ has an infinite number of primes. Numbers of this form are known as Mersenne numbers, and there are currently 51 Mersenne primes that have been discovered, with the largest prime number to be discovered being one of them. More detailed background on Mersenne primes can be found in [2]. The sequence $2^n - 1$ is an example of a type of sequence called a Lucas sequence, and information on these sequences is given in pages $53 - 73$ of [3]. The results of this project have found cases where there are Lucas sequences with very few or no primes.

The Lucas sequences $U_n(P, Q)$ and $V_n(P, Q)$ are sequences that satisfy recurrence relations of the form $x_n = P \cdot x_{n-1} - Q \cdot x_{n-2}$, as shown on page 107 of [4]. The difference between the two sequences lies in their initial conditions. $U_n(P, Q)$ has the initial conditions $U_0(P, Q) = 0$ and $U_1(P, Q) = 1$, while $V_n(P, Q)$ has initial conditions $V_0(P, Q) = 2$ and $V_1(P, Q) = P$.

For example, $U_n(3, 2)$ is the sequence of Mersenne numbers, and it has terms

$$0, 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023, 2047, 4095, 8191...$$

Just like any Lucas sequence $U_n(P, Q)$, the initial two terms are 0 and 1. Each term beyond that is 3 times the previous term minus 2 times the term that is two places preceding it. For instance, 7 is the next term after 3 because $7 = 3(3) - 2(1)$, and 15 is the next term because $15 = 3(7) - 2(6)$.

However, $V_n(3, 2)$ is a different sequence due to its initial conditions. In this case, $P = 3$, and so the initial two terms are 2 and 3.
This results in $V_n(3, 2)$ being the sequence $2, 3, 5, 9, 17, 33, 65, 129, 257, 513, 1025, 2049, 4097, 8193....$

Another famous Lucas sequence is the Fibonacci sequence $U_n(1, -1)$, which has terms $0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, ...$
In this sequence, Each term beyond the initial two values is the sum of the previous two terms.

The corresponding V_n sequence is $2, 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, 199, 322, 521, ...$

In general, recurrence relations have associated characteristic equations that can be solved to produce explicit formulas. The relation $x_n = P \cdot x_{n-1} - Q \cdot x_{n-2}$ has an associated characteristic equation of $x^2 = Px - Q$. Rearranging this gives $x^2 - Px + Q = 0$. Using the quadratic formula, the solutions to this equation are $x = \frac{P+\sqrt{P^2-4Q}}{2}$ and $y = \frac{P-\sqrt{P^2-4Q}}{2}$. Let $a = \frac{P+\sqrt{P^2-4Q}}{2}$ and $b = \frac{P-\sqrt{P^2-4Q}}{2}$. Then $P = a + b$ and $Q = ab$. If a and b are distinct, then it can be shown that $U_n(P, Q) = \frac{a^n-b^n}{a-b}$ and $V_n(P, Q) = a^n + b^n$ as stated on page 107 of [4].

The Sequence of Mersenne numbers can be expressed either with the explicit formula $U_n = 2^n - 1$ or recursively as $U_n(3, 2)$, and the sequence $V_n(3, 2)$ can be expressed as $V_n = 2^n + 1$. Similarly, the Fibonacci numbers $U_n(1, -1)$ have the formula $U_n = \frac{(\frac{1+\sqrt{5}}{2})^n-(\frac{1-\sqrt{5}}{2})^n}{\sqrt{5}}$ and $V_n(1, -1)$ has the formula $V_n = (\frac{1+\sqrt{5}}{2})^n + (\frac{1-\sqrt{5}}{2})^n$

While the formulas for $U_n(1, -1)$ and $V_n(1, -1)$ look more complicated and involve square roots, the terms of the sequences are still integers since the sequences are also recurrence relations.

2 Properties of Lucas Sequences

Next, some facts about $U_n(P,Q)$ will be stated.

1. If n is divisible by m, then $U_n(P,Q)$ is divisible by $U_m(P,Q)$. Thus, $U_n(P,Q)$ is considered a divisibility sequence. This is property $IV.15$ on page 60 of [3]. Therefore, if n is composite, $U_n(P,Q)$ will typically be composite, the exception being the case where $U_m(P,Q)$ equals 1.

To demonstrate a case of this, consider

$$U_6(7,10) = U_6(5+2, 5\cdot 2) = \frac{5^6 - 2^6}{3}.$$

We have

$$\begin{aligned}\frac{5^6 - 2^6}{3} &= \frac{(5^3 - 2^3)(5^3 + 2^3)}{3} = \frac{5^3 - 2^3}{3} \\ &= U_3(5+2, 5\cdot 2)\cdot(5^3 + 2^3) = U_3(7,10)\cdot(5^3 + 2^3).\end{aligned}$$

2. If P is positive, then $U_n(P,Q) = (-1)^{n+1}\cdot U_n(-P,Q)$.

Proof. This will be done by induction. When $n = 0$, $U_n(P,Q) = 0$ and $U_n(-P,Q) = 0$, so $U_n(P,Q) = (-1)^{0+1}U_n(-P,Q)$.
When $n = 1$, $U_n(P,Q) = 1$ and $U_n(-P,Q) = 1$, so $U_n(P,Q) = (-1)^{1+1}U_n(-P,Q)$.
Now, assume that $n \geq 2$ and that the result is true for $1, ..., n-1$.

Then $U_n(P,Q) = P\cdot U_{n-1}(P,Q) - Q\cdot U_{n-2}(P,Q) =$
$(-1)^n P\cdot U_{n-1}(-P,Q) - (-1)^{n-1}Q\cdot U_{n-2}(-P,Q)$ by the inductive hypothesis.

Also, $U_n(-P,Q) = -P\cdot U_{n-1}(P,Q) - Q\cdot U_{n-2}(P,Q)$.

When n is even, $U_n(P,Q)$ equals
$P\cdot U_{n-1}(-P,Q) + Q\cdot U_{n-2}(-P,Q) = (-1)^{n+1}\cdot U_n(-P,Q)$.

When n is odd, $U_n(P,Q)$ equals
$-P\cdot U_{n-1}(-P,Q) - Q\cdot U_{n-2}(-P,Q) = (-1)^{n+1}\cdot U_n(-P,Q)$.

□

As an example, consider $U_n(2,3)$ and $U_n(-2,3)$.

For the first, we have $U_n(2,3)$ is $0,1,2,1,-4,-11,-10,13....$

For the second, we have $U_n(-2,3)$ is $0,1,-2,1,4,-11,10,13,...$

In these sequences, the values are exactly the same if the negative signs are dropped. The significance of this is that $U_n(P,Q)$ and $U_n(-P,Q)$ can be treated as the same sequence for the purposes of primality testing since a negative sign will not change the primality of a number. Therefore, for primality proofs in this paper, P can be assumed to be positive.

3. If a and b are distinct integers that share a common factor, then $U_n(a+b,ab)$ is composite when $n \geq 2$.

Proof. Suppose that a and b share the common factor d. Then a can be written as $a'd$ and b can be written as $b'd$.

Then,

$$\begin{aligned} U_n(a+b,ab) &= \frac{a^n-b^n}{a-b} = \frac{(a'd)^n-(b'd)^n}{a'd-b'd} = \frac{d^n[(a')^n-(b')^n]}{d(a'-b')} \\ &= d^{n-1}\frac{(a')^n-(b')^n}{a'-b'} = d^{n-1}U_n(a'+b',a'b'). \end{aligned}$$

Now d is greater than 1, and $\frac{(a')^n-(b')^n}{a'-b'}$ is greater than 1 when $n \geq 2$ since (a') is greater than (b'). Therefore, $U_n(a,b)$ is composite for $n \geq 2$.

□

The example this time will be $U_n(22,112) = U_n(14+8,14\cdot 8)$.
We have

$$\begin{aligned} U_n(14+8,14\cdot 8) &= \frac{2^n(7^n-4^n)}{6} \\ &= (\frac{2^n}{2})(\frac{7^n-4^n}{3}) \\ &= 2^{n-1}U_n(7+4,7\cdot 4) \\ &= 2^{n-1}U_n(11,28). \end{aligned}$$

4. If a and b are distinct, then $U_n(a+b, ab) = \sum_{i=0}^{n-1} a^{n-i-1}b^i$

Proof. Now, $U_n(a+b, ab) = \frac{a^n - b^n}{a-b}$ and $a^n - b^n$ factors as $(a-b)\sum_{i=0}^{n-1} a^{n-i-1}b^i$, so $\frac{a^n-b^n}{a-b} = \frac{(a-b)\sum_{i=0}^{n-1} a^{n-i-1}b^i}{a-b} = \sum_{i=0}^{n-1} a^{n-i-1}b^i$.

□

5. If m, n, and z are positive integers, $\frac{mn}{z}$ is an integer, and z is less than both m and n, then $\frac{mn}{z}$ is composite.

Proof. Since $\frac{mn}{z}$ is an integer, the prime factors of z must also exist in the numerator of this fraction. m must have a prime factor p that z does not have since otherwise m would be less than or equal to z. Likewise, n must have a prime factor q that z does not have. Therefore, $\frac{mn}{z}$ must have factors p and q, making it composite.

□

We also have the following equality:

6. $U_n(a+b, ab) = aU_{n-1}(a+b, ab) + b^{n-1}$.

Proof. Using the right hand side of the equation,

$$\begin{aligned} aU_{n-1}(a+b, ab) + b^{n-1} &= a\frac{a^{n-1} - b^{n-1}}{a-b} + b^{n-1} \\ &= \frac{a^n - ab^{n-1}}{a-b} + \frac{(a-b)b^{n-1}}{a-b} \\ &= \frac{a^n - ab^{n-1}}{a-b} + \frac{ab^{n-1} - b^n}{a-b} \\ &= \frac{a^n - b^n}{a-b} = U_n(a+b, ab). \end{aligned}$$

□

7. Let d equal $GCD(m, n)$. Then $U_d(P, Q) = GCD(U_m(P, Q), U_n(P, Q))$. This is property $IV.26$ on page 64 of [3].

Property $IV.11$ on page 59 of [3] gives us the following:

8. $U_n(P,Q) = V_{n-1}(P,Q) + QV_{n-3}(P,Q) + Q^2V_{n-5}(P,Q) + ...+$ (last summand),

where the last summand equals $Q^{\frac{n-2}{2}}P$ if n is even,

and $Q^{\frac{n-1}{2}}$ if n is odd.

3 Numerical Investigations

Data was collected on various Lucas sequences to determine the primality of their terms. First, data was collected for the case when a and b are integers. Sequences $U_(a+b, ab)$ that were initially tested were the cases $2 \leq a \leq 100$, $1 \leq b < a$ for $1 \leq n \leq 1000$. The b terms that were tested were always less than a because $\frac{a^n-b^n}{a-b} = \frac{b^n-a^n}{b-a}$, so if b were higher than a, the a and b terms could just be swapped. The testing was done using both the Python and Mathematica programming languages. Both languages had probabilistic primality testing packages that were used. Since there were many sequences to be tested and since $U_n(a+b, ab)$ grows exponentially, the calculation time needed to check the primality of these numbers was significant. To speed up the process, the programs that were written only tested sequences $U_n(a+b, ab)$ where a and b share no common factors since if they did have a common factor, result 3 implies that $U_n(a, b)$ is composite for $n \geq 2$. Similarly, result 1 implies that $U_n(a+b, ab)$ need only be tested for prime values of n since $U_n(a+b, ab)$ will be composite otherwise. There were 3043 values of (a, b) tested and 168 primes for $n < 1000$, so $511,224$ numbers were tested for primality. The data output listed ordered triplets (a, b, n) for which the sequence $U_n(a+b, ab)$ was found to be prime. Using this data, a program was written to determine how many primes were in the sequences $U_n(a+b, ab)$ up to $n = 1000$. Then another program was written to determine for any number x, how many sequences $U_n(a+b, ab)$ had exactly x primes up to $n = 1000$. For example, there were 114 sequences that had no primes up to $n = 1000$, 423 sequences that had 1 prime up to $n = 1000$, and 640 sequences that had 2 primes up to $n = 1000$. Many of the sequences that had no primes up to $n = 1000$ had a and b values that were perfect squares or perfect cubes. This discovery led to the following result.

4 Results

Theorem 1: Consider two integers, call them a and b. If at least one of a and b is greater than 1 in absolute value, a and b are relatively prime, each is a perfect k^{th} power, and k has a prime factor s, then $U_n(a+b, ab)$ is never prime when $n \neq s$.

Proof. We will first assume that k is prime and extend the result to composite k later. Since a and b are perfect k^{th} powers they can be written as $a = x^k$ and $b = y^k$, where x, y, and k are integers.

Then,

$$\begin{aligned} U_n(x^k + y^k, x^k y^k) &= \frac{x^{kn} - y^{kn}}{x^k - y^k} \\ &= \frac{(x^n)^k - (y^n)^k}{x^k - y^k} \\ &= \frac{(x^n - y^n)\sum_{i=0}^{k-1}(x^n)^{k-i-1}(y^n)^i}{x^k - y^k} \\ &= \frac{\frac{x^n - y^n}{x-y}\sum_{i=0}^{k-1}(x^n)^{k-i-1}(y^n)^i}{\frac{x^k - y^k}{x-y}}. \end{aligned}$$

This last expression is equal to $\frac{\sum_{i=0}^{n-1} x^{n-i-1}y^i \sum_{i=0}^{k-1}(x^n)^{k-i-1}(y^n)^i}{\sum_{i=0}^{k-1} x^{k-i-1}y^i}$ by result 4 and is also equal to $\frac{U_n(x+y,xy)U_k(x^n+y^n,x^ny^n)}{U_k(x+y,xy)}$.

When a and b are both positive integers, then x and y are both positive integers. Then $\sum_{i=0}^{k-1} x^{k-i-1}y^i$ is less than $\sum_{i=0}^{k-1}(x^n)^{k-i-1}(y^n)^i$, or equivalently, $U_k(x+y, xy) < U_k(x^n + y^n, x^n y^n)$. By result 7, $GCD(U_k(x+y, xy), U_n(x+y, xy)) = U_{GCD(k,n)}(x+y, xy)$. Since k is prime and $n \neq k$, $U_{GCD(k,n)}(x+y, xy) = U_1(x+y, xy) = 1$. Thus, $U_k(x+y, xy)$ must divide $U_k(x^n + y^n, x^n y^n)$, making $U_n(x^k + y^k, x^k y^k)$ composite by result 5. When a and b are negative, then x and y must be negative. Then x and y can be written as $x = -x'$ and $y = -y'$, where x' and y' are positive integers. With

this substitution,

$$\begin{aligned} U_n(x^k+y^k, x^ky^k) &= \frac{(-x')^{kn}-(-y')^{kn}}{(-x')^k-(-y')^k} \\ &= \frac{(-1)^{kn}}{(-1)^k}\cdot\frac{(x')^{kn}-(y')^{kn}}{(x')^k-(y')^k} \\ &= |\frac{(x')^{kn}-(y')^{kn}}{(x')^k-(y')^k}|, \end{aligned}$$

meaning $U_n(x^k+y^k, x^ky^k)$ is composite since we have already determined that $|\frac{(x')^{kn}-(y')^{kn}}{(x')^k-(y')^k}| = |U_n((x')^k+(y')^k, (x')^k(y')^k)|$ is composite.

Now, consider when one of a and b is positive and the other is negative. Then $Q = ab$ is negative.

In this case, consider when P is positive. Now, $U_n(a+b, ab) = P\cdot U_{n-1}(a+b, ab) - Q\cdot U_{n-2}(a+b, ab)$. Since $U_0(a+b, ab) = 0$, $U_1(a+b, ab) = 1$, P is positive, and Q is negative, it follows inductively that $U_n(a+b, ab)$ is a strictly increasing sequence for $n \geq 2$. For negative P, $U_n(a+b, ab)$ is strictly increasing in absolute value by result 2.

Now, again consider when P is positive, and also consider the number $\frac{U_k(x^n+y^n, x^ny^n)}{U_k(x+y, xy)}$. This is equal to $\frac{\frac{x^{nk}-y^{nk}}{x^n-y^n}}{\frac{x^k-y^k}{x-y}} = \frac{\frac{x^{nk}-y^{nk}}{x^k-y^k}}{\frac{x^n-y^n}{x-y}} = \frac{U_n(x^k+y^k, x^ky^k)}{U_n(x+y, xy)}$. We are dealing with the case when P is positive and exactly one of a and b is negative. Without loss of generality, assume a is the positive number. Then $a > |b|$ since P is positive, and so $x > |y|$. Since $x > |y|$, $x^k + y^k > x + y$. Also, $|x^ky^k|$ is greater than $|xy|$.

Now, $U_2(x^k+y^k, x^ky^k) = x^k+y^k$ is greater than $U_2(x+y, xy) = x+y$. This handles the base case.

Assume that $U_m(x^k+y^k, x^ky^k)$ is greater than $U_m(x+y, xy)$ for all m such that $2 \leq m < n$.

Then $U_n(x^k+y^k, x^ky^k) = (x^k+y^k)\cdot U_{n-1}(x^k+y^k, x^ky^k) - x^ky^k\cdot U_{n-2}(x^k+y^k, x^ky^k)$ is greater than $U_n(x+y, xy) = (x+y)\cdot U_{n-1}(x+y, xy) - xy\cdot U_{n-2}(x+y, xy)$.
Thus by induction, $U_n(x^k+y^k, x^ky^k) > U_n(x+y, xy)$ for $n \geq 2$. When $n \geq k$, $U_k(x+y, xy)$ is less than both $U_n(x+y, xy)$ and $U_k(x^n+y^n, x^ny^n)$,
so $U_n(x^k+y^k, x^ky^k)$ is composite by result 5.

When P is negative, $|U_k(x+y,xy)|$ is smaller than $|U_n(x+y,xy)|$ and $|U_k(x^n+y^n,x^ny^n)|$ by result 2, so $U_n(x^k+y^k,x^ky^k)$ is still composite.

Now, consider the case when $n \leq k$. Again, we know that $U_n(x^k+y^k,x^ky^k) = \frac{U_n(x+y,xy)U_k(x^n+y^n,x^ny^n)}{U_k(x+y,xy)}$. Also, $GCD(U_k(x+y,xy),U_n(x+y,xy)) = 1$ by result 7, so $U_k(x+y,xy)$ must divide $U_k(x^n+y^n,x^ny^n)$. Since $U_k(x+y,xy)$ is smaller than $U_k(x^n+y^n,x^ny^n)$, $U_n(x^k+y^k,x^ky^k)$ is composite by result 5.

Now, suppose that k is composite. Then $k = st$, where s and t are integers and s is prime.

Then,

$$\begin{aligned}
U_n(x^k+y^k,x^ky^k) &= \frac{x^{kn}-y^{kn}}{x^k-y^k} \\
&= \frac{x^{stn}-y^{stn}}{x^{st}-y^{st}} \\
&= \frac{(x^{tn})^s-(y^{tn})^s}{x^{st}-y^{st}} \\
&= \frac{(x^{tn}-y^{tn})\sum_{i=0}^{s-1}(x^{tn})^{s-i-1}(y^{tn})^i}{x^{st}-y^{st}} \\
&= \frac{\frac{x^{tn}-y^{tn}}{x^t-y^t}\sum_{i=0}^{s-1}(x^{tn})^{s-i-1}(y^{tn})^i}{\frac{x^{st}-y^{st}}{x^t-y^t}} \\
&= \frac{U_n(x^t+y^t,x^ty^t)U_s(x^{tn}+y^{tn},x^{tn}y^{tn})}{U_s(x^t+y^t,x^ty^t)}.
\end{aligned}$$

When $n \neq s$, $GCD(U_s(x^t+y^t,x^ty^t),U_n(x^t+y^t,x^ty^t)) = 1$. Then $U_s(x^t+y^t,x^ty^t)$ must divide $U_s(x^{tn}+y^{tn},x^{tn}y^{tn})$. Since $U_s(x^t+y^t,x^ty^t)$ is smaller than $U_s(x^{tn}+y^{tn},x^{tn}y^{tn})$, $U_n(x^k+y^k,x^ky^k)$ is composite. This completes the proof of Theorem 1.

□

From Theorem 1, a few more facts can be observed.

1.1 If k is prime, then $U_n(a+b,ab)$ is never prime for $n \neq k$.

1.2 If k has two distinct factors s and t, then $U_n(a+b,ab)$ is never prime.

1.3 For $U_n(a+b, ab)$ to ever be prime, k must equal s^r, where r is a positive integer.

1.4 $U_n(a+b, ab)$ can be prime at most once.

Data was also collected for the general case $U_n(P, Q)$, where a and b need not be integers. The ranges on P and Q were $1 \leq P \leq 100$, $-100 \leq Q \leq 100$. Note that P is restricted to non-negative values because of result 2. Similar to the case where a and b have a common factor, if P and Q have a common factor, then $U_n(P, Q)$ will be composite for sufficiently large n. Therefore, $U_n(P, Q)$ was only tested for primality for P and Q without a common factor, and it again only needed to be tested for prime n as well. There were $12,175$ pairs (P, Q), leading to $2,045,400$ primality tests. In this case, there were 658 sequences with no primes up to $n = 1000$. The pairs of (P, Q) that had no primes up to $n = 1000$ had many cases where Q is a square. This suggests that $U_n(P, Q)$ can only be prime for a small number of n values.

To show that this is true, the identity $U_{m+n} = U_m U_{n+1} - QU_{m-1}U_n$ was used. This is property $IV.4$ on page 57 of [3].
Then,

$$\begin{aligned} U_{2n+1} &= U_{(n+1)+n} \\ &= U_{n+1}U_{n+1} - QU_{(n+1)-1}U_n \\ &= U_{n+1}U_{n+1} - QU_nU_n \\ &= U_{n+1}^2 - QU_n^2 \\ &= (U_{n+1} - U_n\sqrt{Q})(U_{n+1} + U_n\sqrt{Q}). \end{aligned}$$

Then when both $(U_{n+1} - \sqrt{Q})$ and $(U_{n+1} + \sqrt{Q})$ are larger than 1, $U_{2n+1}(P, Q)$ is composite. Therefore, the only case where U_{2n+1} can possibly be prime is when one of these factors equals 1.

For any Lucas sequence $U_n(P, Q) = U_n(a+b, ab)$, if k is a positive integer, $a^k + b^k$ and $a^k b^k$ are also integers. Note that $a^k + b^k$ is an integer because it the number $V_k(a+b, ab)$ and $a^k b^k$ is an integer because $a^k b^k = (ab)^k = Q^k$. Then $U_n(a^k+b^k, a^k b^k)$ is a Lucas sequence. Using the same factorizations as the ones used for the proof of Theorem 1, $U_n(a^k + b^k, a^k b^k) = \frac{U_n(a+b,ab)U_k(a^n+b^n,a^n b^n)}{U_k(a+b,ab)}$.

If $U_k(a+b, ab)$ is less than both $U_n(a+b, ab)$ and $U_k(a^n + b^n, a^n b^n)$, then $U_n(a^k + b^k, a^k b^k)$ is composite by result 5. In order to show this, it was necessary to show that $U_n(a+b, ab)$ is an increasing sequence in n and $U_k(a^n+b^n, a^n b^n)$ is an increasing sequence in n. Then when $k < n$, $U_k(a+b, ab)$ is less than both $U_n(a+b, ab)$ and

$U_k(a^n+b^n, a^nb^n)$. In the case where a and b are real numbers, these facts were shown to be true. The result is not generally true when a and b are complex numbers. These proofs will be given with the aid of the following lemmas. In all of these lemmas, it is assumed that a and b are real.

Lemma 1: If P and Q are relatively prime, $P > 0$, $Q \neq 0$, and it is not the case that $P = 2$ and $Q = 1$, then $a \geq 1 + |b|$. In particular, $a > 1$.

Proof. Since $Q \neq 0$, $b \neq 0$. If $b > 0$, then $a - b = \frac{P+\sqrt{P^2-4Q}}{2} - \frac{P-\sqrt{P^2-4Q}}{2} = \sqrt{P^2-4Q}$. Since P and Q are relatively prime and since it is not simultaneously true that $P = 2$ and $Q = 1$, $P^2 - 4Q \neq 0$. Therefore, $a - b = \sqrt{P^2-4Q} \geq 1$, and so $a \geq 1 + |b|$. If $b < 0$, then $|b| = \frac{-P+\sqrt{P^2-4Q}}{2}$, so that $a - |b| = \frac{P+\sqrt{P^2-4Q}}{2} - \frac{-P+\sqrt{P^2-4Q}}{2} = P \geq 1$. Thus, $a \geq 1 + |b|$.

□

Lemma 2: If P and Q are relatively prime, $P > 0$, and $Q \neq 0$, then $U_n(P, Q)$ is a strictly increasing sequence for $n \geq 2$.

Proof. When $b > 0$, by result 6, for all $n \geq 1$, we have $U_n(a + b, ab) > aU_{n-1}(a + b, ab) > U_{n-1}(a + b, ab)$.

If $b < 0$, then $Q < 0$. Then from the equation $U_n(P, Q) = P \cdot U_{n-1}(P, Q) - Q \cdot U_{n-2}(P, Q)$, it is evident that $U_n(P, Q) > P \cdot U_{n-1}(P, Q)$, so $U_n(P, Q)$ is increasing for $n \geq 2$.

□

Lemma 3: If P and Q are relatively prime, $P > 0$, and $Q \neq 0$, then $V_n(P, Q)$ is a strictly increasing sequence for $n \geq 2$.

Proof. We have

$$\begin{aligned} V_n(a + b, ab) - V_{n-1}(a + b, ab) &= (a^n + b^n) - (a^{n-1} + b^{n-1}) \\ &= (a^n - a^{n-1}) + (b^n - b^{n-1}) \\ &= a^{n-1}(a - 1) + b^{n-1}(b - 1), \end{aligned}$$

which is greater than or equal to $(|b|+1)^{n-1}|b|+b-b^{n-1}$ by Lemma 1.
This in turn is greater than or equal to

$$\begin{aligned}((n-1)|b|^{n-2}+1)|b|+b-b^{n-1} &= (n-1)|b|^{n-1}-b^{n-1}+|b|+b \\ &\geq (n-2)|b|^{n-1}+|b|+b>0\end{aligned}$$

for $n \geq 2$.

□

Lemma 4: If $b>0$, then $U_k(a^n+b^n, a^nb^n) > U_k(a^{n-1}+b^{n-1}, a^{n-1}b^{n-1})$.

Proof. Since $b>0$, we have $Q>0$, meaning $Q \geq 1$. Thus $Q^i \geq Q^j$ for all $i>j$.
Also, $V_k(a^n+b^n, a^nb^n) = V_{kn}(a+b, ab) > V_{kn-k}(a+b, ab) = V_k(a^{n-1}+b^{n-1}, a^{n-1}b^{n-1})$ by Lemma 3.
Using result 8, we have $U_k(a^n+b^n, a^nb^n) = V_{k-1}(a^n+b^n, a^nb^n) + Q^nV_{k-3}(a^n+b^n, a^nb^n) + Q^{2n}V_{k-5}(a^n+b^n, a^nb^n) + ...$
This is greater than $V_{k-1}(a^{n-1}+b^{n-1}, a^{n-1}b^{n-1}) + Q^{n-1}V_{k-3}(a^{n-1}+b^{n-1}, a^{n-1}b^{n-1}) + Q^{2n-2}V_{k-5}(a^{n-1}+b^{n-1}, a^{n-1}b^{n-1}) + ...$, which equals $U_k(a^{n-1}+b^{n-1}, a^{n-1}b^{n-1})$.

□

Lemma 5: If n is even, then $U_k(a^n+b^n, a^nb^n) > U_k(a^m+b^m, a^mb^m)$ for all $0<m<n$.

Proof. By result 8,
we have that $U_k(a^m+b^m, a^mb^m)$ equals

$$V_{k-1}(a^m+b^m, a^mb^m) + Q^mV_{k-3}(a^m+b^m, a^mb^m) + Q^{2m}V_{k-5}(a^m+b^m, a^mb^m) + ... \leq$$

$$V_{k-1}(a^m+b^m, a^mb^m) + |Q|^mV_{k-3}(a^m+b^m, a^mb^m) + |Q|^{2m}V_{k-5}(a^m+b^m, a^mb^m) + ... <$$

$$V_{k-1}(a^n+b^n, a^nb^n) + |Q|^nV_{k-3}(a^n+b^n, a^nb^n) + |Q|^{2n}V_{k-5}(a^n+b^n, a^nb^n) + ... =$$

$$V_{k-1}(a^n+b^n, a^nb^n) + Q^nV_{k-3}(a^n+b^n, a^nb^n) + Q^{2n}V_{k-5}(a^n+b^n, a^nb^n) + ... =$$

$$U_k(a^n+b^n, a^nb^n).$$

□

Lemma 6: If $n>1$ and $k>1$, then $U_k(a^n+b^n, a^nb^n) > U_k(a^m+b^m, a^mb^m)$ for all $0<m<n$.

Proof. We have shown this for $b > 0$ and for even n, so suppose n is odd and $b < 0$. Then $Q < 0$ as well. The proof will follow by induction on k.
When $k = 0$, $U_k(a^n + b^n, a^n b^n) = 0 = U_k(a + b, ab)$ and when $k = 1$,
$U_k(a^n + b^n, a^n b^n) = 1 = U_k(a + b, ab)$.

Moreover, when $k = 2$, $U_k(a^n + b^n, a^n b^n) = a^n + b^n > a + b = U_k(a + b, ab)$.

Assuming that $U_m(a^n + b^n, a^n b^n) > U_m(a^{n-1} + b^{n-1}, a^{n-1} b^{n-1})$ for all m with $2 \leq m \leq k - 1$, we have

$$U_k(a^n + b^n, a^n b^n) = (a^n + b^n)U_{k-1}(a^n + b^n, a^n b^n) - a^n b^n U_{k-2}(a^n + b^n, a^n b^n)$$

$$= V_n(a + b, ab)U_{k-1}(a^n + b^n, a^n b^n) - Q^n U_{k-2}(a^n + b^n, a^n b^n)$$

$$= V_n(a + b, ab)U_{k-1}(a^n + b^n, a^n b^n) + |Q|^n U_{k-2}(a^n + b^n, a^n b^n)$$

$$> V_{n-1}(a + b, ab)U_{k-1}(a^{n-1} + b^{n-1}, a^{n-1} b^{n-1}) + |Q|^{n-1} U_{k-2}(a^{n-1} + b^{n-1}, a^{n-1} b^{n-1})$$

$$> V_{n-1}(a + b, ab)U_{k-1}(a^{n-1} + b^{n-1}, a^{n-1} b^{n-1}) + Q^{n-1} U_{k-2}(a^{n-1} + b^{n-1}, a^{n-1} b^{n-1})$$

$$= U_k(a^{n-1} + b^{n-1}, a^{n-1} b^{n-1}).$$

□

Theorem 2: If a and b are the solutions to the characteristic equation for $U_n(P, Q)$, a and b are real, and k is a positive integer with s as a factor, then $U_n(a^k + b^k, a^k b^k)$ can only be prime for $n = s$.

Proof. Using the same factorizations as the ones at the beginning of the proof of Theorem 1, $U_n(a^k + b^k, a^k b^k)$ is equal to $\frac{U_n(a+b,ab)U_k(a^n+b^n,a^n b^n)}{U_k(a+b,ab)}$.

Suppose that $k < n$. Then by Lemma 2, $U_k(a + b, ab) < U_n(a + b, ab)$.
By Lemma 6, $U_k(a + b, ab) < U_k(a^n + b^n, a^n b^n)$.
Thus, $U_n(a^k + b^k, a^k b^k)$ is composite by result 5.

Suppose that $k \geq n$. The proof that $U_n(a^k + b^k, a^k b^k)$ is composite when $n \neq s$ is the same as the proof of the case where $k \geq n$ and $n \neq s$ in Theorem 1.

□

Notice that Theorem 2 is a generalization of Theorem 1, with the difference being that a and b were required to be integers in Theorem 1.

Theorem 3: When Q is a square and a and b are real numbers, then $U_n(P,Q)$ can only be prime when $n = 2$.

Proof. We have the formula

$$\begin{aligned} U_{2n+1}(P,Q) &= U_{n+1}^2(P,Q) - QU_n^2(P,Q) \\ &= (U_{n+1}(P,Q) - \sqrt{Q}U_n(P,Q))(U_{n+1}(P,Q) + \sqrt{Q}U_n(P,Q)). \end{aligned}$$

If both of these factors are integers greater than 1, then U_{2n+1} is composite.
Since Q is a square, $\sqrt{Q}$ is an integer.
Then since U_n, U_{n+1}, and $\sqrt{Q}$ are all integers,
both of the factors are integers as well.
Since Q is a square, $\sqrt{Q} \geq 1$.
For $n \geq 1$, $U_n(P,Q) \geq 1$ and $U_{n+1}(P,Q) \geq 1$.
Thus, both terms $U_{n+1}(P,Q)$ and $\sqrt{Q}U_n(P,Q)$ are at least 1,
so $(U_{n+1}(P,Q) + \sqrt{Q}U_n(P,Q)) \geq 2$.

We are assuming a and b are real. Thus, $P^2 - 4Q > 0$. Factoring this, we have $(P - 2\sqrt{Q})(P + 2\sqrt{Q}) > 0$. The second term is positive, so the first term must be as well. That is, $P > 2\sqrt{Q}$. As a result, $P \geq 3$. Since $P = a + b$ and $Q = ab$, $P - 2\sqrt{Q} = a - 2\sqrt{a}\sqrt{b} + b = (\sqrt{a} - \sqrt{b})^2$. Thus, $(\sqrt{a} - \sqrt{b})^2 \geq 1$ and $\sqrt{a} > \sqrt{b}$, so $\sqrt{a} - \sqrt{b} \geq 1$.

The sequence $U_n(P,Q)$ has the first terms $0, 1, P, P^2 - Q, ...$
From this, we can see that $U_2(P,Q)$ is prime if and only if P is prime.

Also, $U_3(P,Q) = P^2 - Q = (P - \sqrt{Q})(P + \sqrt{Q})$.

Since $P \geq 3$ and $\sqrt{Q} \geq 1$, $P + \sqrt{Q} \geq 4$.

Also, $P - \sqrt{Q} > 2\sqrt{Q} - \sqrt{Q} = \sqrt{Q} \geq 1$.

Therefore, $P - \sqrt{Q} > 1$. As such, $U_3(P,Q)$ cannot be prime.

For prime $n > 3$, $n = 2k + 1$, where k is an integer, so $U_p(P,Q) = (U_{k+1}(P,Q) - \sqrt{Q}U_k(P,Q))(U_{k+1}(P,Q) + \sqrt{Q}U_k(P,Q))$ with $k \geq 2$. The second term is larger than 1, so what is left to be shown is that the first term is also larger than 1. Using the

formula $U_{k+1}(P,Q) = aU_k(P,Q) + b^k$, we have

$$\begin{aligned} U_{k+1}(P,Q) - \sqrt{Q}U_k(P,Q) &= aU_k(P,Q) + b^k - \sqrt{a}\sqrt{b}U_k(P,Q) \\ &= \sqrt{a}U_k(P,Q)(\sqrt{a} - \sqrt{b}) + b^k. \end{aligned}$$

Since $\sqrt{a} > 1$, $\sqrt{a} - \sqrt{b} \geq 1$, and $U_k(P,Q) \geq U_2(P,Q) = P \geq 3$,
we have that $U_{k+1}(P,Q) - \sqrt{Q}U_k(P,Q) > 3 + b^k$. In particular, it is an integer larger than 2.

If n is not prime, say $n = pk$ for some prime p and $k > 1$, then $U_n(P,Q)$ is divisible by $U_p(P,Q)$ by result 1. Therefore, $U_n(P,Q)$ is composite.

□

While Theorems 2 and 3 required a and b to be real numbers, it is likely that they hold true for complex numbers as well. However, this could not be shown over the course of the project. The difficulty with a and b being complex is that $U_n(a+b, ab)$ and $U_k(a^n + b, a^n b^n)$ are not necessarily increasing in n. However, it seems to be the case that the general trend in these sequences is that they increase in absolute value as n increases, even though it may not be true on a term to term basis. Further exploration may result in a modification of Theorems 2 and 3 that do not require a and b to be real.

5 Possibilities for Future Work

There were many Lucas sequences $U_n(P,Q)$ that produced no primes up to $n = 1000$ that could not be explained by the theorems in this paper. Since there were many sequences tested, it could just be the case that one would expect some of these sequences to produce no primes up to $n = 1000$, but to later produce a prime for a large enough value of n. However, it also may be that there are some underlying reasons for the compositeness of these sequences. If this is the case, perhaps future analysis could discover why this occurs.

References:

[1] Caldwell, C. K. *How Many Primes Are There?* Retrieved from https://primes.utm.edu/howmany

[2] *Great Internet Mersenne Prime Search.* Retrieved from https://www.mersenne.org/

[3] Ribenboim, P. (1988) *The New Book of Prime Number Records.*
New York, New York: Springer-Verlag New York, Inc.

[4] Riesel, H. (1994) *Prime Numbers and Computer Methods for Factorization.*
Boston, Massachusetts: Birkhäuser.