An Investigation of Lucas Sequences: Progress Report

January 1, 2018

1 Introduction

Definition 1 *The two Lucas sequences, V_n and U_n, are defined as $V_0 = 2$, $V_1 = P$, $V_{n+1} = PV_n - QV_{n-1}$ and $U_0 = 0$, $U_1 = 1$, and $U_{n+1} = PU_n - QU_{n-1}$.*

There are interesting connections between linear recurrence equations, trigonometric functions, and solutions of the Pellian equation, $x^2 - Dy^2 = r^2$. For a specific example, consider the rotation matrix $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$. By defining $c_n = \cos(n\theta)$ and $s_n = \sin(n\theta)$, we can show that

$$\begin{pmatrix} c_{n+1} \\ s_{n+1} \end{pmatrix} = 2c_1 \begin{pmatrix} c_n \\ s_n \end{pmatrix} - \begin{pmatrix} c_{n-1} \\ s_{n-1} \end{pmatrix}$$

which satisfies the recurrence relation of the Lucas Sequences V and U with $P = 2\cos\theta$ and $Q = 1$. Additionally, (c_n, s_n) is a solution of $x^2 - Dy^2 = 1$ when $D = -1$. We will explore these connections further below.

2 The Equation $x^2 - Dy^2 = r^2$

Suppose $X, Y \in \mathbb{R}$ such that $X^2 - DY^2 = r^2$. Defining the sequences

$$x_n = \frac{r}{2}\left(\left(\frac{X}{r} + \sqrt{D}\frac{Y}{r}\right)^n + \left(\frac{X}{r} - \sqrt{D}\frac{Y}{r}\right)^n\right)$$

and

$$y_n = \frac{r}{2\sqrt{D}}\left(\left(\frac{X}{r} + \sqrt{D}\frac{Y}{r}\right)^n - \left(\frac{X}{r} - \sqrt{D}\frac{Y}{r}\right)^n\right)$$

and using quite a bit of algebraic manipulation, we obtain the recurrence relations

$$x_{n+k} + \sqrt{D}y_{n+k} = \frac{1}{r}\left((x_n x_k + Dy_n y_k) + \sqrt{D}(x_n y_k + y_n x_k)\right) \tag{1}$$

and

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} + \begin{pmatrix} x_{n-1} \\ y_{n-1} \end{pmatrix} = \frac{2X}{r}\begin{pmatrix} x_n \\ y_n \end{pmatrix} \tag{2}$$

as well as $x_{-k} = x_k$ and $y_{-k} = -y_k$.

By expanding x_n and y_n using the bionomial theorem and simplifying, we can define them in a way that doesn't require us to assume $2, D \in R^\times$ and that $\sqrt{D} \in R$, which we assumed in the original definitions.

Also, each x_n and y_n satisfy the Pellian equation, meaning we can generate an arbitary number of solutions from a single solution.

3 Groups of the Form $\{(x, y) : x^2 - Dy^2 = r^2\}$

We can define a group $G = \{(x_n, y_n) : n \in \mathbb{Z}\}$ with the binary operation given by

$$(x_k, y_k) * (x_l, y_l) = \left(\frac{1}{r}(x_k x_l + D y_k y_l), \frac{1}{r}(x_k y_l + y_k x_l)\right)$$

This turns out to be (x_{k+l}, y_{k+l}) by equation (1). This group is abelian with identity x_0, y_0; this means given two solutions of the Pellian equation, we can generate a third (as long as the two solutions were generated by the same solution X, Y). This motivates us to extend the definition of $*$ to larger sets.

Definition 2 *Let R be a commutative ring with identity and let $r, D \in R$. Let $\mathcal{L}_R = \{(x, y) \in R \times R : x^2 - Dy^2 = r^2\}$.*

We can then define a binary operation $*$ on $\mathcal{L}$ by $(x, y) * (x', y') = (r^{-1}(xx' + Dyy'), r^{-1}(xy' + x'y))$. Then, $(\mathcal{L}_R, *)$ is an abelian group with identity $(r, 0)$. We can prove associativity by associating each term with a two by two matrix with determinant r^2.

Now, we consider two specific group, $\mathcal{L}_\mathbb{Z}$ and $\mathcal{L}_{\mathbb{F}_q}$, which we can state several theorems about.

Theorem 1 *If $D \in \mathbb{Z}$ is not a square and $r = 1$, then $\mathcal{L}_\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$.*

First, we can simplify the problem by noting that for all $(a, b) \in \mathcal{L}$, $(a, b) = (-1, 0) * (-a, b)$. Also, $(-1, 0) * (-1, 0) = (1, 0)$ which is the identity, so we can express all elements of $\mathcal{L}$ in the form $(-1, 0)^i * (|a|, b)$, where $i = 0$ if $a > 0$ and $i = 1$ if $a < 0$. Because $\{(-1, 0)^n\} \cong \mathbb{Z}_2$, we must now show that $\mathcal{L}' = \{(x, y) \in \mathcal{L} : x > 0\} \cong \mathbb{Z}$. We show this in two parts: (a) $\mathcal{L}' \cong \mathbb{Z}$ if $\mathcal{L}' \backslash \{(1, 0)\}$ is nonempty and (b) $\mathcal{L}' \backslash \{(1, 0)\}$ is nonempty.

We will first prove a lemma that will be useful for both parts of the main proof:

Lemma 1 *For $a, b, x, y, r \in \mathbb{N}$ such that $a^2 - Db^2 = x^2 - Dy^2 = r^2$, $r < x < a$, and $0 < y < b$, we have $0 < ax - Dby$ and $0 < bx - ay < br$.*

Proof: We have the inequalities

$$\frac{a}{\sqrt{D}b} = \sqrt{\frac{a^2}{Db^2}} = \sqrt{1 + \frac{r^2}{Db^2}} > 1$$

and

$$\frac{x}{\sqrt{D}y} = \sqrt{\frac{x^2}{Dy^2}} = \sqrt{1 + \frac{r^2}{Dy^2}} > 1$$

which imply $\frac{ax}{Dby} > 1 \implies ax - Dby > 0$. To prove $0 < bx - ay$, note that

$$\frac{a^2}{b^2} = D + \frac{r^2}{b^2} < D + \frac{r^2}{y^2} = \frac{x^2}{y^2} \implies bx - ay > 0$$

Now, to prove the final part of the lemma, that $bx - ay < br$, we will proceed via proof by contradiction. Assume $br \leq bx - ay$. Then

$$\begin{aligned} b(x-r) &\geq ay > 0 \\ b^2(x^2 - 2xr + r^2) &\geq a^2y^2 \\ b^2(Dy^2 + r^2 - 2xr + r^2) &\geq (Db^2 + r^2)y^2 \\ b^2(2r^2 - 2xr) &\geq r^2y^2 \\ 2rb^2(r-x) &\geq r^2y^2 > 0 \end{aligned}$$

However, we know $r - x < 0$ by our earlier definition, and clearly $2rb^2 > 0$, so their product is negative, and we have reached a contradiction. Thus, $bx - ay < br$.

Now, we will prove a. We will show that $\mathcal{L}' = \{(x_n, y_n)\}$, using the definitions of x_n, y_n as found in section 2, and choosing $(X, Y) \in \mathcal{L}' \setminus (1, 0)$ such that $Y > 0$ and Y is minimal. This suffices to prove an isomorphism between $\mathcal{L}'$ and $\mathbb{Z}$ because $\{(x_n, y_n)\} \cong \mathbb{Z}$ as long as $(X, Y) \neq (1, 0)$, and we have excluded $(1, 0)$.

Choose $(a, b) \in \mathcal{L}'$ such that $(a, b) \notin \{(x_n, y_n)\}$ and b is positive and minimal. As $y_0 = 0 < b$ and $\{y_n\}$ is an increasing sequence, there exists some k such that $y_k < b < y_{k+1}$. Now consider the product

$$(a, b) * (x_k, -y_k) = (ax_k - Dby_k, bx_k - ay_k)$$

By the lemma we proved earlier, $ax_k - Dby_k$ and $bx_k - ay_k$ are both positive, and they are both also not in the sequences $\{x_n\}$ and $\{y_n\}$, as otherwise that would imply $(a, b) \in \{(x_n, y_n)\}$. Thus, $bx_k - ay_k$ contradicts the minimality of b, and we are done.

Now, to prove part b, that there exists some pair (a, b) in $\mathcal{L}' \setminus (1, 0)$, we observe that there exist infinitely many coprime pairs (x, y) that satisfy

$$|\frac{x}{y} - \sqrt{D}| < \frac{1}{y^2}$$

Now, if $\frac{x}{y} < \sqrt{D}$, we have $|x + \sqrt{D}y < 2\sqrt{D}y|$, which implies

$$|x^2 - Dy^2| = |x - \sqrt{D}y||x + \sqrt{D}y| < \frac{1}{y} 2sqrtDy = 2\sqrt{D}$$

Next, if $\frac{x}{y} > \sqrt{D}$, we have $|x + \sqrt{D}y| < 2x$, which implies

$$|x^2 - Dy^2| = |x - \sqrt{D}y||x + \sqrt{D}y| < \frac{1}{y} 2x = 2\frac{x}{y} < 2\left(\sqrt{D} + \frac{1}{y^2}\right) \leq 2(\sqrt{D} + 1)$$

Thus, in both cases, $|x^2 - Dy^2| < 2\sqrt{D} + 2$, so we can construct the infinite set

$$\{(x, y) \in \mathbb{N} \times \mathbb{N} : |x^2 - Dy^2| < 2\sqrt{D} + 2\}$$

Because there are finitely many integers in the interval $(-2\sqrt{D} - 2, 2\sqrt{D} + 2)$ but our set is infinite, there must be some m such that $|m| < 2\sqrt{D} + 2$ such that

$$\{(x, y) \in \mathbb{N} \times \mathbb{N} : x^2 - Dy^2 = m\}$$

is also an infinite set. If we partition the set into equivalence classes such that $(x, y) \sim (x', y')$ if and only if $x \equiv x' \mod m$ and $y \equiv y' \mod m$, because there are finitely many equivalence classes, there must be some distinct pairs (a_1, b_1) and (a_2, b_2) that satisfy $a_1^2 - Db_1^2 = a_2^2 - Db_2^2 = m$ and $a_1 - a_2 \equiv b_1 - b_2 \equiv 0 \mod m$. This implies $a_1a_2 - Db_1b_2 \equiv a_1^2 - Db_1^2 \equiv 0 \mod m$ and $a_1b_2 - b_1a_2 \equiv a_1b_1 - b_1a_1 = 0 \mod m$. Thus, we know that we can define $x' = \frac{1}{m}(a_1a_2 - Db_1b_2)$ and $y' = \frac{1}{m}(a_1b_2 - b_1a_2)$ such that both x' and y' are integers. Without loss of generality, $a_1 < a_2$, which implies $b_1 < b_2$, so we can apply the lemma we derived ealier to show that x' and y' are both positive. Thus, it remains to show that $(x')^2 - D(y')^2 = 1$, but that is simply a matter of algebraic manipulation:

$$\begin{aligned}(x')^2 - D(y')^2 &= \frac{1}{r^2}((a_1^2a_2^2 - 2Da_1a_2b_1b_2 + D^2b_1^2b_2^2) - D(a_1^2b_2^2 - 2a_1a_2b_1b_2 + b_1^2a_2^2)) \\ &= \frac{1}{r^2}(a_2^2(a_1^2 - Db_1^2) - Db_2^2(a_1^2 - Db_1^2)) \\ &= \frac{1}{r^2}(m(a_2^2 - Db_2^2)) \\ &= 1\end{aligned}$$

Theorem 2 *The group $\mathcal{L}_{\mathbb{F}_q}$, with q an odd prime, has order $q - \left(\frac{D}{q}\right)$, where $\left(\frac{D}{q}\right)$ is the the Legendre symbol.*

Proof: We proceed by casework. For the first case, let $\left(\frac{D}{q}\right) = 1$. Then we can define $d \in \mathbb{F}_q$, $d^2 = D$. To find the order of $\mathcal{L}_{\mathbb{F}_q}$, we will prove an isomorphism between $\mathcal{L}$ and

$$\mathcal{H} := \{(a, b) \in \mathbb{F}_q^\times \times \mathbb{F}_q^\times : ab = 1\}$$

Now, consider the map $\rho : (x, y) \to (x + dy, x - dy)$. We will show that this map is a bijection between $\mathcal{L}$ and $\mathcal{H}$. First, to show that $\rho : \mathcal{L} \to \mathcal{H}$, note that if $(x, y) \in \mathcal{L}$, we have $(x + dy)(x - dy) = x^2 - Dy^2 = 1$. Next, we will show surjectivity. Notice that $\frac{a+b}{2} + d\frac{a-b}{2d} = a$ and $\frac{a+b}{2} - d\frac{a-b}{2d} = b$. This motivates us to let $(a, b) \in \mathcal{H}$ and attempt to prove that $(x, y) = (\frac{a+b}{2}, \frac{a-b}{2d})$ is in $\mathcal{L}$. However, this is true, because

$$x^2 - Dy^2 = \frac{(a+b)^2}{4} - D\frac{(a-b)^2}{4D} = \frac{4ab}{4} = 1$$

so ρ is surjective. Finally, we will show injectivity. Let $(x, y), (x', y') \in \mathcal{L}$. Then $x + dy = x' + dy'$ and $x - dy = x' - dy'$ imply $x = x'$ and $y = y'$, so ρ is injective. Thus,

$$|\mathcal{L}| = |\mathcal{H}| = |\mathbb{F}_q^\times| = q - 1 = q - \left(\frac{D}{q}\right)$$

For the second case, assume that $\left(\frac{D}{q}\right) = -1$. This time, we will attempt to prove an isomorphism between $\mathcal{L} \setminus (\pm 1, 0)$ and $\mathcal{H}' := \{(a, b) \in \mathbb{F}_q^\times \times \mathbb{F}_q^\times : ab = D\}$. Consider the map $\rho' : (x, y) \to \left(\frac{x+1}{y}, \frac{x-1}{y}\right)$. Then, letting $(x, y) \in \mathcal{L} \setminus (\pm 1, 0)$, we can see that $\frac{x+1}{y} \cdot \frac{x-1}{y} = \frac{x^2-1}{y^2} = D$, so $\rho' : \mathcal{L} \setminus (\pm 1, 0) \to \mathcal{H}'$. Next, we will show surjectivity. If we let $(a, b) \in \mathcal{H}'$, then $a \neq b$ (because $\left(\frac{D}{q}\right) = -1$, so we can define $x = \frac{a+b}{a-b}$ and $y = \frac{2}{a-b}$. Notice that $\frac{x+1}{y} = a$ and $\frac{x-y}{y} = b$, and

$$x^2 - Dy^2 = \frac{(a+b)^2 - 4D}{(a-b)^2} = \frac{(a-b)^2}{(a-b)^2} = 1$$

which shows that ρ' is surjective. Finally, we will prove injectivity. Let $(x, y), (x', y') \in \mathcal{L} \setminus (\pm 1, 0)$. Then $\frac{x+1}{y} = \frac{x'+1}{y'}$ and $\frac{x-1}{y} = \frac{x'-1}{y'}$ imply $y = y'$ and $xy' = x'y$, so ρ' is injective. Then,

$$|\mathcal{L}| = |\mathcal{H}'| + 2 = |\mathbb{F}_q^\times| + 2 = q + 1 = q - \left(\frac{D}{q}\right)$$

Theorem 3 *The group $\mathcal{L}_{\mathbb{F}_q}$ is cyclic.*

Proof: We proceed by casework on the Legendre Symbol, $\left(\frac{D}{q}\right)$.

Let $\left(\frac{D}{q}\right) = 1$, $d^2 = D$, a be a primitive root $\pmod q$ and $b = a^{-1}$. Then, we define $X = (a+b)/2$ and $Y = (a-b)/2d$, noticing that $X^2 - DY^2 = 1$. Because $X + dY = a$ and $X - dY = b$, we can define x_n and y_n as we did earlier:

$$x_n = \frac{1}{2}((X+dY)^n + (X-dY)^n) = \frac{a^n + b^n}{2} \tag{3}$$

$$y_n = \frac{1}{2d}((X+dY)^n - (X-dY)^n) = \frac{a^n - b^n}{2d} \tag{4}$$

Now, using the binary operation we defined for $\mathcal{L}$, we see that $(X,Y)^n = (x_n, y_n)$. Now, it remains to prove that (x_n, y_n) takes on different values for each $n = 1, 2, \ldots, q-1$ (because we already proved that the order of $\mathcal{L}_{\mathbb{F}_q}$ is $q - \left(\frac{D}{q}\right)$). For the sake of contradiction, let

$$\left(\frac{a^n + b^n}{2}, \frac{a^n - b^n}{2d}\right) = \left(\frac{a^m + b^m}{2}, \frac{a^m - b^m}{2d}\right)$$

where $1 \leq m < n \leq q-1$. Then with a little algebraic manipulation, it is easy to see that $a^n = a^m$. But a is a primitive root $\pmod q$, so $a^n = a^m \implies m = n$, which contradicts our choice of m, n. Thus, (x_n, y_n) is unique for all $n \in \mathbb{F}_q^x$, so $((a+b)/2, (a-b)/2d)$ generates $\mathcal{L}$.

Now, let $\left(\frac{D}{q}\right) = -1$

Theorem 4 *For p and q odd primes, $\mathcal{L}_{\mathbb{Z}_{pq}} \cong \mathcal{L}_{\mathbb{Z}_p} \times \mathcal{L}_{\mathbb{Z}_q}$.*

Proof: We use the Chinese Remainder Theorem. First, note that $\mathbb{Z}_{pq} \cong \mathbb{Z}_p \times \mathbb{Z}_q$. Now, we consider the map $\rho : \mathbb{Z}_{pq}^2 \to \mathbb{Z}_p^2 \times \mathbb{Z}_q^2$ that sends $a \pmod{pq}$ to $a \pmod p$ and $a \pmod q$. We wish to show that ρ is an isomorphism between $\mathcal{L}_{\mathbb{Z}_{pq}}$ and $\mathcal{L}_{\mathbb{Z}_p} \times \mathcal{L}_{\mathbb{Z}_q}$. We will prove this by showing injectivity, then surjectivity. Let $((a', b'), (a'', b'')) \in \mathcal{L}_{\mathbb{Z}_p} \times \mathcal{L}_{\mathbb{Z}_q}$. Now, from the Chinese Remainder Theorem, we know there exists a unique ordered pair $(a, b) \in \mathbb{Z}_{pq}^2$ such that $a \equiv a' \pmod p$, $a \equiv a'' \pmod q$, $b \equiv b' \pmod p$, and $b \equiv b'' \pmod q$. Thus, ρ is injective. Next, we know if $a^2 - Db^2 \not\equiv 1 \pmod{pq}$ then either $a^2 - Db^2 \not\equiv 1 \pmod p$ or $a^2 - Db^2 \not\equiv 1 \pmod q$, which contradicts our initial choice of $((a', b'), (a'', b''))$. Thus, $a^2 - Db^2 \equiv 1 \pmod{pq}$, and ρ is surjective.

4 Lucas Sequences

Write a section on Lucas Numbers here, then you can take out some of the definitions in Theorem 5. Also include how we can extend both the Lucas and Fibonacci Numbers to negative indices.

Theorem 5 *Let V_n be the sequence of Lucas Numbers and let U_n be the auxiliary sequence of Lucas Numbers, otherwise known as the Fibonacci Numbers. Let $L_N(D)$ be the set of all ordered pairs $(V_m \mod N, U_m \mod N)$, and define a binary operation $*$ on $L_N(D)$ by $(V_m \mod N, U_m \mod N) * (V_k \mod N, U_k \mod N) = (V_{m+k} \mod N, U_{m+k} \mod N)$. Then $(L_N(D), *)$ is a cyclic group.*

Proof: The operation $*$ is clearly closed, as V_{m+k} and U_{m+k} are still Lucas Numbers and Fibonacci Numbers, respectively. It is also associative, because $*$ adds indices, and addition is associative. There is an identity element, $(V_0 \mod N, U_0 \mod N) = (2 \mod N, 0 \mod N)$, and each element has an inverse: $(V_m \mod N, U_m \mod N)^{-1} = (V_{-m} \mod N, U_{-m} \mod N)$. Thus, $L_N(D)$ is a group. To show that it's cyclic, note that the element $(V_1 \mod N, U_1 \mod N)$ generates $L_N(D)$, because 1 generates $\mathbb{Z}$, and the indices are in bijection with $\mathbb{Z}$.

The relationship between the orders of the Lucas Group and Pisano Periods that I observed was that when the modulus, p, was congruent to $\pm 1 \mod 10$, and $\left(\frac{D}{q}\right) = 1$, then the order of the Lucas Group was a multiple of the Pisano Period. In fact, most of the time, it was equal to the Pisano Period. I then checked the Online Encyclopedia of Integer Sequences, and it appears that the Pisano Period equals $p - 1$ whenever p is a prime with a Fibonnaci primitive root. Thus, whenever p is a prime with a Fibonnaci primitive root and $\left(\frac{D}{q}\right) = 1$, the order of the Lucas Group equals the Pisano Period.