From Lucas Sequences to Lucas Groups

Kayson T. Hansen

January 1, 2019

1 Abstract

We study Lucas Sequences, recursive sequences that generalize the Fibonacci Sequence, and Lucas Groups, solutions of a variant of Pells Equation mod p. Lucas Sequences have a broad background in the literature, but Lucas Groups have seldom been studied before. When taken mod some prime p, Lucas Sequences form a cyclic group, which will be a subgroup of the corresponding Lucas Group. We show exactly when these two groups are isomorphic by relating a constant associated with the Lucas Sequence and primitive roots of the field with p elements. Furthermore, we prove how often this isomorphism occurs for each prime $p > 3$. We also give a computationally efficient method to find the index of the Lucas Sequence in the Lucas Group when they are not isomorphic.

2 An Isomorphism Between the Lucas Sequence and the Lucas Group

Definition 1 *Let $\mathcal{L}_p$ be the Lucas Group, defined by $\mathcal{L} = \{(x, y) \in \mathbb{Z}_p^2 \,|\, x^2 - Dy^2 = 4 \mod p\}$.*

Definition 2 *Let L_p be the group formed by elements of the Lucas Sequences, defined by $L_p = \{(V_n \mod p, U_n \mod p)\}$ where V_n and U_n are the Lucas Sequences defined in the usual way.*

Lemma 1 *$(P, 1)$ is always a generator of L_p.*

Proof: In $\mathcal{L}_p$, $(V_m, U_m) * (V_n, U_n) = (V_{m+n}, U_{m+n})$. This is proved in [2]. Therefore, because 1 is a generator of $\mathbb{Z}_p$, (V_1, U_1), will be a generator of L_p, and by definition, $(V_1, U_1) = (P, 1)$.

Theorem 1 *Let a be a primitive element in $\mathbb{F}_p$, and let $\left(\frac{D}{p}\right) = 1$. Then $L_p \cong \mathcal{L}_p$ if and only if $P = a + a^{-1} \mod p$.*

Proof: First we will prove the if direction. Let $d = \sqrt{D}$. Note that $P = a + a^{-1} \implies (P, 1) = (a + a^{-1}, \frac{a - a^{-1}}{d})$. Let $(x, y) = (a + a^{-1}, \frac{a - a^{-1}}{d})$. Note that by Lemma 1, $(P, 1)$ will always generate L_p, so if we can show that (x, y) generates $\mathcal{L}_p$, then when $(P, 1) = (x, y)$, $(P, 1)$ will be a generator of both L_p and $\mathcal{L}_p$, so $|L_p| = |\mathcal{L}_p|$. To prove this, we will show that $(x, y)^n = (a^n + a^{-n}, \frac{a^n - a^{-n}}{d})$. We proceed by induction. For the base case, note that $(x, y) * (x, y) = (a^2 + a^{-2}, \frac{a^2 - a^{-2}}{d})$. Now, observe that

$$(a^n + a^{-n}, \frac{a^n - a^{-n}}{d}) * (a + a^{-1}, \frac{a - a^{-1}}{d})$$
$$= (2^{-1}(a^{n+1} + a^{n-1} + a^{1-n} + a^{-n-1} + a^{n+1} - a^{n-1} - a^{-n+1} + a^{-n-1}),$$
$$2^{-1}(\frac{a^{n+1} - a^{n-1} + a^{1-n} - a^{-n-1} + a^{n+1} - a^{n-1} - a^{1-n} - a^{-n-1}}{d}))$$
$$= (a^{n+1} + a^{-n-1}, \frac{a^{n+1} - a^{-n-1}}{d})$$

so we are done with the induction. Now, note that for every $n \in [1, p-1]$, $(x, y)^n$ is unique, because otherwise, $a^n + a^{-n} = a^m + a^{-m} \mod p$ and $a^n - a^{-n} = a^m - a^{-m} \mod p \implies a^m = a^n \mod p$, which is a contradiction, because a is a primitive root $\mod p$. Thus, (x, y) is a generator of $\mathcal{L}_p$, and we are done.

Now, we will prove the reverse direction. This is equivalent to showing that every generator (x, y) takes the form $(a+a^{-1}, \frac{a-a^{-1}}{d})$. There are $\phi(\phi(p)) = \phi(p-1)$ generators of $\mathcal{L}_p$. Now, observe that for two distinct primitive roots a and b, $a + a^{-1} = b + b^{-1} \mod p \implies a^2b + b = b^2a + a \mod p \implies ab(a - b) = a - b \mod p \implies ab = 1 \mod p$. Thus, if $b \neq a^{-1}$, then $a + a^{-1}$ is unique for all generators a. Because there are $\phi(p-1)$ primitive elements a, this implies that there are $\phi(p-1)/2$ unique values for $a + a^{-1}$. Furthermore, there are two values of $\frac{a-a^{-1}}{d}$ for each value of $a + a^{-1}$; one from the positive root of D, and one from the negative root. Thus, there are $\phi(p-1)$ unique values in total, which is also the total number of generators of $\mathcal{L}_p$.

Theorem 2 *Let $\left(\frac{D}{p}\right) = -1$, and set $d = \sqrt{D}$. Consider the field $\mathbb{F} \cong \mathbb{F}_{p^2}$ defined by $\mathbb{F} = \{x + yd \,|\, x, y \in \mathbb{F}_p\}$ and $(x_1 + y_1 d) + (x_2 + y_2 d) = (x_1 + x_2 + (y_1 + y_2)d)$, $(x_1 + y_1 d) * (x_2 + y_2 d) = (x_1 x_2 + D y_1 y_2 + (x_1 y_2 + y_1 x_2)d)$. Let $a = a_1 + a_2 d$ be a primitive element in $\mathbb{F}$. Then $L_p \cong \mathcal{L}_p$ if and only if $P = \frac{a_1}{a_2} - 2 \mod p$.*

Proof: First, we will prove the if direction. Note that

$$P = \frac{a_1}{a_2} - 2 \mod p \implies (P, 1) = \left(\frac{2a_1^2 + 2Da_2^2}{a_1^2 - Da_2^2} \mod p, \frac{4a_1 a_2}{a_1^2 - Da_2^2} \mod p \right).$$

Let $||x + yd|| = x^2 - Dy^2$. Now consider the functions

$$h(x + yd) = \frac{(x + yd)^2}{\sqrt{||(x + yd)^2||}} \tag{1}$$

and

$$f(x + yd) = (2x, 2y). \tag{2}$$

We will show that

$$\left(\frac{2a_1^2 + 2Da_2^2}{a_1^2 - Da_2^2} \mod p, \frac{4a_1 a_2}{a_1^2 - Da_2^2} \mod p \right)$$

is equivalent to $f(h(a))$. First, notice that

$$||(x + yd)^2|| = (x^2 + Dy^2)^2 - D(2xy)^2 = (x^2 - Dy^2)^2 = (||x + yd||)^2 \tag{3}$$

so we can simplify $h(x + yd) = \frac{(x+yd)^2}{\sqrt{||(x+yd)^2||}} = \frac{(x+yd)^2}{||x+yd||}$. Then,

$$f(h(a)) = f\left(\frac{a_1^2 + Da_2^2}{||a_1 + da_2||} + \frac{2da_1 a_2}{||a_1 + da_2||} \right) = \left(\frac{2a_1^2 + 2Da_2^2}{a_1^2 - Da_2^2}, \frac{4a_1 a_2}{a_1^2 - Da_2^2} \right)$$

Now, by applying Lemma 1 once again, $(P,1)$ will always generate L_p, so if we can show that $f(h(a))$ is a generator of $\mathcal{L}_p$, then when $(P,1) = f(h(a))$, we will have $L_p \cong \mathcal{L}_p$.

Consider the multiplicative group of $\mathbb{F}$, $\mathbb{F}^\times$. We will show that h, as defined in Theorem 2, is a homomorphism from $\mathbb{F}^\times$ to $G = \{x + yd \in \mathbb{F} \,|\, x^2 - Dy^2 = 1 \mod p\}$. To do this, we'll first show that h has domain $\mathbb{F}^\times$ by showing that (a) the denominator is never 0 and (b) that $||(x+yd)^2||$ is always a perfect square. We'll prove (a) by contradiction: let $\sqrt{||(x+yd)^2||} = 0 \mod p$. Then $(x^2+Dy^2)^2 - D(2xy)^2 = 0 \mod p \implies x^4 + D^2y^4 - 2Dx^2y^2 = 0 \mod p \implies x^2 - Dy^2 = 0 \mod p \implies x^2 = Dy^2 \mod p \implies \left(\frac{D}{p}\right) = 1$, which is a contradiction. To prove (b), observe that by (3), $||(x+yd)^2||$ is always a perfect square.

Next, we will show that G is the codomain of h. For this to be true, we must have $||h(x+yd)|| = 1$ for all $x + yd \in \mathbb{F}^\times$. To prove this, first note that for any constant c, we have $||c(x+yd)|| = c^2||x+yd||$. Now, the following argument suffices (here we use the simplified form of h):

$$h(x+yd) = \left|\left| \frac{(x+yd)^2}{||x+yd||} \right|\right| = \frac{1}{(||x+yd||)^2}||(x+yd)^2|| = 1$$

Now that we know the domain and codomain of h, we will show that h is a homomorphism between the two groups. We will do this in two steps: first, we will show that $((x_1+y_1d)(x_2+y_2d))^2 = (x_1+y_1d)^2(x_2+y_2d)^2$, and second, we will show that $||(x_1+y_1d)(x_2+y_2d)|| = ||x_1+y_1d||||x_2+y_2d||$; if both of these are true, then h is a homomorphism. The former is trivially true, because multiplication in $\mathbb{F}$ is defined the same way as multiplication in $\mathbb{C}$. The latter is also true, by the following argument: we have

$$||(x_1+y_1d)(x_2+y_2d)|| = ||x_1x_2 + Dy_1y_2 + (x_1y_2 + y_1x_2)d||$$
$$= (x_1x_2 + Dy_1y_2)^2 - D(x_1y_2 + y_1x_2)^2 = x_1^2x_2^2 + D^2y_1^2y_2^2 - Dx_1^2y_2^2 - Dy_1^2x_2^2$$

and

$$||x_1+y_1d||||x_2+y_2d|| = (x_1^2 - Dy_1^2)(x_2^2 - Dy_2^2) = x_1^2x_2^2 + D^2y_1^2y_2^2 - Dx_1^2y_2^2 - Dy_1^2x_2^2.$$

Thus, h is a homomorphism.

Now that we know h is a homomorphism, and because homomorphisms map generators of the domain to generators of the codomain, if a is a generator of $\mathbb{F}^\times$, then it will be a generator of G. Now, f, as defined in Theorem 2, is trivially a function from G to $\mathcal{L}_p$, and we will now prove that it's a homomorphism as well. Observe that

$$f((x_1+y_1d)(x_2+y_2d)) = f(x_1x_2 + Dy_1y_2 + (x_1y_2 + y_1x_2)d)$$
$$= (2x_1x_2 + 2Dy_1y_2, 2x_1y_2 + 2y_1x_2)$$

and

$$f(x_1+y_1d)f(x_2+y_2d)$$
$$= (2x_1, 2y_1) * (2x_2, 2y_2) = (2^{-1}(4x_1x_2 + 4Dy_1y_2, 2^{-1}(4x_1y_2 + 4y_1x_2))$$
$$= (2x_1x_2 + 2Dy_1y_2, 2x_1y_2 + 2y_1x_2)$$

so f is a homomorphism. Thus, $f(h(a))$ maps from $\mathbb{F}^\times$ to $\mathcal{L}_p$, and because a is a generator in $\mathbb{F}^\times$, it will also be a generator in $\mathcal{L}_p$. So if

$$(P,1) = f(h(a)) = \left(\frac{2a_1^2 + 2Da_2^2}{a_1^2 - Da_2^2} \mod p, \frac{4a_1a_2}{a_1^2 - Da_2^2} \mod p \right)$$

it will be a generator of both L_p and $\mathcal{L}_p$, which implies $|L_p| = |\mathcal{L}_p|$, and we are done.

Now, we will prove the reverse direction, which is equivalent to showing, similarly as before, that every generator of $\mathcal{L}_p$ comes in the form $f(h(a))$. It is well-known that if a homomorphism from H to H' is surjective, then the images of the generators of G generate G'. Thus, it is sufficient to show that both h and f are surjective. To prove the former, by observing the identity $x^2 - Dy^2 = 1$ for any $x + yd \in G$, one can show that $h(x + 1 + yd) = x + yd$:

$$\frac{(x+1+yd)^2}{(x+1)^2 - Dy^2} = \frac{x^2 + 2x + 2xyd + 1 + 2yd + Dy^2}{x^2 + 2x + 1 - Dy^2} = \frac{2x(x+1) + 2yd(x+1)}{2x+2} = x + yd$$

To prove the latter, note that for any $(x, y) \in \mathcal{L}_p$, we can take $2^{-1}x + 2^{-1}yd \in G$, and clearly, $f(2^{-1}x + 2^{-1}yd) = (x, y)$. Thus, we are done.

Now, while these theorems give necessary and sufficient conditions for the isomorphism between the Lucas Sequence and the Lucas Group, we can generalize them to show what the ratios of the orders are between the groups, by seeing not only when $(P, 1) = (a + a^{-1}, \frac{a-a^{-1}}{d})$ or $(P, 1) = \frac{a_1}{a_2} - 2$, but also when $(P, 1) = (a + a^{-1}, \frac{a-a^{-1}}{d})^n$ or $(P, 1) = (\frac{a_1}{a_2} - 2)^n$ (where multiplication is the operation in the Lucas Group). Whatever n is will be the ratio of the orders of the two groups, or in other words, the index of the Lucas Sequence in the Lucas Group. This reduces computation of the index of the two groups to solving a discrete logarithm, which can be done efficiently using the Silver-Pohlig-Hellman Algorithm.

Theorem 3 *There are*

$$\frac{\phi(p-1) + \phi(p+1)}{2} + 1$$

nonzero values of P such that $L_p \cong \mathcal{L}_p$ for each prime $p > 3$.

Proof: There are $\phi(p-1)$ generators when $\left(\frac{D}{p}\right) = 1$, and $\phi(p+1)$ generators when $\left(\frac{D}{p}\right) = -1$. For the first case, when proving Theorem 1, we showed that there are $\phi(p-1)$ unique values of $(a + a^{-1}, \frac{a-a^{-1}}{d})$, and exactly half of those ordered pairs have $\frac{a-a^{-1}}{d} = 1$, which corresponds to $\phi(p-1)/2$ values of P.

Next, notice that by Theorem 2, every generator of $\mathcal{L}_p$ is in the form

$$f(h(a)) = \left(\frac{2a_1^2 + 2Da_2^2}{a_1^2 - Da_2^2} \mod p, \frac{4a_1a_2}{a_1^2 - Da_2^2} \mod p \right)$$

Thus, because there are $\phi(p+1)$ generators of $\mathcal{L}_p$, there are $\phi(p+1)$ unique values of $f(h(a))$. When setting $\frac{2a_1^2+2Da_2^2}{a_1^2-Da_2^2}$ equal to P and simplifying, we obtain a quadratic $a_1^2 = a_2^2(P+2)^2$, and taking one root of this equation gives us $P = \frac{a_1}{a_2} - 2$, which is the only solution to $(P, 1) = f(h(a))$. Therefore, much like the case when $\left(\frac{D}{p}\right) = 1$, only half of these generators can equal $(P, 1)$, so the total number of unique values for $f(h(a))$ such that $L_p \cong \mathcal{L}_p$ is $\phi(p+1)/2$. Thus, the total number of values such that $L_p = \mathcal{L}_p$ when $\left(\frac{D}{p}\right) = \pm 1$ is $\frac{\phi(p-1)+\phi(p+1)}{2}$, minus whatever overlap there is between the two cases (i.e. $P = a + a^{-1}$ when $\left(\frac{D}{p}\right) = -1$). However, there is no overlap between the two, because $P = a + a^{-1} \implies D = (a - a^{-1})^2 \implies \left(\frac{D}{p}\right) = 1$ and $P = \frac{a_1}{a_2} \implies \left(\frac{D}{p}\right) = -1$, because to even construct $\mathbb{F}$, we need $\left(\frac{D}{p}\right) = -1$.

Finally, we add one because of the degenerate case when $P = -2$, $D = 0$. In this case, the order of the Lucas Sequence is always even, because V_n alternates between 2 and -2. Also, we have $|\mathcal{L}_p| = 2p$, as $x^2 - Dy^2 = 4 \implies x^2 = 4 \implies x = \pm 2$, so there are 2 possible values for x and p possible values for y. Because L_p is a subgroup of $\mathcal{L}_p$, by Lagrange's Theorem, we must have $|L_p| = 1, 2, p, \text{or } 2p$. However, $|L_p| \geq 3$, as $(V_0, U_0) = (2, 0)$, $(V_1, U_1) = (-2, 1)$, and $(V_2, U_2) = (2, -2)$. Thus, because $|L_p|$ is even and greater than 2, it must be $2p$, so $L_p \cong \mathcal{L}_p$, giving us a total of $\frac{\phi(p-1)+\phi(p+1)}{2} + 1$ unique values for P.

References

[1] F. Arnault. *The Rabin-Monier Theorem for Lucas Pseudoprimes.* **Mathematics of Computation**, vol. 66, no. 218, 1997, 869-882.

[2] D. Hinkel. *An Investigation of Lucas Sequences.* **ScholarWorks Boise State University Scholarship and Research**, 2007.

[3] R. Baillie and S. S. Wagstaff, Jr. *Lucas Pseudoprimes.* **Mathematics of Computation**, vol. 35, no. 152, 1980, 1391-1417.