The Euler Totient Function on Lucas Sequences

J.C. Saunders[1]

[1]Department of Mathematics and Statistics
University of Calgary

BIRS: Alberta Number Theory Days XIII

Binary Recurrence Sequences

The Fibonacci sequence is $1, 1, 2, 3, 5, 8, 13, \ldots$

The Fibonacci sequence is an example of a *binary recurrence sequence*.

Definition

A *binary recurrence sequence* is a sequence of integers that satisfies a given recursion relation of the form $u_n = Pu_{n-1} + Qu_{n-2}$ where P and Q are fixed integers and $(u_n)_n$ is the sequence in question. There are two important kinds of binary recurrence sequences.

We have an explicit form for the nth term of such a sequence begin $u_n = a\alpha^n + b\beta^n$, where a nnd b are constants and α and β are the roots of the polynomial $x^2 - Px - Q$. If $ab \neq 0$ and α/β isn't a root of unity, then $(u_n)_n$ is *nondegenerate*.

Lucas Sequences

There are two special kinds of binary recurrence sequences.

Definition

A *Lucas sequence of the first kind* is a binary recurrence sequence $(u_n)_n$, starting with $u_0 = 0$ and $u_1 = 1$. A *Lucas sequence of the second kind* is a binary recurrence sequence $(v_n)_n$, starting with $v_0 = 2$ and $v_1 = P$.

The Fibonacci sequence is a Lucas sequence of the first kind. Another example of a Lucas sequence of the first kind is the Pell sequence: $1, 2, 5, 12, 29, 70, 169, \ldots$. An example of a Lucas sequence of the second kind are the Lucas numbers: $2, 1, 3, 4, 7, 11, 18, \ldots$.

If $(u_n)_n$ is a Lucas sequence of the first kind, then $u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$. If $(v_n)_n$ is a Lucas sequence of the second kind, then $v_n = \alpha^n + \beta^n$

The Euler Totient Function and Luca's Result

The Euler Totient Function φ counts the number of integers from 1 to n that are coprime to n. It is a multiplicative function, i.e. $\varphi(mn) = \varphi(m)\varphi(n)$ for any coprime pairs of positive integers m and n.

Theorem (Luca (2002))

Let $(u_n)_n$ and $(v_n)_n$ be two nondegenerate binary recurrence sequences with $u_n = r_1 u_{n-1} + s_1 u_{n-2}$, $v_n = r_2 v_{n-1} + s_2 v_{n-2}$ with the roots of the charactristic equations being α_1 and β_1, and α_2 and β_2, respectively, satisfying one of the statements

A1) Not all four numbers α_1, β_1, α_2, β_2 are integers.

A2) $\log|\alpha_1|$ and $\log|\alpha_2|$ are linearly independent over Q.

A3) $|\alpha_1| > \max\left\{|\beta_1|^2, |\beta_2|^2\right\} > 1$.

Also, suppose (v_n) is a Lucas sequence of the second kind or that s_2 is even and r_2 is odd. Then the equation

$$\varphi(|au_m|) = |bv_n|.$$

Examples

Removing the assumptions A1 through A3 is likely not possible. For instance, take $u_n = v_n = 2^n - 1$. If $n = p$ a prime such that $2^p - 1$ is a Mersenne prime, then we have

$$\varphi(u_p) = \varphi(2^p - 1) = 2^p - 2 = 2(2^p - 1) = 2v_p$$

and it is conjectured that there are infinitely many Mersenne primes. On the other hand, Luca's result shows that the equations $\varphi(L_m) = L_n$ and $\varphi(F_m) = L_n$ only have finitely many solutions where F_m is the mth Fibonacci number and L_n is the nth Lucas number. Moreover, Luca found all of the solutions to these two equations, which are
$(m, n) = (0, 1), (1, 1), (2, 0), (3, 0)$ and
$(m, n) = (1, 1), (2, 1), (3, 1), (4, 0), (5, 3), (6, 3)$, respectively.

When $(u_n)_n$ and $(v_n)_n$ are the same sequence

One case that the assumptions A1 through A3 excludes is the equation

$$\varphi(|au_m|) = |bu_n|.$$

where $(u_n)_n$ is a Lucas sequence of the first kind. There are also results on this more specific equation. For instance, when $u_n = \frac{b^n-1}{b-1}$, where $b > 1$, we have further results by Luca, and Faye and Luca.

Theorem (Luca (2005))

Let $b > 1$ and $1 \leq x, y < b$. Then the equation

$$\varphi\left(x\frac{b^n-1}{b-1}\right) = y\frac{b^m-1}{b-1}$$

only has finitely many solutions.

Theorem (Chen and Tian (2017))

Let $x > y \geq 1$. Then all of the solutions to

$$\varphi\left(\frac{x^m - y^m}{x - y}\right) = \frac{x^n - y^n}{x - y}$$

are $(x, y, m, n) = (a, b, 1, 1)$ for any integers $a > b \geq 1$. Also, all of the solutions to

$$\varphi\left(x^m - y^m\right) = x^n - y^n$$

are $(x, y, m, n) = (a + 1, a, 1, 1)$ for any integer $a \geq 1$.

Theorem (Bai (2020))

Let $x > y \geq 1$. Then all of the solutions to

$$\varphi\left(\left|\frac{x^m - y^m}{x - y}\right|\right) = \left|\frac{x^n - y^n}{x - y}\right|,$$

where $xy \neq 0$ and $n, m > 0$, are $(x, y, m, n) = (a \pm 1, -a, 1, 2), (a \pm i, -a, 2, 1)$, where a is an integer and $i = 1, 2$. Also, all of the solutions to

$$\varphi\left(|x^m - y^m|\right) = |x^n - y^n|$$

are $(x, y, m, n) = \left(2^{t-1} \pm 1, -2^{t-1} \pm 1, 2, 1\right), \left(-2^{t-1} \pm 1, 2^{t-1} \pm 1, 2, 1\right)$, where $t \geq 2$ is an integer.

Useful Properties of Lucas Sequences

Let $(u_n)_n$ be a Lucas sequence of the first kind. For all natural numbers N there exists $z(N) \in \mathbb{N}$ such that $N \mid u_n$ if and only if $z(N) \mid n$. We call $z(N)$ the *order of appearance* of N in the sequence $(u_n)_n$.

Lemma (Lucas (1878))

Let p be a prime. Then $z(p) = p$ if $p \mid D$. Also, if $p \nmid D$ and D is a quadratic residue $\pmod{p}$, then $z(p) \mid p-1$. If $p \nmid D$ and D isn't a quadratic residue $\pmod{p}$, then $z(p) \mid p+1$.

Lemma (Lucas (1878))

Let $a, k, m \in \mathbb{N}$ and q be a prime such that $q^a \| u_m$ and $q \nmid k$. Then for any $l \geq 0$, we have $q^{a+l} | u_{kmq^l}$ with $q^{a+l} \| u_{kmq^l}$ if $q^a \neq 2$.

Primitive Prime Factors

Another interesting result we'll be using on the prime factors of u_n is due to Carmichael. First, a definition.

Definition

A *primitive prime factor* of u_n (respectively, v_n) is a prime factor p of u_n (respectively, v_n) such that $p \nmid u_m$ (respectively, $p \nmid v_m$) for all $1 \leq m < n$.

Lemma (Carmichael (1913))

If $n \neq 1, 2, 6$, *then* u_n *has a primitive prime factor, except in the case of* $n = 12$ *in the usual Fibonacci sequence* $1, 1, 2, 3, 5, 8, \ldots$.

Method of Proof

Let $u_n = \frac{b^n-1}{b-1}$, $x = y = 1$, and $\gcd(n, m) = k \leq n - m = \lambda$. Then we have

$$b^k \leq b^\lambda < \frac{u_n}{u_m} = \prod_{p \mid u_n} \left(1 + \frac{1}{p-1}\right).$$

Therefore,

$$k \leq \lambda \ll \sum_{p \mid u_n} \frac{1}{p} = \sum_{d \mid n} S_d,$$

where

$$S_d := \sum_{z(p)=d} \frac{1}{p}.$$

We get

$$S_d \leq \sum_{\substack{p \equiv 1 \pmod{d} \\ p \leq d^2}} \frac{1}{p} + \frac{\omega_d}{d^2} \ll \frac{\log \log d}{\varphi(d)}.$$

We deduce

$$k \leq \lambda \ll 1 + \sum_{p|n} \frac{\log\log p}{p}$$

We obtain

$$\sum_{p|k} \frac{\log\log p}{p} \ll (\log\log\log k)^2,$$

by the Prime Number Theorem. Also, if $p \mid n$ and $p \nmid m$, then $p^{\gamma} \| u_m$ where we can bound γ. If $p \mid d \mid n$, then u_d has a primitive prime factor, say q, and we have $d \mid q-1$, since $q \mid u_{q-1}$. So, $q \mid u_n$, so that $p \mid q-1 \mid u_m$. Therefore, we can bound the number of factors of n/p, which allows us to bound

$$\sum_{\substack{p|n \\ p\nmid m}} \frac{\log\log p}{p}.$$

The prime factors of n are bounded using this technique, bounding n.

Fibonacci and Pell Sequences

Theorem (Luca and Nicolae (2009))

The only Fibonacci numbers whose Euler totient function is another Fibonacci number are $1, 2$, *and* 3.

Theorem (Faye and Luca (2015))

The only Pell numbers whose Euler totient function is another Pell number are 1 *and* 2.

My Result

Theorem (S. (2021))

For any fixed natural number $P \geq 3$, if we define the sequence $(u_n)_n$ as $u_0 = 0$, $u_1 = 1$, and $u_n = Pu_{n-1} + u_{n-2}$ for all $n \geq 2$, then the only solution to the Diophantine equation $\varphi(u_n) = u_m$ is $\varphi(u_1) = \varphi(1) = 1 = u_1$.

This completely exhausts the problem of finding solutions to $\varphi(u_n) = u_m$ where $(u_n)_n$ is a Lucas sequence of the first kind with recurrence relation $u_n = Pu_{n-1} + u_{n-2}$ and $P > 0$. If, instead, we have $P < 0$ and $(u_n)_n$ is the corresponding Lucas sequence, then we can see that $(|u_n|)_n$ is the corresponding Lucas sequence of $-P$. Therefore, it suffices to investigate the case of $P > 0$ for a Lucas sequence of the first kind with $Q = 1$, which we do here.

Lemma

Let $m, j \in \mathbb{N}$.

i) Suppose P is odd. Then $3 \cdot 2^j \mid m$ if and only if $2^{j+2} \mid u_m$.

ii) Suppose P is even and $2^{t_1} \| P$. Then $2^j \mid m$ if and only if $2^{j+t_1-1} \mid u_m$.

We first deduce that m is even. Let k be the number of distinct prime factors of u_n and let $q_1, \ldots, q_k$ be these prime factors. Then $2^{k-1} \mid u_m$, so that $2^k \ll m$ where the implies constant depends on the P.

The Case of $2^{416} < m < n$

Let $l := n - m$. For large enough P or α, we have

$$\prod_{i=1}^{r} \left(\frac{p_i}{p_i - 1} \right) < \alpha^l < \frac{u_n}{u_m} = \prod_{i=1}^{k} \left(\frac{q_i}{q_i - 1} \right)$$

where p_i is the ith prime. For smaller values of α, we can "eliminate" a lot of the possible p_i primes and/or show that $l \geq 2, 3$, so that we still get $k > r$.

n even

Suppose n is even. Then $n = 2^s n_1$ where $s \geq 1$ and n_1 is odd. It turns out, for all i, we have $u_{2i} = u_i v_i$, where v_i is the corresponding Lucas sequence of the second kind. Also, in general, we have

$$v_i^2 - Du_i^2 = 4(-Q)^i.$$

So if i is odd and $p \mid v_i$, then

$$-Du_i^2 \equiv -4Q^i \pmod{p}.$$

If $Q = 1$, then D is a quadratic residue $\pmod{p}$, so that $z(p) \mid p - 1$. Also,

$$u_n = u_{n_1} v_{n_1} v_{2n_1} \cdots v_{2^{s-1} n_1}.$$

We can derive

$$l \log \alpha < \log \log \alpha + 2.163 + \sum_{\substack{d \mid n \\ d > \alpha^2}} T_d,$$

where

$$T_d := \sum_{\substack{l_p = d \\ p > \alpha^4}} \frac{1}{p}.$$

We split up the sum

$$\sum_{\substack{d \mid n \\ d > \alpha^2}} T_d = L_1 + L_2,$$

where

$$L_1 := \sum_{\substack{d \mid n \\ r \mid d \implies r \mid 2M \\ d > \alpha^2}} T_d \text{ and } L_2 := \sum_{\substack{d \mid n \\ r \mid d \text{ for some } r \nmid m \\ d > \alpha^2}} T_d.$$

n odd

Suppose n is odd. Then

$$v_n^2 - Du_n^2 = -4$$

So, if $p \mid u_n$, then -1 is a quadratic residue $\pmod{p}$, so that $p = 2$ or $p \equiv 1 \pmod{4}$. Therefore, $4^{k-1} \mid u_m$, so $4^k \ll n$. We show that $n \lll 4^k$, leading to a contradiction for $n > m > 2^{416}$.

We have

$$\alpha^{-l} > \frac{u_m}{u_n} = \prod_{i=1}^{k} \left(1 - \frac{1}{q_i}\right) \geq \prod_{2 \leq p \leq p_k} \left(1 - \frac{1}{p}\right)$$
$$> \frac{1}{1.79 \log p_k \left(1 + \frac{1}{2(\log p_k)^2}\right)}.$$

Noting that $2^k \ll m$ gives

$$l < \frac{\log \log \log n}{\log \alpha} + 0.83.$$

We prove by induction that

$$q_1 q_2 \cdots q_i < \left(2k\alpha^{1.83} \log \log n\right)^{\frac{3^i - 1}{2}}.$$

Therefore,

$$u_n \leq q_1 q_2 \cdots q_k u_l < \left(2k\alpha^{1.83} \log \log n\right)^{\frac{3^k - 1}{2}} (\log \log n) \alpha^{-0.17}$$
$$< \left(2k\alpha^{1.83} \log \log n\right)^{\frac{3^k + 1}{2}}.$$

Future Research

Can we get the same result for any Q? What about other binary recurrence sequence?

Can we replace the Euler totient function with another arithmetic function, such as the sum of the divisors function or the sum of the kth powers of the divisors function? Luca proved that if $k \geq 2$ in this problem and the sequence is the Fibonacci sequence, then $n = m = 1$ or $k = 2$, $m = 3$, and $n = 5$.

Acknowledgements

I would like to thank the Univeristy of Calgary for the award of a postdoctoral fellowship, which made this research possible.

Thanks for listening! Any questions?