Generalized Lucas Sequences Part II

Daryl DeFord

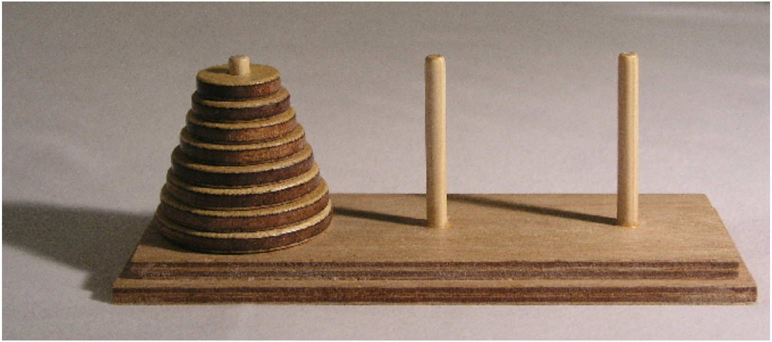
Washington State University

February 4, 2013

Èdouard Lucas:

The theory of recurrent sequences is an inexhaustible mine which contains all the properties of numbers; by calculating the successive terms of such sequences, decomposing them into their prime factors and seeking out by experimentation the laws of appearance and reproduction of the prime numbers, one can advance in a systematic manner the study of the properties of numbers and their application to all branches of mathematics.

Èdouard Lucas:



Roadmap

Recurrence Relation Solutions

Problem

High order recurrence relation solutions are unsatisfactory.

Recurrence Relation Solutions

Problem

High order recurrence relation solutions are unsatisfactory.

Can we get terms for free?

Recurrence Relation Solutions

Problem

High order recurrence relation solutions are unsatisfactory.

Can we get terms for free?

Efficiency, practicality, asymptotics...

Vector Spaces

Given a particular recurrence relation $\mathcal{R}$ of order n, the set of sequences that satisfy that relation form a vector space (over $\mathbb{C}$). Since each sequence is uniquely determined by its initial conditions, the order of the space is also n.

If the roots of $\mathcal{R}$ are $\alpha_1, \alpha_2, \ldots, \alpha_k$ with respective multiplicities $m_1, m_2, \ldots, m_k$, then the set of generalized power sums (GPS) of the form:

$$\sum_{i=1}^{k} p_i(n)\alpha_i^n$$

where the p_i are polynomials of degree strictly less than m_i forms an equivalent vector space.

Vector Spaces

Given a particular recurrence relation $\mathcal{R}$ of order n, the set of sequences that satisfy that relation form a vector space (over $\mathbb{C}$). Since each sequence is uniquely determined by its initial conditions, the order of the space is also n.

If the roots of $\mathcal{R}$ are $\alpha_1, \alpha_2, \ldots, \alpha_k$ with respective multiplicities $m_1, m_2, \ldots, m_k$, then the set of generalized power sums (GPS) of the form:

$$\sum_{i=1}^{k} p_i(n)\alpha_i^n$$

where the p_i are polynomials of degree strictly less than m_i forms an equivalent vector space.

If we consider the set of all sequences that satisfy some LHCCRR and the set of all GPS of algebraic numbers, we see that these larger sets form a commutative ring (actually an integral domain)

Bases

- Since we have a vector space, it makes sense to talk about a basis for that space

Bases

- Since we have a vector space, it makes sense to talk about a basis for that space
- What sequences should we select?

Bases

- Since we have a vector space, it makes sense to talk about a basis for that space
- What sequences should we select?
- GPS coefficients / Sequence terms / Generating function numerator

Bases

- Since we have a vector space, it makes sense to talk about a basis for that space
- What sequences should we select?
- GPS coefficients / Sequence terms / Generating function numerator
- Consider the tribonacci numbers, Padovan numbers etc.

Bases

- Since we have a vector space, it makes sense to talk about a basis for that space
- What sequences should we select?
- GPS coefficients / Sequence terms / Generating function numerator
- Consider the tribonacci numbers, Padovan numbers etc.
- Combinatorial interpretations (f_n) / Number–theoretic properties (F_n)

Second Order

Luckily, in the case of second order sequences a natural basis presents itself.
Considering the simplest second order relation:

$$T_n = T_{n-1} + T_{n-2}$$

Second Order

Luckily, in the case of second order sequences a natural basis presents itself.
Considering the simplest second order relation:

$$T_n = T_{n-1} + T_{n-2}$$

We can take $F_0 = 0$ and $F_1 = 1$ as well as $L_0 = 2$ and $L_1 = 1$. Obviously $[0, 1]$ and $[2, 1]$ are linearly independent as initial conditions, however, the respective GPS are also simple:

Second Order

Luckily, in the case of second order sequences a natural basis presents itself.
Considering the simplest second order relation:

$$T_n = T_{n-1} + T_{n-2}$$

We can take $F_0 = 0$ and $F_1 = 1$ as well as $L_0 = 2$ and $L_1 = 1$. Obviously $[0, 1]$ and $[2, 1]$ are linearly independent as initial conditions, however, the respective GPS are also simple:

$$F_n = \frac{\varphi^n - \overline{\varphi}^n}{\sqrt{5}}$$

$$L_n = \varphi^n + \overline{\varphi}^n$$

Identities

- Obviously, there are innumerable identities linking these two very well known sequences...
- This is exactly what we want from a basis
- What about other second order sequences?

Lucas Sequences

Lets consider the more general form of a second order recurrence relation:

$$T_n = PT_{n-1} - QT_{n-2}$$

This relation has:

- characteristic equation $x^2 - Px + Q$
- discriminant $D = P^2 - 4Q$
- roots $\alpha = \frac{P+\sqrt{D}}{2}$ and $\beta = \frac{P-\sqrt{D}}{2}$

$T_n = PT_{n-1} - QT_{n-2}$

Definition (Fundamental Lucas Sequence)

$$u_0 = 0, u_1 = 1$$

with GPS

$$u_n = \frac{\alpha^n - \beta^n}{\sqrt{D}}$$

$T_n = PT_{n-1} - QT_{n-2}$

Definition (Fundamental Lucas Sequence)

$$u_0 = 0, u_1 = 1$$

with GPS

$$u_n = \frac{\alpha^n - \beta^n}{\sqrt{D}}$$

Definition (Primordial Lucas Sequence)

$$v_0 = 2, v_1 = P$$

with GPS

$$v_n = \alpha^n + \beta^n$$

Èdouard Lucas:

... we then show the connection that exists between the symmetric functions and the theory of determinants, combinations, continued fractions, divisibility, divisors of quadratic forms, continued radicands, division of the circumference of a circle, indeterminate analysis of the second degree quadratic residues, decomposition of large numbers into their prime factors, etc.

Definition

Definition

A sequence a_n is called a divisibility sequence if for any two natural numbers m and n such that $m|n$ we also have the property $a_m|a_n$.

Definition

Definition

A sequence a_n is called a divisibility sequence if for any two natural numbers m and n such that $m|n$ we also have the property $a_m|a_n$.

Example (Fibonacci Numbers)

The Fibonacci numbers are a divisibility sequence. Notice $F_7 = 13$ while $F_{21} = 10946 = 13 * 842$. In addition, every third Fibonacci number is even, etc.

More Examples

Example

- More generally any fundamental Lucas sequence is a divisibility sequence.
- Any constant sequence is trivially a divisibility sequence.
- For any two integers $\ell \geq k$, the GPS

$$\ell^n - k^n$$

  is a divisibility sequence.
- Products of sequences
- Others...

Congruence Cycles

For any modulus m, a LHCCRR is periodic. Thus, there exists some k depending on m and the coefficients such that for all n

$$a_{n+k} \equiv a_n \pmod{m}$$

Congruence Cycles

For any modulus m, a LHCCRR is periodic. Thus, there exists some k depending on m and the coefficients such that for all n

$$a_{n+k} \equiv a_n \pmod{m}$$

If m is prime and m does not divide the discriminant of $\mathcal{R}$, then k can be defined more specifically

Prime Factors

Theorem

If a_n is a divisibility sequence and a_k has a factor m, relatively prime to Q, then $a_0 \equiv 0 \pmod{m}$

Prime Factors

Theorem

If a_n is a divisibility sequence and a_k has a factor m, relatively prime to Q, then $a_0 \equiv 0 \pmod{m}$

This theorem separates divisibility sequences into two categories: degenerate sequence

$$a_0 \neq 0$$

and regular sequences

$$a_0 = 0$$

.

Degenerate Sequences

When $a_0 \neq 0$, you can use the previous Theorem to show that any prime dividing any a_n must divide either a_0 or Q. In general, this is the least interesting case. As an example consider the first order case...

Regular Sequences

When $a_0 = 0$ there is more freedom. Again applying the previous Theorem we can show that every prime not dividing Q divides some a_n. The first n for which $p|a_n$ is known as the rank of apparition of p.

Third–Order Recurrences

Although the smaller order cases come together nicely, when we reach third–order recurrences we are no longer guaranteed the ability to construct regular divisibility sequences for all recurrences. The problem gets worse as the order grows...

Primality Testing

Lucas used the theory of these symmetric functions to determine a variety of primality tests. Particularly for when the prime factors of $N+1$ or $N-1$ were known. Probably most famously, he showed that

$$2^{127} - 1 = 170141183460469231731687303715884105727$$

is prime, by hand. This stood as the largest known prime for 75 years.

Èdouard Lucas:

...by searching for the addition formulas of the numerical functions which originate from recurrence sequences of the third or fourth degree, and by studying in a general way the laws of residues of these functions for prime moduli ... we would arrive at important new properties of prime numbers.

Èdouard Lucas:

...by searching for the addition formulas of the numerical functions which originate from recurrence sequences of the third or fourth degree, and by studying in a general way the laws of residues of these functions for prime moduli ... we would arrive at important new properties of prime numbers.

- Computers
- Modern Sieves
- University of Calgary

Tiling Problems

Considering our original problem, divisibility sequences offer some interesting potential, but are in general too restrictive to help with counting problems.

Tiling Problems

Considering our original problem, divisibility sequences offer some interesting potential, but are in general too restrictive to help with counting problems. From a combinatorial perspective the natural insight is to work backwards.

Tiling Problems

Considering our original problem, divisibility sequences offer some interesting potential, but are in general too restrictive to help with counting problems. From a combinatorial perspective the natural insight is to work backwards.

What is a_0?

Tiling Problems

Considering our original problem, divisibility sequences offer some interesting potential, but are in general too restrictive to help with counting problems. From a combinatorial perspective the natural insight is to work backwards.

What is a_0?

- Tiling models
- Binomial Coefficients

Motivation

The most direct way to get "terms for free" appeared to arise from the equation

$$a_n = |a_{-n}|.$$

- Even sequences $a_n = a_{-n}$ (Primordial)
- Odd sequences $a_n = -a_{-n}$ (Fundamental)

Examples: Domino Tilings

Order	Recurrence Relation	Initial Conditions
1	$a_n = a_{n-2}$	[1,0]
2	$a_n = a_{n-1} + a_{n-2}$	[0,1]
3	$a_n = 4a_{n-2} - a_{n-2}$	[1,1]
4	$a_n = a_{n-1} + 5a_{n-2} + a_{n-3} - a_{n-4}$	[0,1,1,5]
5	$a_n = 15a_{n-1} - 32a_{n-2} + 15a_{n-3} - a_{n-4}$	[1, 8, 95, 1183]
$\vdots$	$\vdots$	$\vdots$

Conjecture

Conjecture

For any fixed natural number k, the sequence formed by counting the number of ways to tile a $k \times n$ board with 1×2 dominoes satisfies a symmetric recurrence relation.

Low Order Cases

A006125 A001835 A002414 A003697 A003729 A003735 A003741 A003747 A003757 A003763 A003769 A003775 A004253 A005178 A007762 A028420 A038758 A054344

Arbitrary sequences

We were not so lucky in this case, even with well–motivated counting problems. The question then became to determine when such additional structure could be found.

Examples

EXAMPLES

That's all...

THANK YOU