2003

Combinatorial Proofs of Congruences

Jeremy Rouse
Harvey Mudd College

Combinatorial Proofs of Congruences

by

Jeremy Rouse
Arthur T. Benjamin, Advisor

Advisor: ______________________________

Second Reader: ______________________________

(Naiomi Cameron)

May 2003

Department of Mathematics

HARVEY MUDD COLLEGE

Abstract

Combinatorial Proofs of Congruences

by Jeremy Rouse

May 2003

Combinatorial techniques can frequently provide satisfying "explanations" of various mathematical phenomena. In this thesis, we seek to explain a number of well-known number-theoretic congruences using combinatorial methods. Many of the results we prove involve the Fibonacci sequence and its generalizations.

Table of Contents

Acknowledgments

I would like to thank my advisor, Professor Arthur Benjamin, for the mathematical inspiration he's given me throughout my time at Harvey Mudd College. I would also like to thank Professor Naiomi Cameron for her helpful comments and general enthusiasm.

Chapter 1

Introduction

In this thesis, we will provide combinatorial proofs of well-known number theoretic results. A *combinatorial* proof, in contrast with an algebraic proof, is a proof that relies completely (or almost completely) on counting.

Many of the results we will prove will involving Lucas sequences. A *Lucas sequence of the first kind* $U_n(a,b)$ is defined by $U_0(a,b)=0$, $U_1(a,b)=1$, and $U_n(a,b)=aU_{n-1}(a,b)+bU_{n-2}(a,b)$ for $n \geq 2$. Here a and b are nonnegative integers. In the case when $a=b=1$, we get the Fibonacci sequence

$$0,1,1,2,3,5,8,13,21,34,55,\ldots$$

A *Lucas sequence of the second kind* $V_n(a,b)$ is defined by $V_0(a,b)=2$, $V_1(a,b)=a$, and $V_n(a,b)=aV_{n-1}(a,b)+bV_{n-2}(a,b)$ for $n \geq 2$. In the case when $a=b=1$ we get the sequence of Lucas numbers

$$2,1,3,4,7,11,18,29,47,76,\ldots$$

Lucas sequences have fascinated mathematicians for many centuries (see [6], [8]). In order to prove results combinatorially involving Lucas sequences, we have to find counting questions that they answer.

The Fibonacci numbers, $U_n(1,1)$, count the ways to tile a board of length $n-1$ (a $1\times(n-1)$ rectangle) with squares (1×1 tiles) and dominoes (1×2 tiles). More generally,

Theorem 1.1. *For nonnegative integers a and b, $U_n(a, b)$ counts the ways to tile a board of length $n - 1$ with squares of a colors and dominoes of b colors.*

This can be proved by induction on n (or see [4] or [2]).

We interpret Lucas sequences of the second kind in a similar way, except we will tile "bracelets" instead of rectangles. In this case, we think of the left side of the tiling being connected to the right side of the tiling, with a "clasp" (placed at the left side of the tiling) identified.

Theorem 1.2. *For nonnegative integers a and b, $V_n(a, b)$ counts the length n bracelet tilings where each square is given one of a colors and each domino is given one of b colors.*

In any tiling, we call the ith 1×1 region in the tiling (reading from the left) the ith cell.

Using these interpretations, many results have been proven involving Fibonacci and Lucas numbers (see [4]). Also, these interpretations can be easily extended to take into account different linear recurrence relations (such as $a_n = a_{n-1} + 3a_{n-2} + 2a_{n-3}$) and different initial conditions.

In the next chapter, we will provide combinatorial proofs of basic number theoretic results, elementary combinatorial proofs of congruences involving Lucas sequences of the second kind. Then, we will build on these results, resulting in congruences involving Lucas sequences of the first kind.

In the third chapter, we will discuss integer partitions, and the partition function. I will discuss possible approaches for giving combinatorial proofs for two results involving partitions, one due to Leonhard Euler, and one due to Srinivasa Ramanujan. We will also discuss extending linear recurrence relations and their combinatorial interpretations to negative indices.

Chapter 2

Congruences

In this chapter, we will give combinatorial proofs of well-known number theoretic results (including Fermat's Little Theorem and Wilson's Theorem), a result about Lucas sequences of the second kind mod p, and finally results about Lucas sequences of the first kind mod p.

In these proofs, our idea is to partition a set into some number of equivalence classes of size p and equivalence classes of size 1. Then, to determine the size of the set mod p, it suffices to count the equivalence classes of size 1. The following lemma is a formalization of this technique that will be useful in many of the proofs.

Lemma 2.1. *Suppose that S is a finite set, p is a prime, and $f : S \to S$ is a function such that*

$$f^p(s) = s$$

for all elements s of S (here f^p denotes p compositions of f). Let $T = \{s : f(s) = s\}$. Then,

$$|S| \equiv |T| \pmod p.$$

Proof. Suppose $s \in S$ and m is the smallest positive integer such that $f^m(s) = s$. Since $f^p(s) = s$, we must have $1 \le m \le p$. Now, suppose n is a positive integer such that $f^n(s) = s$. Then, applying the division algorithm to n, there exist integers $q \ge 0$ and r such that $n = qm + r$ where $0 \le r < m$. Then, $s = f^n(s) = f^{qm+r}(s) = f^r(f^{qm}(s)) = f^r(s)$, since $f^{qm}(s) = f^m(f^m(\cdots(f^m(s)))) = s$. Hence, $f^r(s) = s$, which contradicts the minimality of m. Hence, $r = 0$ and m divides n.

Since $f^p(s) = s$ for all s, for any $s \in S$, the smallest positive integer m such that $f^m(s) = s$ divides p. Since p is prime, $m = 1$ or $m = p$.

Now, for any $n > 0$, let $n = pq + r$ where $q \geq 0$ and $0 \leq r < p$. Then,

$$f^n(s) = f^{pq+r}(s) = f^r(f^{pq}(s)) = f^r(s).$$

Now, for any $s, t \in S$, we say that $s \sim t$ if there is a positive integer k such that $f^k(s) = t$. Clearly, $\sim$ is reflexive. Also if $s \sim t$ we can choose k so that $f^k(s) = t$ and $k < p$. Then $f^{p-k}(t) = f^{p-k}(f^k(s)) = f^p(s) = s$, so $t \sim s$, so $\sim$ is symmetric. Finally, if $s \sim t$ and $t \sim u$, there are integers $k, l < p$ such that $f^k(s) = t$ and $f^l(t) = u$. Then, $f^{k+l}(s) = f^l(t) = u$, so $s \sim u$. Thus, $\sim$ is an equivalence relation.

Clearly, if $f(s) = s$, then s lies in an equivalence class of size 1. Now, if $f(s) \neq s$, then the smallest integer m such that $f^m(s) = s$ is p. Hence, if $t \sim s$, then there exists an integer k with $0 \leq k < p$ such that $f^k(s) = t$. Hence,

$$t \in (s, f(s), \ldots, f^{p-1}(s))$$

Clearly, all elements in the above p-tuple are equivalent to s. I claim that each of these elements is distinct, since if $f^i(s) = f^j(s)$ with $0 < i < j < p$, then applying f $p - j$ times to each sides gives $f^{p-j+i}(s) = s$. Since $j > i$, $0 < p - j - i < p$, a contradiction.

Hence, for all $s \in S$, the equivalence class containing s has size 1 or p. Note that the number of equivalence classes of size 1 is $|T|$, where $T = \{s : f(s) = s\}$. Thus,

$$|S| \equiv |T| \pmod{p},$$

as desired. $\square$

Using this lemma, we can easily prove many basic number theoretic results.

Theorem 2.2 (Fermat's Little Theorem). *For any integer a,*

$$a^p \equiv a \pmod{p}.$$

Proof. Consider the set S of tilings of a length p bracelet using squares of a colors, and no dominoes. Clearly, $|S| = a^p$. For $s \in S$, define $f(s)$ to be the tiling obtained by shifting every tile of s one cell to the right. It is clear that $f^p(s) = s$ for all $s \in S$. Let T be the set of tilings fixed by f. From Lemma 2.1, it follows that $|S| \equiv |T| \pmod{p}$.

Now, suppose t is fixed by f. Then, since if $j > i$ $f^{j-i}(t) = t$ and f^{j-i} sends cell i to cell j, the contents of these two cells must be the same. Thus, all the squares in t must be the same color. Conversely, if s is a tiling where all the squares are the same color, then $s \in T$. Thus, $|T| = a$. It follows that

$$a^p \equiv a \pmod{p},$$

as desired. ☐

Theorem 2.3. *If p is prime, and $V_n(a, b)$ is a Lucas sequence of the second kind, then*

$$V_p(a, b) \equiv a \pmod{p}.$$

Proof. In this case, let S be the set of length p colored bracelet tilings, where colored squares and dominoes are allowed, with a choices for squares and b choices for dominoes. From Theorem 1.2 $|S| = V_p(a, b)$. For $s \in S$ define $f(s)$ to be the tiling obtained by shifting every tile of s one cell to the right.

Let T be the set of tilings fixed by f and suppose $t \in T$. As before, if $j > i$, then f^{j-i} sends the contents of cell i to cell j. Thus, the contents of all the cells must be the same. This implies that the tiling t can contain no dominoes, since if one cell contains the beginning of a domino, every cell must contain the beginning of a domino. Also, all the squares must be the same color as well. Thus, a tiling s is fixed by f if and only if s consists of squares of the same color. Thus,

$$V_p(a, b) = |S| \equiv |T| \equiv a \pmod{p},$$

as desired. ☐

It is interesting to note that Theorem 2.3 is a special case of Theorem 2.2. Taking $b = 0$, $V_n(a, 0)$ counts the number of length n bracelet tilings with colored squares. Hence, $V_n(a, 0) = a^n$ for all n, so from Theorem 2.3, $a^p \equiv a \pmod{p}$.

Theorem 2.3 can be generalized.

Theorem 2.4. *For all $k \geq 1$,*

$$V_{kp}(a, b) \equiv V_k(a, b) \pmod{p}.$$

Proof. Let S be the set of length kp colored bracelet tilings. From Theorem 1.2 $|S| = V_{kp}(a, b)$. For $s \in S$ define $f(s)$ to be the tiling obtained by shifting every tile of s k cells to the right. Now, $f^p(s)$ rotates s by pk cells, so $f^p(s) = s$.

Now, if t is fixed by f, then if $i \equiv j \pmod{k}$, then the contents of cells i and j must be the same. Thus, t is determined entirely by the contents of cells 1 through k. Thus, any length k bracelet tiling can be extended to a length pk tiling that is fixed by f (since if the bracelet is not breakable before cell 1 then it will not be breakable before cell $k + 1$). Thus, there are $V_k(a, b)$ such tilings fixed by f. Thus,

$$V_{kp}(a, b) \equiv V_k(a, b) \pmod{p}.$$

□

One corollary of this result is that we can evaluate the right hand side explicitly when k is itself a prime power.

Theorem 2.5. *For all $e \geq 1$,*

$$V_{p^e}(a, b) \equiv a \pmod{p}.$$

Proof. We will proceed by induction on e. The case $e = 1$ has already been proven. If $e > 1$, let $k = p^{e-1}$. Then, from Theorem 2.4 and the induction hypothesis we have

$$V_{p^e}(a, b) \equiv V_{p^{e-1}}(a, b) \equiv a \pmod{p}.$$

□

Another simple number theoretic result is the following.

Theorem 2.6. *If* $0 < k < p$, *then*

$$\binom{p}{k} \equiv 0 \pmod{p}.$$

Proof. Let S be the set of all k-element subsets of $\{0, \ldots, p-1\}$. If $s \in S$, define $f(s) = \{j + 1 \bmod p : j \in s\}$. Clearly, for any $s \in S$, $f^p(s) = s$. Let T be the set of all subsets in S fixed by f. If $t \in T$ then $j \in t$ implies that $j + 1 \bmod p \in t$. Thus, if t is non-empty, $t = \{0, \ldots, p-1\}$. Hence, there are no sets fixed by f so $|T| = 0$. Thus,

$$|S| = \binom{p}{k} \equiv |T| = 0 \pmod{p},$$

as desired. □

One more classical number theoretic result that can be proved using these techniques is Wilson's theorem.

Theorem 2.7 (Wilson's). *If* p *is prime, then*

$$(p-1)! \equiv p - 1 \pmod{p}.$$

Proof. Let S be the set of permutations of $\{0, 1, 2, \ldots, p-1\}$ that contain only one cycle. If $\pi \in S$, we will represent π in cycle notation, and begin with zero. We will count the number of elements in S. For each $k \geq 1$, we have $p - k$ choices for the kth number in the cycle, so $|S| = (p-1)!$.

Let $f : S \to S$ add one to each number and reduce mod p. For example, for $p = 5$ if $\pi = (0\ 2\ 3\ 1\ 4)$, then $f(\pi) = (1\ 3\ 4\ 2\ 0) = (0\ 1\ 3\ 4\ 2)$. Then $f^p(\pi) = \pi$ for all $\pi \in S$. Let $T = \{\pi \in S : f(\pi) = \pi\}$. Suppose $\pi \in T$ and let $x = \pi(0)$.

Note that if π is written in cycle notation, then the first entry is 0 and the second entry is x. Thus, if we apply f^k to π, then the first entry in the cycle (before shifting it to begin with zero) is $k \bmod p$ and the second entry is $x + k \bmod p$. Thus, for all k, $\pi(k) = k + x \bmod p$. Now,

$$(0\ x\ \ldots) = \pi = f^k(\pi) = (k\ x+k\ \ldots).$$

In particular, when $k = x$, we have

$$(0\ x\ 2x\ \ldots) = \pi = f^x(\pi) = (x\ 2x\ 3x\ \ldots)$$

thus $f(x) = 2x \bmod p$. When $k = 2x$, $\pi(2x) = 3x \bmod p$, and inductively $\pi(nx) = (n+1)x \bmod p$. Thus, all π that satisfy $f(\pi) = \pi$ are of the form

$$(0\ x\ 2x\ 3x\ \cdots\ (p-1)x)\,.$$

for some x with $1 \leq x \leq p-1$. Conversely, it is easy to see that any permutation of this form is in T and therefore $|T| = p - 1$. Thus,

$$(p-1)! = |S| \equiv |T| \equiv p - 1 \pmod{p},$$

as desired. $\square$

Before we prove the next result, recall that if a is an integer and p is an odd prime, then the *Legendre* symbol is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \not\equiv 0 \text{ is a square } \bmod p \\ -1 & \text{if } a \text{ is not a square } \bmod p \\ 0 & \text{if p divides a.} \end{cases} \cdot$$

The following result gives a simple way to calculate Legendre symbols.

Theorem 2.8 (Euler's Criterion). *If p is an odd prime and* a *is an integer between* 0 *and p, then*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Proof. First, assume $a \equiv 0 \pmod{p}$. Then, $a^{\frac{p-1}{2}} \equiv 0 \equiv \left(\frac{a}{p}\right) \pmod{p}$.

Second, suppose $a \not\equiv 0$ is a square mod p, and choose x greater than p such that $x^2 \equiv a \pmod{p}$. Let T be the multiset containing x copies each of all length $p-1$

tilings using all squares, where each square is given one of x colors. For example, when $p = 3$, $a = 1$, and $x = 4$ with colors from $\{1, 2, 3, 4\}$,

$$\begin{aligned} T = \Big\langle\, & \overbrace{\square}^{1}\overbrace{\square}^{1}, \overbrace{\square}^{1}\overbrace{\square}^{1}, \overbrace{\square}^{1}\overbrace{\square}^{1}, \overbrace{\square}^{1}\overbrace{\square}^{1} \\ & \overbrace{\square}^{1}\overbrace{\square}^{2}, \overbrace{\square}^{1}\overbrace{\square}^{2}, \overbrace{\square}^{1}\overbrace{\square}^{2}, \overbrace{\square}^{1}\overbrace{\square}^{2}, \ldots \\ & \overbrace{\square}^{4}\overbrace{\square}^{4}, \overbrace{\square}^{4}\overbrace{\square}^{4}, \overbrace{\square}^{4}\overbrace{\square}^{4}, \overbrace{\square}^{4}\overbrace{\square}^{4} \Big\rangle. \end{aligned}$$

Since there are x^{p-1} colored tilings of length $p-1$, and each is listed x times, we have $|T| = x^p$. From Fermat's Little Theorem, it follows that $|T| \equiv x \pmod{p}$. Let $U \subset T$ be the multiset of x copies of each length $p-1$ tiling where for all $1 \leq j \leq \frac{p-1}{2}$, cells $2j-1$ and $2j$ receive the same color, and that color is chosen from the set $\{1, \ldots, a\}$. Here, $|U| = xa^{\frac{p-1}{2}}$. Next, we claim that $|T - U| \equiv 0 \pmod{p}$.

Note that a length $p-1$ colored square-tiling is in $T-U$ if and only if there exists a $1 \leq j \leq \frac{p-1}{2}$ such that cells $2j-1$ and $2j$ are filled with two squares of different colors, or with two squares one of whose colors is larger than a. If we condition on the smallest such j, we have that for $1 \leq k \leq j-1$, the squares in cells $2k-1$ and $2k$ may be colored a ways and 1 way, respectively. The squares in cells $2j-1$ and $2j$ may be colored in $x^2 - a$ ways, since we must rule out the cases when these two squares are both the same color and that color is less than or equal to a. Finally, if $j < k \leq \frac{p-1}{2}$, there are x^2 ways to color cells $2k-1$ and $2k$. Further, there are x copies of each tiling, and this gives that

$$|T - U| = x \sum_{j=1}^{\frac{p-1}{2}} a^{j-1}(x^2 - a)x^{p-1-2j}.$$

By assumption, $x^2 \equiv a \pmod{p}$, so $|T - U| = |T| - |U| \equiv 0 \pmod{p}$. This gives that

$$x \equiv |T| \equiv |U| = xa^{\frac{p-1}{2}} \pmod{p}.$$

Since $\gcd(a,p)=1$, $\gcd(x,p)=1$. Therefore,

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

as desired.

Finally, suppose that a is not a square mod p. We aim to show that $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Let T' be the set of all tilings of length $p-1$ using only squares, where for $1 \leq i \leq \frac{p-1}{2}$ the ith square may be assigned a color from the set $\{1,2,\ldots,p+i\}$.

Thus, $|T'| = (p+1)(p+2)\cdots(2p-1)$. Now, we could use modular arithmetic and Wilson's theorem to get $|T'| \equiv (p-1)! \equiv -1 \pmod{p}$, but we prefer a more combinatorial approach. Let $U' \subset T'$ be the set of all tilings for which there exists an $1 \leq i \leq \frac{p-1}{2}$ such that the ith square is assigned a color from the set $C_i = \{i+1, i+2, \ldots, i+p\}$.

Now, for $u \in U'$, condition on the smallest j such that the color of the jth square is in C_j. For $i < j$, square i can be given color $1,2,\ldots,i-1$ or i. Thus, there are i choices for the color of square i. For $i = j$, square j has p choices. For $i > j$, then square i can be given any color from 1 to $p+i$. Hence, for each j, there are

$$(j-1)!p\prod_{k=j}^{p-1}(p+k)$$

tilings. Summing over j, we get that

$$|U'| = p\sum_{j=1}^{p-1}(j-1)!\prod_{k=j}^{p-1}(p+k).$$

Since $U' \subset T'$, and $|U'| \equiv 0 \pmod{p}$, $|T'| \equiv |T' - U'| \pmod{p}$. Now, $T' - U'$ is the set of all tilings for which the ith square is given color $1,2,\ldots,i-1$ or i. Thus, $|T' - U'| = (p-1)!$, so $|T'| \equiv |T' - U'| \equiv (p-1)!$. By Wilson's theorem, $(p-1)! \equiv p-1 \equiv -1 \mod p$.

Our goal remains to prove that if a is not a square mod p, then $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

Let $S = \{1, 2, \ldots, p-1\}$. For $x, y \in S$, we say that $x \sim y$ if $xy \equiv a \pmod{p}$. If $x \sim y$, then $x \neq y$ since a is not a square mod p. Also, if $x \sim y$, and $x \sim z$, then $xy \equiv xz$, so $y \equiv z \pmod{p}$, and therefore $y = z$.

For each tiling in $t \in T'$, we will rearrange the squares as follows, constructing a new tiling t' (which might not be in T'). We construct the tiling from left to right two squares at a time. Begin the tiling with the first square from t and the ath square from t. Then, at each successive step, take the smallest number k in S such that the kth square in t has not been placed. Append the kth square to the tiling and then append the lth square, where l is the unique integer such that $kl \equiv a \pmod{p}$.

Note that $l > k$, since if $l < k$, then the lth square would already have been placed next to some integer $m \neq k$. Then, $l \sim m$ and $l \sim k$, implying that $k \equiv m \pmod{p}$, a contradiction.

Continue this process until all $p-1$ squares have been placed. For $1 \leq i \leq p-1$, let n_i be the cell (in t) that the ith square in t' came from.

For example, if $a = 3$ and $p = 7$, we rearrange a length 6 tiling

$$\overbrace{\square}^{1}\overbrace{\square}^{2}\overbrace{\square}^{3}\overbrace{\square}^{4}\overbrace{\square}^{5}\overbrace{\square}^{6},$$

as follows. We begin the tiling with squares 1 and 3. Then, 2 is the smallest number that hasn't been placed, so we append square 2 and square 5 ($2 \cdot 5 = 10 \equiv 3 \pmod{7}$). Then, we append squares 4 and 6 ($4 \cdot 6 = 24 \equiv 3 \pmod{7}$). This gives

$$\overbrace{\square}^{1}\overbrace{\square}^{3}\overbrace{\square}^{2}\overbrace{\square}^{5}\overbrace{\square}^{4}\overbrace{\square}^{6},$$

and hence $n_1 = 1$, $n_2 = 3$, $n_3 = 2$, $n_4 = 5$, $n_5 = 4$ and $n_6 = 6$.

Let W be the set of all the new tilings t'. Clearly, $|W| = |T'|$, since each tiling $w \in W$ was obtained by rearranging the squares in a tiling $t \in T'$. Note that for any tiling $t' \in W$, the number of ways to color the square in cell i is $p + n_i$.

I claim that $|W| \equiv a^{\frac{p-1}{2}} \pmod p$.

Let $X \subset W$ be the set of tilings such that the squares in cells $2k-1$ and $2k$ always have the same color, and that color is chosen from $\{1, 2, \ldots, a\}$. Clearly, $|X| = a^{\frac{p-1}{2}}$. We will now show that

$$|W - X| = \sum_{j=0}^{\frac{p-1}{2}} a^{j-1} \left(\left(p + n_{2j-1}\right)\left(p + n_{2j}\right) - a \right) \prod_{k=2j+1}^{p-1} p + n_k.$$

If z is a tiling in $W - X$, then there exists a j with $1 \leq j \leq \frac{p-1}{2}$ such that the squares in cells $2j-1$ and $2j$ either do not have the same color, or the color of one of the two squares is greater than a.

We condition on the smallest such j. In this case, there are a ways to color squares $2k-1$ and $2k$ for $k < j$. Then, there are

$$\left(p + n_{2j-1}\right)\left(p + n_{2j}\right) - a$$

ways to color square j, since the squares in cells $2j-1$ and $2j$ can be given any color from 1 to $p + n_{2j-1}$ or 1 to $p + n_{2j}$ except that they cannot both receive colors $1, 2, \ldots, a-1$ or a.

Now, for $k > 2j$, the square in cell k can receive $p + n_k$ colors. Hence, for a given j the number of tilings is

$$a^{j-1} \left(\left(p + n_{2j-1}\right)\left(p + n_{2j}\right) - a \right) \prod_{k=2j+1}^{p-1} p + n_k.$$

Summing over j gives that

$$|W - X| = \sum_{j=0}^{\frac{p-1}{2}} a^{j-1} \left(\left(p + n_{2j-1}\right)\left(p + n_{2j}\right) - a \right) \prod_{k=2j+1}^{p-1} p + n_k.$$

Now, the squares were arranged so that $n_{2j-1}n_{2j} \equiv a \pmod p$ for all j and therefore

$$\begin{aligned}(p+n_{2j-1})(p+n_{2j})-a &\equiv p^2+p(n_{2j-1}+n_{2j})+n_{2j-1}n_{2j}-a\\ &\equiv n_{2j-1}n_{2j}-a\\ &\equiv 0 \pmod{p}.\end{aligned}$$

Hence, the total number of tilings in $|W-X|$ is a multiple of p.

Thus, $|W| \equiv |X| \equiv a^{\frac{p-1}{2}} \pmod{p}$, as desired.

Finally,

$$-1 \equiv |T'| \equiv |W| \equiv a^{\frac{p-1}{2}} \pmod{p},$$

and the result follows. □

Finally, using the material above, we can prove the following result involving Lucas sequences of the first kind.

Theorem 2.9. *If p is an odd prime, then*

$$U_p(a,b) \equiv \left(\frac{a^2+4b}{p}\right) \pmod{p}.$$

Before we can prove this, we will need the following identity involving Lucas sequences of the first kind. This is a generalization of an identity from [1] with a simpler combinatorial proof.

Theorem 2.10. *If $n \geq 1$, then*

$$2^n U_{n+1}(a,b) = \sum_{k=0}^{n} \binom{n}{k} a^{n-2\lfloor \frac{k}{2} \rfloor} \left(a^2+4b\right)^{\lfloor \frac{k}{2} \rfloor}.$$

Proof. Recall that $U_{n+1}(a,b)$ counts the number of length n tilings with squares of a colors and dominoes of b colors. Thus, $2^n U_{n+1}(a,b)$ counts the number of length n tilings where each square can be given one of $2a$ colors and each domino one of $4b$ colors (this gives twice as many options per cell, hence the 2^n). We will say that a of the square colors are “light” and a of them are “dark”.

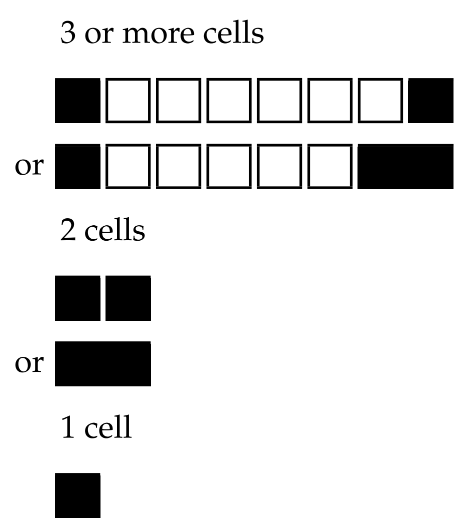
We will show that every k-element subset S of $\{1,\ldots,n\}$ generates exactly

$$a^{n-2\lfloor\frac{k}{2}\rfloor}\left(a^2+4b\right)^{\lfloor\frac{k}{2}\rfloor}$$

tilings.

Suppose $S=\{x_1,\ldots,x_k\}$, where $x_1<x_2<\ldots<x_k$. Define for $j=1,\ldots,\lfloor\frac{k}{2}\rfloor$ the interval $I_j=[x_{2j-1},x_{2j}]$. If k is odd, we also create the single point interval $I_{\frac{k+1}{2}}=[x_k,x_k]$.

Now, any cell not belonging to one of the I_j is colored with a light square. An interval with three or more cells may be tiled by a dark square followed by a string of light squares, then ending with a dark square. It may also be tiled by a dark square, followed by a string of light squares (possibly zero if the interval has three cells), followed by a domino. An interval of length 2 may be tiled by two dark squares or it may be tiled by a domino. An interval of length 1 (which occurs only in the case when k is odd) must be tiled by a dark square.



Note that there are $\lfloor\frac{k}{2}\rfloor$ intervals of length 2 or more. Each interval of length 2 or more contains either two dark squares (which may be chosen a^2 ways) or a domino (which may be chosen $4b$ ways). Every other tile (regardless of whether or not it is contained in an interval) is a square with a prescribed shade (light or dark), and therefore can be chosen exactly a ways. Thus, the set S generates

$$\left(a^2+4b\right)^{\lfloor \frac{k}{2} \rfloor} a^{n-2\lfloor \frac{k}{2} \rfloor}$$

tilings.

Conversely, given a length n tiling t, we construct the unique set S that generates t. By our construction, every cell occupied by a light square is not in S. Every cell occupied by a dark square or the second half of a domino must be in S. It remains to determine if $j \in S$ when cell j is covered by the first half of a domino. If a domino covers cells j and $j+1$, j may or may not be in S, depending on whether or not the domino is in an interval of length 2 or in an interval of length 3 or more, respectively. Certainly if $j = 1$, then $j \in S$.

Suppose that for all $i < j$, it has already been determined whether $i \in S$ or $i \notin S$. If there are an even number of $i < j$ in S, then the domino must be at the start of an interval, and hence in an interval of length 2. In this case, $j \in S$. Otherwise, the domino is at the end of an interval of length 3 or more, so $j \notin S$.

Thus, given a tiling, it is possible to find a unique set S that generated it, so the identity holds. $\square$

Now we will prove Theorem 2.9. The proof will use algebraic manipulations, together with the results that we have proven above.

Proof. Suppose that p is an odd prime. Then, we have that

$$U_{p+1}(a,b) = aU_p + bU_{p-1} \qquad (1).$$

Also, from Theorem 2.10,

$$2^p U_{p+1}(a,b) = \sum_{k=0}^{p} \binom{p}{k} a^{p-2\lfloor \frac{k}{2} \rfloor} \left(a^2+4b\right)^{\lfloor \frac{k}{2} \rfloor}. \qquad (2)$$

Since $\binom{p}{k} \equiv 0 \pmod{p}$ if $0 < k < p$, the only nonzero terms (mod p) are when $k = 0$ and $k = p$. Thus

$$2^p U_{p+1}(a,b) \equiv a^p + a^{p-2\lfloor \frac{p}{2} \rfloor} \left(a^2 + 4b\right)^{\lfloor \frac{p}{2} \rfloor} \pmod{p}.$$

From Fermat's Little Theorem, $2^p \equiv 2 \pmod{p}$, $a^p \equiv a \pmod{p}$. Further, since p is odd, $\lfloor \frac{p}{2} \rfloor = \frac{p-1}{2}$. Also, from Theorem 2.8, we have that

$$\left(a^2 + 4b\right)^{\frac{p-1}{2}} \equiv \left(\frac{a^2 + 4b}{p}\right).$$

Combining these, we get

$$2U_{p+1}(a,b) \equiv a + a\left(\frac{a^2 + 4b}{p}\right) \pmod{p}. \tag{3}$$

It can be seen combinatorially that

$$V_n(a,b) = aU_n(a,b) + 2bU_{n-1}(a,b) \tag{4}$$

for $n \geq 2$ since $aU_n(a,b)$ counts the number of n-bracelets with a square on cell 1, and $2bU_{n-1}(a,b)$ counts the number of n-bracelets with a domino on cell 1. In particular, taking $n = p$ it follows from (4) and from Theorem 2.3 that

$$aU_p(a,b) + 2bU_{p-1}(a,b) = V_p(a,b) \equiv a \pmod{p}. \tag{5}$$

Setting $U_{p+1}(a,b) = aU_p(a,b) + bU_{p-1}(a,b)$ in (3) leads to

$$2aU_p(a,b) + 2bU_{p-1}(a,b) \equiv a + \left(\frac{a^2 + 4b}{p}\right) \pmod{p}. \tag{6}$$

Subtracting (5) from (6) gives us

$$aU_p(a,b) \equiv a\left(\frac{a^2 + 4b}{p}\right) \pmod{p}.$$

If p does not divide a, then

$$U_p \equiv \left(\frac{a^2 + 4b}{p}\right) \pmod{p}.$$

We will show that the same conclusion is true if $p|a$.

First we claim that for even numbers n,

$$U_{n+1}(a,b) = b^{n/2} + a \sum_{k=0}^{n/2-1} b^k U_{n-2k}(a,b). \tag{7}$$

The left hand side counts the number of colored tilings of length n. We condition on the location of the first square in the tiling. If there is no such square, the tiling consists of all dominoes. Such a tiling can be created in $b^{n/2}$ ways. If there is a square, and the first square lies in cell $2k+1$, it must be preceded by k dominoes, and followed by a colored tiling of length $n-2k-1$. There are

$$b^k a U_{n-2k}(a,b),$$

such tilings. Summing over k yields (7).

Now, if $p|a$, then taking $n = p-1$, an even number, in the above identity gives

$$\begin{aligned} U_p &= b^{\frac{p-1}{2}} + a \sum_{k=0}^{(p-3)/2} b^k U_{n-2k} \\ &\equiv b^{\frac{p-1}{2}} \\ &\equiv \left(\frac{b}{p}\right) \pmod{p}. \end{aligned}$$

Now, b is a square mod p if and only if $4b$ is. Since $p|a$, $4b \equiv a^2 + 4b \pmod{p}$, so

$$\left(\frac{b}{p}\right) = \left(\frac{4b}{p}\right) = \left(\frac{a^2+4b}{p}\right).$$

Thus,

$$U_p \equiv \left(\frac{a^2+4b}{p}\right) \pmod{p},$$

as desired. $\square$

A number of corollaries can be drawn from this.

Corollary 2.11. *If p is an odd prime, and $F_p = U_p(1,1)$ is the pth Fibonacci number, then $F_p \equiv 1 \pmod{p}$ if $p = 5k \pm 1$ and $F_p \equiv -1 \pmod{p}$ if $p = 5k \pm 2$.*

For example, if $p = 7$, $F_7 = 13 \equiv -1 \pmod 7$. Also, if $p = 19$, $F_{19} = 4181 = 220 \cdot 19 + 1 \equiv 1 \pmod{19}$.

Proof. From Theorem 2.9,

$$F_p \equiv \left(\frac{5}{p}\right).$$

From the law of quadratic reciprocity, if p and q are distinct odd primes, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Hence, in the case that $q = 5$, we have that

$$\left(\frac{p}{5}\right)\left(\frac{5}{p}\right) = (-1)^{2\cdot\frac{q-1}{2}} = (-1)^{q-1} = 1.$$

Thus,

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right).$$

Since p is a square mod 5 if and only if $p \equiv 1, 4 \pmod 5$, the desired result follows.

□

Theorem 2.9 can help determine other members in Lucas sequences of the first kind mod p. From [3], we have a combinatorial proof of the identity

$$U_{mr}(a,b) = \sum_{j=1}^{r} \binom{r}{j} U_j(a,b) U_m^j(a,b) b^{r-j} U_{m-1}^{r-j}(a,b).$$

If we take $r = p$, the only nonzero term (mod p) is when $j = p$. This gives

$$U_{mp}(a,b) \equiv U_p(a,b) U_m^p(a,b) \pmod p.$$

From Fermat's little theorem, we have that $U_m^p(a,b) \equiv U_m(a,b) \pmod p$. Therefore from this congruence and Theorem 2.9 we have the following result from [6].

Corollary 2.12. *If m is a positive integer and p is and odd prime, then*

$$U_{mp}(a,b) \equiv \left(\frac{a^2+4b}{p}\right) U_m(a,b) \pmod p.$$

Here is another result from [6].

Corollary 2.13. *For all $e \geq 1$, if p is an odd prime then*

$$U_{p^e}(a,b) \equiv \left(\left(\frac{a^2+4b}{p}\right)\right)^e \pmod{p}.$$

Proof. The result is clearly true for $e = 1$. Now, if it is true for e, then from Corollary 2.12

$$\begin{aligned} U_{p^{e+1}}(a,b) &\equiv \left(\frac{a^2+4b}{p}\right) U_{p^e}(a,b) \pmod{p} \\ &\equiv \left(\frac{a^2+4b}{p}\right)\left(\left(\frac{a^2+4b}{p}\right)\right)^e \\ &\equiv \left(\left(\frac{a^2+4b}{p}\right)\right)^{e+1} \pmod{p}. \end{aligned}$$

□

One simple corollary of this is that if p does not divide a^2+4b then $\gcd(a^2+4b, p) = 1$. Thus,

$$U_{p^2}(a,b) \equiv \left(\left(\frac{a^2+4b}{p}\right)\right)^2 \equiv 1 \pmod{p}.$$

Chapter 3

Further Work

3.1 Integer Partitions

The partition function $p(n)$ counts the number of ways to represent the n as the sum of a non-increasing sequence of positive integers. For example, $p(4) = 5$ since

$$\begin{aligned} 4 &= 4 \\ &= 3+1 \\ &= 2+2 \\ &= 2+1+1 \\ &= 1+1+1+1. \end{aligned}$$

For convenience we define $p(0) = 1$ and $p(k) = 0$ if $k < 0$. $p(n)$ can be thought of as the number of ways to tile a board of length n with tiles of any size, but with the restriction that the tile lengths cannot increase from left to right.

The partition function has fascinated mathematicians for many years. In fact, one of the results I'd like to find a combinatorial proof for is due to Euler and states that

$$\begin{aligned} p(n) = {} & p(n-1) + p(n-2) - p(n-5) - p(n-7) \\ & + p(n-12) + p(n-15) - p(n-22) - p(n-26) + \cdots . \end{aligned}$$

The sequence $1, 2, 5, 7, \ldots$ is the set of numbers of the form

$$\frac{3k^2 \pm k}{2}.$$

Combinatorial proofs of this are known, and Bressoud and Zeilberger give an elegant bijective proof in [5].

However, my approach is different from that of Bressoud and Zeilberger. I define $q_k(n)$ to be the number of partitions of n with all parts having size k or greater. Using the following lemma, we can express $q_k(n)$ in terms of $p(n)$.

Lemma 3.1. *For $k \geq 1$ and a positive integer n,*

$$q_{k+1}(n) + q_k(n-k) = q_k(n).$$

Proof. Given a partition of n with all parts larger than or equal to k, either the last part is of size k or not. If it is not, then the last part has size $k+1$ or greater, and since the parts are in non-increasing order, all parts have size $k+1$ or greater. The number of such partitions is $q_{k+1}(n)$. On the other hand, if the last part has size k, removing this part gives a partition of $n-k$ where all parts have size k or greater. Conversely, given a partition of $n-k$ into parts of size k or greater, adding k gives a partition of n with all parts of size k or greater. Hence, in the second case, there are $q_k(n-k)$ partitions. Thus, the result holds. $\square$

Since $q_1(n) = p(n)$ and $q_{k+1}(n) = q_k(n) - q_k(n-k)$, we have

$$\begin{aligned}
&q_1(n) = p(n)\\
&q_2(n) = p(n) - p(n-1)\\
&q_3(n) = p(n) - p(n-1) - p(n-2) + p(n-3)\\
&q_4(n) = p(n) - p(n-1) - p(n-2) + p(n-4) + p(n-5) - p(n-6)\\
&q_5(n) = p(n) - p(n-1) - p(n-2) + 2p(n-5) - p(n-8) - p(n-9) + p(n-10)\\
&q_6(n) = p(n) - p(n-1) - p(n-2) + p(n-5) + p(n-6) + p(n-7) - p(n-8)\\
&\qquad - p(n-9) - p(n-10) + p(n-13) + p(n-14) - p(n-15)
\end{aligned}$$

Clearly, for a fixed $n \geq 2$, $q_n(n+1) = 0$. Plugging in this expression above gives special cases of the desired formula for $n = 1, 2, \ldots, 6$. Generalizing this argument would lead to the result.

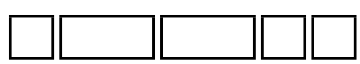
Another result (that is actually a congruence) that I wish to investigate is one discovered by the well-known Indian mathematician Ramanujan.

Theorem 3.2. *If n is a non-negative integer, then*

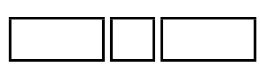
$$p(5n + 4) \equiv 0 \pmod 5.$$

This result, although very simple to state is rather difficult to prove. In fact, according to Dr. Bruce Berndt at the University of Illinois, Urbana-Champaign, no combinatorial proof of this fact is known, although there have been many attempts by people such as Freeman Dyson to find such a proof. One possible combinatorial approach to this problem is the following.

Given a partition of n, we can turn it into a square-domino tiling of length n in the following way. Take each part that has size 2 or greater and turn it into some number of squares (possibly zero) followed by a domino. Then, we add a square for each part of size 1. For example, if we have $7 = 3 + 2 + 1 + 1$, the corresponding tiling is

.

Now, not all length n tilings correspond to partitions. For example, if $n = 5$ the following tiling



does not correspond to a partition. However, it is known that if $m|n$, then $F_m|F_n$ (for a combinatorial proof, see [3]). Taking $m = 5$, we get that if $5|n$, then $5 = F_5|F_n$. Hence, F_{5n+5}, the number of tilings of length $5n + 4$, is a multiple of 5. It suffices to prove that the number of tilings of length $5k+4$ that do not correspond to partitions is a multiple of 5.

So far, I have been able to find an expression for the number of tilings that do not correspond to partitions. I give the result below.

Theorem 3.3. *If n is a positive integer, then*

$$F_{n+1} - p(n) = \sum_{a+b+c \leq n, b \geq 2, c > b} F_{c-1}\, q_b(a-b).$$

Proof. Given a tiling that does not correspond to a partition, we divide it into four sections.

i) A region where the tiles are in non-increasing order. (This region cannot be empty).

ii) The first tile that isn't in non-increasing order (this tile must be larger than the tile immediately before it).

iii) A region containing some tiling with tiles of length 2 or greater that need not be in any particular order (this region can be empty).

iv) Some number of squares (this region can also be empty).

Then, if region (i) has length a and ends with a tile of length b (b must be greater than or equal to 2), the number of ways to tile it is $q_b(a-b)$. If region (ii) has length c (c must be greater than b), then there is one tile of length c in it, and one way to tile the region. If region (iii) region has length c, then the number of ways to tile it is F_{c-1}. In any case, there is only one way to tile region (iv). This gives

$$F_{n+1} - p(n) = \sum_{a+b+c \leq n, b \geq 2, c > b} F_{c-1}\, q_b(a-b),$$

as desired. □

This result, unfortunately, makes it appear that it is difficult to divide the tilings that do not correspond to partitions into groups of 5. It is possible that further work in this area might shed some insight. Another approach would be to apply some of the techniques of Garcia and Milne as described in [7].

3.2 Combinatorial Interpretation of Negative Indices

Normally, the Fibonacci numbers are defined by $F_0 = 0$, $F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$. However, we can extend this definition by insisting that

$$F_n = F_{n-1} + F_{n-2}$$

be valid for all integers n. For example, we must have that $F_{-1} + F_0 = F_1$, so $F_{-1} = 1$. Similarly, $F_{-2} = -1$, $F_{-3} = 2$, and the pattern continues with

$$-3, 5, -8, 13, -21, 34, -55, 89, \ldots$$

leading us to conjecture that for all integers n, $F_n = (-1)^n F_{-n}$.

Perhaps there is a way of extending our combinatorial interpretation of the Fibonacci numbers to count F_n when n is negative. This is what we shall do.

Notice that we can obtain the length n tiling given the length $n + 1$ tilings and $n + 2$ tilings with the following procedure.

i) Add a square to each of the $(n + 1)$-tilings.

ii) Subtract this set from the set of $(n + 2)$-tilings.

iii) Remove a domino from each tiling in the resulting set.

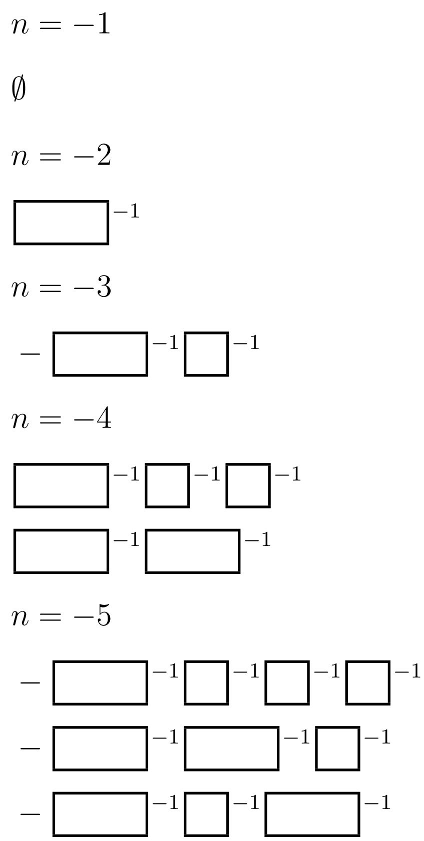
When n is non-negative, every $(n + 2)$-tiling is created from an $(n + 1)$-tiling by adding a square or from an n-tiling by adding a domino. Thus, after step ii) above, each tiling remaining will be an n-tiling followed by a domino.

We can carry out this procedure when n is negative as well, provided we can make sense of "subtract" and "remove a domino" in these circumstances. We will apply the procedure when $n = -1$. There is one length 1-tiling, and one "empty" 0-tiling. Hence, by adding a square to the 0-tiling and subtracting from the 1-tiling, we end up with the empty set, and hence step iii) has no effect. This implies that the set of -1-tilings is empty and therefore $F_0 = 0$.

Applying the procedure when $n = -2$ runs into a little problem. Here, the set of $(n+1)$-tilings is empty, so subtracting this set from the set of $n = 0$ tilings is easy. However, removing a domino from the length 0 empty tiling is problematic. To get around this, we postulate the existence of an "anti-domino", denoted by $\boxed{\quad\;}^{-1}$ with length -2 and the property that $\boxed{\quad\;}\boxed{\quad\;}^{-1} = \boxed{\quad\;}^{-1}\boxed{\quad\;} = |$, the empty tiling. This implies that there is a single -2-tiling, namely an anti-domino.

Applying the procedure when $n = -3$ runs into a different problem. Here, in step ii), we must subtract the set of -2-tilings with a square appended from the empty set. To get around this, we will assign weights to our tilings, and assign the one resulting length -3 tiling a weight of -1. This results in the tiling $-\boxed{\quad\;}^{-1}\square\boxed{\quad\;}^{-1}$.

To ease notation when working with negative index tilings we will introduce the notation $\square^{-1} = \square\boxed{\quad\;}^{-1}$ and permit $\square^{-1}$ to be a *right* inverse of $\square$. The tile $\square^{-1}$ will be called an "anti-square." Hence, $\square\square^{-1} = |$, the empty tiling, but $\square^{-1}\square$ cannot be simplified in the same way. The result is that to obtain the $-n$-tilings, we add an anti-square to the end of each $-(n-1)$-tiling and negate and add an anti-domino to the end of each $-(n-2)$-tiling. Using this notation, we find that the negative index tilings are as follows.



We notice that the length $-n$ tilings are (up to sign) an anti-domino followed by a length $(n-2)$ tiling. If this is true, we would have $|F_{-n+1}| = |F_{n-1}|$ since F_{-n+1} is the number of length $-n$ tilings and F_{n-1} is the number of length $n-2$ tilings. In fact, this result follows from our inductive definition of the length $-n$ tilings.

Theorem 3.4. *If n is an integer, $F_{-n} = (-1)^n F_n$.*

Proof. It suffices to demonstrate the result for $n > 0$. We will prove this by strong induction on n.

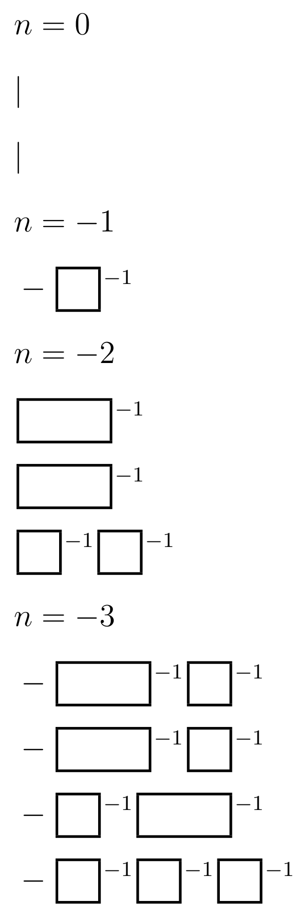
From our observations above, it is clear that the single length -2 tiling is an anti-domino followed by the length 0 tiling. Hence, the result is true for $n = 1$.

Suppose that for $k = 1, 2, \ldots, n-1$, the length $-k$ tilings (up to sign) are the an anti-domino followed by a length $k-2$ tiling with squares and dominoes replaced by anti-squares and anti-dominoes. Suppose further that the sign of all $(-k)$-tilings is the same and is $(-1)^k$.

To get the $(n-2)$-tilings, we append squares to the length $n-3$ tilings and dominoes to the length $n-4$ tilings. To get the length $-n$ tilings, we append anti-squares to the length $-(n-1)$-tilings and anti-dominoes to the length $-(n-2)$-tilings. Hence, if sign is not considered, the length $-n$ tilings are an anti-domino followed by an anti-$(n-2)$-tiling.

Now, if $n-2$ is even, all the length $-(n-2)$ tilings are positive and length $-(n-1)$ tilings are negative. Thus, the resulting $(-n)$-tilings will be positive. Similarly, if n is odd, the length $-(n-2)$ tilings are negative and the $-(n-1)$-tilings are positive, so the length $-n$ tilings will be negative, and the result follows. $\square$

Notice that the procedure for obtaining length n tilings from the $n+1$ and $n+2$ tilings works for a recurrence relationship of the form $a_{n+2} = a_{n+1} + a_n$. Hence, we can expect the same idea to work for Lucas numbers as well. Here we will think of the multiset of length n Lucas tilings as square and domino tilings where if a tiling begins with a domino it has multiplicity two. One subtlety in this case is that the empty tiling has multiplicity two. Applying the procedure described above we obtain the length n Lucas tilings for a non-positive integer n.



Here, it appears that the length $-n$ tilings are (up to sign) anti-n tilings. It is easy to prove this by induction, giving the following result.

Theorem 3.5. *For any integer n, $L_{-n} = (-1)^n L_n$.*

The interpretations of negative index Fibonacci and Lucas sequences can be used to prove a well-known identity involving them.

Theorem 3.6. *If n is an integer, then $L_n = F_{n+1} + F_{n-1}$.*

Proof. I claim that if a domino is added to the left side of all length $n-2$ Fibonacci tilings, the resulting set, together with the length n Fibonacci tilings, will equal the set of Lucas tilings.

This is clear if $n \geq 2$, since in this case, we will have two copies of each tiling that begins with a domino. For $n = 1$, notice that the Fibonacci tilings and Lucas tilings are the same and that the set of length -1 Fibonacci tilings is empty. For $n = 0$, there are two empty Lucas tilings. There is a single empty Fibonacci tiling of length 0 and appending a domino to the anti-domino in the length -2 Fibonacci tiling gives two empty tilings.

Now, suppose that $n < 0$. Then, the length n Fibonacci tilings all begin with an anti-domino. Adding a domino to the beginning of each length $n-2$ Fibonacci tiling cancels the anti-domino there, and gives all anti-n-tilings. Thus, from the length $n-2$ Fibonacci tilings, we have one copy each of the tilings beginning with squares, and one copy each of the tilings beginning with dominoes, and from the length n Fibonacci tilings, we have an additional copy of each tiling beginning with a domino. Finally, n and $n-2$ have the same parity, and hence all the tilings considered have the same sign. Thus, the result follows. □

Now, we will define the Gibonacci (a, b) sequence by $G_0(a, b) = b$, $G_1(a, b) = a$, and

$$G_n(a, b) = G_{n-1}(a, b) + G_{n-2}(a, b).$$

Here, $G_n(a, b)$ counts the multiset of length n tilings where each tiling beginning with a square has multiplicity a and each tiling beginning with a domino has multiplicity b. Hence, $G_n(1, 1) = F_{n+1}$ and $G_n(1, 2) = L_n$. Since the Gibonacci sequence has the same recurrence relation as the Fibonacci and Lucas sequences, the procedure described above gives a combinatorial interpretation of $G_n(a, b)$ for all integers n. For example, consider the sequence $G_n(1, 4)$. It begins with $G_0(1, 4) = 4$ and continues with

$$4, 1, 5, 6, 11, 17, 28, 45, 73, \ldots.$$

For non-positive n, we get

$$4, -3, 7, -10, 17, -27, 44, -71, \ldots$$

Hence, it appears that $G_{-n}(1,4) = (-1)^n G_n(3,4)$. This is a special case of the following result.

Theorem 3.7. *For any integer n,*

$$G_{-n}(a,b) = (-1)^n G_n(b-a,b).$$

Proof. Again it suffices to prove the result for $n \geq 0$.

First, it is easy to see that there are $G_0(a,b) = b$ copies of the length 0 empty tilings, and $G_{-1}(a,b) = a-b$ anti-square tilings. These tilings are the negation of the $G_1(b-a,b)$ tilings.

To construct the length -2 tilings, we add an anti-square to each -1 tiling and negate. Then, we add an anti-domino to each length 0 tiling. Hence, there are $b-a$ anti-square anti-square tilings, and b domino tilings. Hence, $G_{-2}(a,b) = G_2(b-a,b)$. Notice that in each of these cases, the anti-square tilings are all of the same sign and the anti-domino tilings are all of the same sign (though these signs need not be the same).

Now, assume the result is true for $n = 1, 2, \ldots, k-1$ with $k-1 \geq 2$. We will prove that (up to sign) the length $-k$ $G_{-k}(a,b)$ tilings are the same as the length k $G_k(b-a,b)$ tilings. Further, all the square tilings are the same sign and all the domino tilings are the same sign.

To create the length $-k$ $G_{-k}(a,b)$ tilings, we simply add an anti-square to each length $-(k-1)$ tiling and negate, and add an anti-domino to the length $-(k-2)$ tilings. Thus, up to sign, the length $-k$ tilings are the same as the length k, $G_k(b-a,b)$ tilings. Now, it is easy to see that the sign on a tiling will be determined by the parity of the number of anti-squares in it, since a tiling changes sign if and only if an anti-square is added to it. Further, in a tiling of length $-k$, if there are s anti-squares and d anti-dominoes, $s + 2d = k$. Hence, $s \equiv k \pmod 2$, so all the tilings beginning with an anti-square are the same sign and all the tilings beginning with an anti-domino are the same sign.

Now, if $b - a \geq 0$, all the length -1 tilings were negative and hence a tiling beginning with an anti-square is positive if and only if its length is even. In this case, all length k tilings have the same sign and since the $G_k(b-a, b)$ are equal (up to sign) to the $G_{-k}(a, b)$, it follows that $G_{-k}(a, b) = (-1)^k G_k(b-a, b)$.

On the other hand, if $b - a < 0$, all the length -1 tilings were positive and hence a tiling beginning with an anti-square is positive if and only if its length is odd. In this case, the tilings beginning with an anti-square and with an anti-domino always have a different sign. In this case, the $G_k(b-a, b)$ tilings that begin with a square are always negative and the tilings that begin with a domino are always positive. In this case, the $G_{-k}(a, b)$ tilings are negative if and only if they contain an even number of squares, which happens if and only if k is even. Hence, it follows that $G_{-k}(a, b) = (-1)^k G_k(b-a, b)$, as desired. □

While this result provides a workable interpretation of the Gibonacci sequence, one direction of future work is to determine if there is a better one in general or one that works in other special cases.

In addition, looking at an interpretation of other linear recurrence relations for negative indices might be interesting. For example, if we have $a_n = a_{n-1} + 2a_{n-2}$, with $a_0 = 2$ and $a_1 = 1$, we have that for negative n the sequence continues

$$-\frac{1}{2}, -\frac{3}{4}, -\frac{1}{8}, \frac{5}{16}, \frac{7}{32}, \ldots.$$

Finding a combinatorial interpretation for this sequence could be interesting.

Still, there is another level to which things could be taken. Binet's formula states that if n is an integer, then

$$F_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right].$$

If we let

$$F_\theta = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^\theta - \left(\frac{1-\sqrt{5}}{2}\right)^\theta\right].$$

this expression defines a Fibonacci number for any *real* number θ. Extending a combinatorial of the Fibonacci numbers to real indices might allow many of the well-known identities to be generalized. One particular interesting case is the following. The Fibonacci identity

$$F_{n+1}F_{n-1} - F_n^2 = (-1)^n$$

is well-known. The proof of this identity using Binet's formula naturally extends to the following identity.

Theorem 3.8. *If* $\theta \in \mathbb{R}$, *then*

$$F_{\theta+1}F_{\theta-1} - F_\theta^2 = e^{i\pi\theta}.$$

A combinatorial proof of this result would be quite an achievement.

Bibliography

[1] Arthur T. Benjamin and Jennifer J. Quinn. Fibonacci and Lucas identities through colored tilings. *Util. Math.*, 56:137–142, 1999. This article contains a useful Fibonacci and Lucas number identity.

[2] Arthur T. Benjamin and Jennifer J. Quinn. The Fibonacci numbers–exposed more discretely. *Math. Mag.*, 76(3):182–192, 2003. This article provides combinatorial interpretations of Lucas sequences.

[3] Arthur T. Benjamin and Jeremy A. Rouse. When does F_m^L divide F_n, a combinatorial solution. *Fibonacci Quart.* This article has been accepted for publication. It contains a useful Lucas sequence identity.

[4] Arthur T. Benjmain and Jennifer J. Quinn. *Proofs that really count: The Art of Combinatorial Proof*. Mathematical Association of America, Washington, D.C., 2003. This book contains a host of interesting results proven combinatorially.

[5] David M. Bressoud and Doron Zeilberger. Bijecting Euler's partitions-recurrence. *Amer. Math. Monthly*, 92(1):54–55, 1985. This short article presents a very clear and straightforward bijective proof of Euler's partition recurrence.

[6] Paulo Ribenboim. *The little book of big primes*. Springer-Verlag, New York, 1991. This book contains extensive background on Lucas sequences and their applications in number theory.

[7] Dennis Stanton and Dennis White. *Constructive combinatorics*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1986. Ideas from this book,

particularly from chapter 4 and the discussion of Garcia and Milne's use of the involution principle, might be useful in proving partition congruences.

[8] Robert M. Young. *Excursions in calculus*, volume 13 of *The Dolciani Mathematical Expositions*. Mathematical Association of America, Washington, DC, 1992. This book provides a good background on the Fibonacci sequence and its interest to mathematicians.