2014 MSRI-UP
Research Reports

MSRI - UP

Preface

This publication contains the research reports written by the students who participated in the 2014 Mathematical Sciences Research Institute - Undergraduate Program (MSRI-UP) in Berkeley, CA. MSRI-UP is a six-week Research Experience for Undergraduates (REU) funded by National Science Foundation (grant No. DMS-1156499) and the National Security Agency (grant No. H-98230-13-1-0262).

The eighteen students who participated in the 2014 MSRI-UP came from universities in California, Illinois, Massachusetts, Georgia, Iowa, Louisiana, Maine, New Jersey, New York, and Rhode Island. They worked in teams of three on undergraduate research projects in *Arithmetic aspects of elementary functions* (a topic that intersects number theory and combinatorics) under the direction of Professor Victor H. Moll, Tulane University. Professor Moll and the students were supported by an academic staff consisting of Dr. Eric Rowland, Postdoctoral Fellow, University of Liège; Leyda Almodóvar, Graduate Student, University of Iowa; and Asia Wyatt, Graduate Student, University of Maryland, College Park.

The reports contained herein are the culmination of thousands of hours of work (no exaggeration!) by the 2014 MSRI-UP students and staff. We are confident that the interested reader will find the work done by these undergraduates mathematically rich, interesting and impressive.

We mention that Prof. Moll and the rest of the MSRI-UP staff did quite a bit of editing of these reports, but because the quantity of work produced by the students during the short six-week program is so great, and because of other time constraints, these reports should be characterized as "work still in progress." Indeed, it is our hope that some of these reports will receive further attention in the coming months and then submitted for journal publication.

MSRI-UP's primary goal is *to increase the number of graduate degrees in the mathematical sciences, especially doctorates, earned by U.S. citizens and permanent residents by cultivating heretofore untapped mathematical talent.* The summer research experience along with subsequent professional development opportunities and mentoring are designed to cultivate the mathematical talent of the MSRI-UP undergraduates.

Much support for the program was provided by many individuals at MSRI; in particular we thank David Eisenbud, Hélène Barcelo, Alissa Crans, Chris Marshall, Jacari Scott, Mark Howard and Alaina Moore. In addition, MSRI-UP co-directors Duane Cooper, Morehouse College; Ricardo Cortez, Tulane University; Ivelisse Rubio, University of Puerto Rico at Río Piedras; and Suzanne Weeks, Worcester Polytechnic Institute contributed significantly towards the organization and design of the program.

Best of luck to the 2014 MSRI-UP students!

Herbert A. Medina
Director, 2014 MSRI-UP
Berkeley, CA, August 2014

Table of Contents

Sequences of p-adic valuations of polynomials: an analysis of aperiodic and non p-regular behavior

Alyssa Byrnes **Isabelle Nogues** **Amber Yuan**

Tulane University Princeton University University of Chicago

August 2014

Abstract

In the field of number theory, the p-adic valuation is a useful device in studying the divisibility of an integer by powers of a given prime p. This paper centers on 2-adic valuations of quadratic polynomials in $\mathbb{Z}[x]$. In particular, the existence and properties of roots of such polynomials modulo 2^l, are determined and assessed. Polynomials of particular interest are those that yield non 2-regular sequences in $\mathbb{Q}_2$. Such sequences are represented in a novel infinite tree form, and patterns in such trees are analyzed to classify the sequences by their structure and non 2-regular properties. Such classification is further refined through an algebraic analysis of the polynomials at hand.

Contents

1 Introduction

The divisibility of integers by prime powers is a fundamental and long-studied topic in number theory. In this paper, the same study is applied to polynomials in $\mathbb{Z}[x]$. Specifically, the polynomials in question are of the form $f(n) = an^2 + c$. A few concepts central to the study are defined below.

1.1 $\mathbb{Q}_p$: The field of p-adic numbers

As this paper examines polynomials with roots existing in the field of 2-adic numbers, $\mathbb{Q}_2$, the following definitions serve to introduce key properties of $\mathbb{Q}_p$, which will support the later analysis.

Definition 1.1. For a given prime number p, the *p-adic valuation* of a non-zero integer x, $\nu_p(x)$, is the greatest integer $l \in \mathbb{N}$ such that $p^l \mid |x|$.

By convention, $\nu_p(0) = \infty$. The p-adic valuation can also be extended to the rational numbers by defining $\nu_p : \mathbb{Q} \to \mathbb{Z}$, $\nu_p\left(\frac{a}{b}\right) = \nu_p(a) - \nu_p(b)$.

Further properties of ν_p that are utilized in this paper are:

- $\nu_p(m \cdot n) = \nu_p(m) + \nu_p(n)$

- $\nu_p(m + n) \geq \inf \{\nu_p(m), \nu_p(n)\}$

for $m, n \in \mathbb{Z}^*$, i.e. the ring of non-negative integers.

The p-adic valuation can now be used to define the p-adic norm.

Definition 1.2. The *p-adic norm* of $x \in \mathbb{Q}$ is defined as $\|x\|_p = p^{-\nu_p(x)}$ with $\|0\|_p = 0$.

A few useful properties of the p-adic norm are the following:

- (**Non-negativity**) $\|a\|_p \geq 0$

- (**Sub-additivity**) $\|a + b\|_p \leq \|a\|_p + \|b\|_p$

- (**Symmetry**) $\|-a\|_p = \|a\|_p$

1.2 k-regular sequences

In past number theoretical research conducted by Bell [3], Allouche and Shallit [1], [2], sequences of the p-adic valuations of polynomials have been examined according to their recurrence and periodic properties. The present study instead focuses on sequences with unpredictable and non-regular patterns. In particular, polynomials whose p-adic valuations give rise to non k-regular sequences will be studied. The notion of k-regularity is given below.

Definition 1.3 (Allouche and Shallit [1], 1992)**.** Let $k \geq 2$ be an integer. An integer sequence $\{S(n)_{n\in\mathbb{N}}\}_{n\in\mathbb{N}}$ is said to be *k-regular* if the $\mathbb{Z}$-module generated by the set of subsequences $\{S(k^i n + j) | i, j \in \mathbb{N}, 0 \leq j \leq k^i - 1\}$ is finitely generated. In particular, every term $S(k^i n + j)$, and by extension every term $S(k^i(kn + j) + c)$, is a linear combination of the generators of the $\mathbb{Z}$-module.

For k-regular sequences, terms from the set of subsequences $\{S(k^i(kn + j) + c) | i, j \in \mathbb{N}, 0 \leq j \leq k^i - 1, c \in \mathbb{N}\}$ appear in a finite set of recurrences that define the terms of $\{S(n)\}$. More precisely, $\{S(n)\}$ is *p-regular* if it can be expressed as a linear combination of terms from the subsequence $\{S(p^i n + j)\}_{i,j\in\mathbb{N}}$. An example of a p-regular sequence is provided in Section 2.

1.3 p-adic analysis of integer polynomial sequences

The polynomials $f(n) \in \mathbb{Z}[x]$ relevant to the present study must generate non p-regular sequences $\{\nu_p(f(n))\}_{n\in\mathbb{N}}$. Before proceeding, it is necessary to state fundamental properties of polynomials $f(n)$ which yield p-regular sequences $\{\nu_p(f(n))\}_{n\in\mathbb{N}}$, so that such polynomials may be isolated from the study.

Lemma 1.1 (Bell [3], 2007)**.** *$\{\nu_p(f(n))\}_{n\in\mathbb{N}}$ is p-regular if and only if $f(x)$ factors into a product of polynomials, one of which has no roots in $\mathbb{Z}_p \subset \mathbb{Q}_p$ (i.e. the p-adic ring of integers), the other which factors into linear polynomials in $\mathbb{Q}[x]$.*

This implies that polynomials with no roots in $\mathbb{Q}_p$ give rise to non p-regular sequences $\{\nu_p(f(n))\}_{n\in\mathbb{N}}$. For this reason, the studied polynomials are chosen to be irreducible in $\mathbb{Z}[x]$, i.e. to have no roots in $\mathbb{Z}[x]$.

Lemma 1.2 (Bell [3], 2007)**.** *Let $h(x) \in \mathbb{Z}_p[x]$ be a polynomial with no roots in $\mathbb{Q}_p$ (i.e. no roots modulo p^l for some $l > 1$), then the following hold:*

- *The sequence $\{h(n)\}_{n\in\mathbb{N}}$ is periodic.*
- *There exists some $l \geq 2$ such that $|h(n)|_p > p^{-l}$ for all $n \in \mathbb{N}$.*

In light of the previous lemma, the polynomials $f(n)$ for the current study must yield aperiodic sequences $\{\nu_2(f(n))\}_{n\in\mathbb{N}}$. Furthermore, for all $n \in \mathbb{N}$, they must satisfy the property $|f(n)|_p \leq p^{-l} = C$, for all $l \geq 2$. In other words, $f(n)$ must have a finite size in $\mathbb{Q}_p$ for all $n \in \mathbb{N}$.

1.4 Behavior of $\{\nu_2(f(n))\}_{n\in\mathbb{N}}$ according to parity of a and c.

One must consider the different possible parities of the coefficients of $f(n) = an^2 + c$ when studying the corresponding 2-adic valuations of the polynomial. The congruences of $f(n)$ modulo 2 are summarized in the table below:

a	c	Number of Possible Roots	n mod 2
even	even	2	$0, 1$
odd	odd	1	1
even	odd	0	N/A
odd	even	1	0

To study polynomials $f(n)$ for which a and c are even, it suffices to factor $f(n) = an^2 + c$ as $f(n) = 2^i \cdot g(n)$, where $i \geq 1$ is the largest exponent such that 2^i divides a and c, and to study $\{\nu_2(g(n))\}_{n \in \mathbb{N}}$. This is because for $d = \gcd(a, c) \neq 1$, one may write $\nu_2(f(n))$ as $\nu_2(f(n)) = \nu_2(d) + \nu_2(g(n))$, and simply observe $\nu_2(g(n))$. Here, $g(n)$ corresponds to a polynomial for which at least one of a and c is odd.

When a is even and c is odd, $\nu_2(an^2 + c) = 0$. Hence, polynomials with such coefficients have no roots modulo 2^l, $l \geq 1$. This leaves two classes of polynomials $f(n) = an^2 + c$ to consider, $f(n)$ for which a and c are odd, and $f(n)$ for which a is odd and c is even.

This paper describes various methods for determining the existence and properties of 2-adic roots of $f(n) = an^2+c$. In Section 2, the behavior and patterns of $\{\nu_2(f(n))\}$ are represented pictorially in a 2-adic tree. The 2-adic tree will allow one to predict the existence of 2-adic roots for $f(n)$. Section 3 describes the 2-adic roots of $f(n)$ from a purely algebraic perspective. Hensel's Lemma for p-adic roots is used to derive a general formula for 2-adic roots of $f(n)$. In section 4, the roots of $f(n)$ are studied analytically based on of their power series' convergence properties in $\mathbb{Q}_2$. The analysis is first devoted to polynomials $f(n) = an^2 + c$ for which both a and c are odd and later extended to $f(n)$ such that a is odd and c is even.

The central result of this study lies in the following theorem:

Theorem 1.1. *Let $f(n) = an^2 + c$, such that $\gcd(a, c) = 1$. Write c as $c = 4^i \cdot b$ $(i \geq 0)$ where $4 \nmid b$. Then for all $l \in \mathbb{N}$, the roots $\alpha_i = \pm\sqrt{-c/a}$, $(i = 1, 2)$, of $f(n)$*

modulo 2^l *exist in* $\mathbb{Q}_2$.

In particular, the roots α_i *are finite in* $\mathbb{Q}_2$ *if and only if* $a + b \equiv 0 \bmod 8$.

2 Tree Representation of $\nu_p(f(n))_{n\in\mathbb{N}}$

The p-adic valuations of the polynomial $f(n)$ are represented in a *p-adic tree.* A p-adic tree consists of branches, which represent the argument of $f(n)$, and nodes, which indicate the value of $\nu_p(f(n))$ obtained from the value of the parent branch. The p-adic tree construction algorithm is briefly outlined below:

The tree begins with an initial node n. One must then draw p branches from node n, corresponding to the residues of n modulo p, namely $0, 1, \ldots, p-1$, respectively. If, for instance, $\nu_p(f(n))$ yields the same value $i \geq 0$ for all $n \equiv 0 \bmod p$, the branch must be terminated by a node i. No further branches are to be drawn from node i. In the case where $\nu_p(f(n))$ yields non-identical values for $n \equiv 0 \bmod p$, the given branch is terminated by a node labelled with an asterisk. The same reasoning applies for $n \equiv 1 \bmod p, \ldots, n \equiv (p-1) \bmod p$. Then p new branches are drawn from node *, each corresponding as previously to input values congruent to $0, 1, \ldots,$ or $p-1$ modulo p for the subsequence $\nu_p(f(p \cdot n))$, $(\nu_p(f(p \cdot n + 1)), \ldots, \nu_p(f(p \cdot n + p - 1)))$. The tree is now at level $l = 1$. The same criterion as previously is used to evaluate each branch, and the process continues until all nodes in the tree terminate. If the nodes never terminate, the result is an infinite tree.

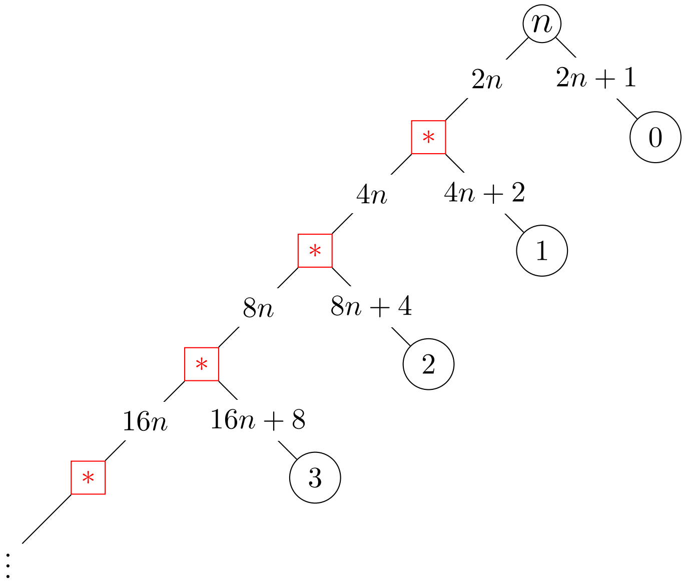
More generally, a branch at level l of the tree will continue to level $l+1$ if $\nu_p(f(p^l \cdot n + j_{l-1} \cdot p^{l-1} + \cdots + j_0 \cdot p^0))$, where $j_0, \ldots, j_{l-1}$ may take on integer values between 0 and $p-1$ and does not yield identical values for all n congruent to $0, 1, \ldots, p-1$ modulo p. Otherwise, the branch will terminate at level l.

Example 2.1 (**p-adic tree of $f(n) = n^2$, $p = 2$**)**.** In the tree representation of $\nu_2(n^2)$ (see diagram here below), the leftmost branch, corresponding to values of the form $2^{l-1} \cdot (2n)$, $l \geq 1$, continues at each level l, and thus is infinite, as $f(2^{l-1} \cdot (2n)) = [2^{l-1} \cdot (2n)]^2 \equiv 0 \bmod 2^l$, for all $l \geq 1$. Meanwhile, the rightmost branch, corresponding to values of the form $2^{l-1} \cdot (2n+1)$ at each level l terminates. Indeed, $f(2^{l-1} \cdot (2n+1)) = 2^{l-1} \cdot (2n+1) \not\equiv 0 \bmod 2^l$, for all $l \geq 1$.

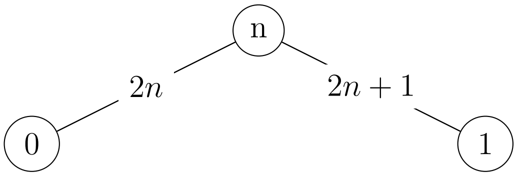
The tree patterns of $\nu_2(n^2)$ are directly dependent on the input n to the sequence term $\nu_2(n^2)$ at level l. The following recurrence relation ensues:

$$\begin{aligned} \nu_2((2n+1)^2) &= 0 \\ \nu_2((2n)^2) &= \nu_2(n^2) + 2. \end{aligned}$$

For this reason, $\nu_2(n)$ is deemed a 2-*regular* sequence.

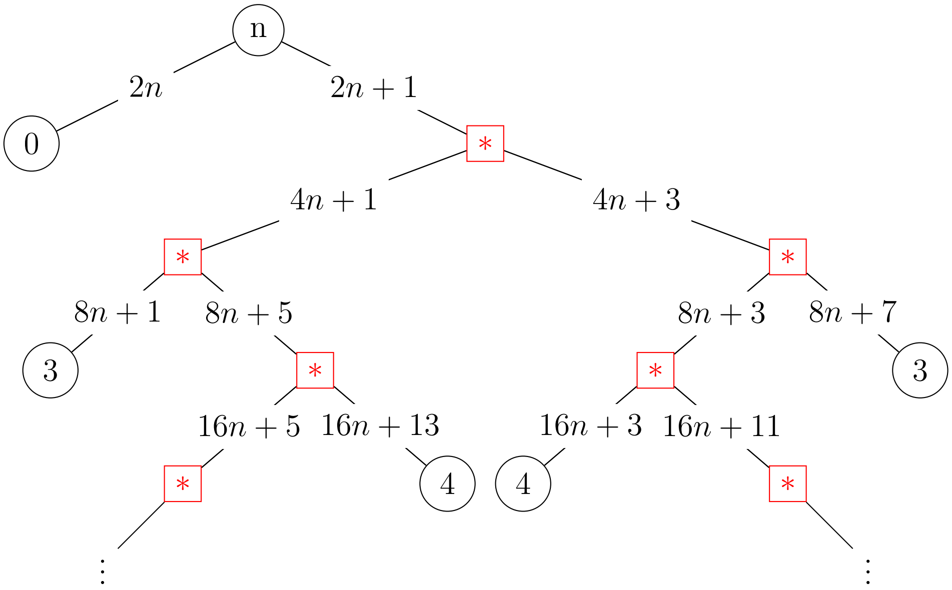


Example 2.2 (**p-adic tree of $f(n) = n^2 + 1$, $p = 2$**)**.** For even n, $f(n)$ is odd. Therefore, $\nu_2(f(n)) = 0$ for all n even, and thus the corresponding branch terminates with a node of value 0. For odd n, $f(n)$ is divisible by 2, but not by 4. Consequently, $\nu_2(f(n)) = 1$ for all odd n, and the right branch terminates with value 1.



Example 2.3 (**p-adic tree of $f(n) = n^2 + 7$, $p = 2$**)**.** For even n, $f(n)$ is odd. Therefore, $f(n) \not\equiv 0 \bmod 2^l$ for even n. Consequently, the leftmost branch, which

corresponds to even values of n, terminates at level $l = 1$. However, for odd n, the behavior of $\{\nu_2(n^2+7)\}_{n\in\mathbb{N}}$ cannot be immediately predicted. At a given level l, one cannot ensure whether the nature of the new input value n to $f(2^l \cdot n + 1)$ will induce its associated branch to terminate at level l or to proceed to the next level. This erratic behavior, observed in the following tree, is indicative of the non 2-regular behavior of $\{\nu_2(n^2+7)\}_{n\in\mathbb{N}}$.



Instead of examining sequences $\{\nu_2(f(n))\}_{n\in\mathbb{N}}$ via this algorithmic, pictorial method, one may analyze the sequences through a purely algebraic approach. The next section describes this method.

3 Algebraic Analysis of $\nu_2(f(n))$

By using Hensel's lemma for roots of polynomials in $\mathbb{Z}_p$, it is possible to determine which solutions to $f(n) \equiv 0 \bmod p^l$, $l \geq 1$, also give rise to solutions to $f(n) \equiv 0 \bmod p^{l+h}$, $1 \leq h \leq l$. Furthermore, a general formula can be derived for such solutions. Birjamer, Gil, and Weiner [2] give a formula for roots of a polynomial of degree m, stated in the following lemma:

Lemma 3.1. *Let $p > 0$ be a prime and let $f(x) = a_0 + a_1 x + \cdots + a_m x^m$ be a polynomial in $\mathbb{Z}_p[x]$. Let $\mu, \kappa \in \mathbb{Z}$ be such that $0 \leq 2\kappa < \mu$. If $r_0 \in \mathbb{Z}$ is such that*

$$f(r_0) \equiv 0 \bmod p^{\mu} \text{ and } \nu_p(f'(r_0)) = \kappa,$$

then r_0 lifts to a p-adic root r of f given by

$$r = r_0 + p^{\kappa} \sum_{n=0}^{\infty} \sum_{k=0}^{n} \frac{(1)^{nk+1}}{c_1^k (n+1)}! \binom{2n+1}{nk} B_{n+k,k}(1!c_1, 2!c_2, \ldots) \left(\frac{c_0}{c_1}\right)^{n+1}.$$

The coefficients $c_j = p^{(j2)\kappa} \cdot \frac{f^{(j)}(r0)}{j!}$ for $j = 0, 1, \ldots, m$. The Bell polynomial $B_{n+k,k}$ is of the following form:

$$B_{n+k,k}(x_1, x_2, \cdots) = \sum \frac{(n+k)!}{j_1! j_2! \ldots j_{n+1}!} \left(\frac{x_1}{1!}\right)^{j_1} \left(\frac{x_2}{2!}\right)^{j_2} \cdots \left(\frac{x_{n+1}}{(n+1)!}\right)^{j_{n+1}},$$

where the sum is taken over all sequences $j_1, j_2, \ldots, j_{n+1}$ of non-negative integers satisfying
$j_1 + j_2 + \cdots + j_{n+1} = k$ and $j_1 + 2j_2 + \cdots + (n+1)j_{n+1} = n + k$.

Remark 1. The power series which appear in the expression of r are not to be interpreted in $\mathbb{R}$, but in $\mathbb{Z}_p$, as r is a p-adic root of $f(x)$.

The general formula for the root r of any quadratic polynomial in $\mathbb{Z}[x]$ satisfying the conditions stated in Lemma 3.1, deriving from a root r_0 of the given polynomial modulo $p > 0$, can therefore be reduced to the following expression:

$$r = r_0 - 2^{\kappa} \sum_{n=0}^{\infty} C(n) \left(\frac{c_0}{c_1}\right)^{n+1} \frac{1}{c_1^n},$$

where $C(n)$ is the n^{th} Catalan number, $C(n) = \frac{1}{n+1}\binom{2n}{n}$.

Example 3.1. The root $r_0 = 1$ of $f(n) = n^2 + 7$ modulo 2 gives rise to the root

$$r = 1 - 2 \sum_{n=0}^{\infty} \frac{(2n)! 2^{n+1}}{(n+1)! n!}.$$

4 Power series interpretation in $\mathbb{Q}_2$

The remainder of the paper is devoted to the proof of Theorem 1.1, restated below:

Let $f(n) = an^2 + c$, such that $c = 4^i \cdot b$ $(i \geq 0)$, $4 \mid b$, and $\gcd(a, c) = 1$. Then for all $l \in \mathbb{N}$, the roots $\alpha_i = \pm\sqrt{-c/a}$, $(i = 1, 2)$, of $f(n)$ modulo 2^l exist in $\mathbb{Q}_2$.
In particular, the roots α_i are finite in $\mathbb{Q}_2$ if and only if $a + b \equiv 0 \bmod 8$.

Theorem 1.1 specifies the conditions that the coefficients a and c in $f(n) = an^2 + c$ must satisfy in order for $f(n)$ to have a solution modulo 2^l, for all $l \in \mathbb{N}$.

The forward direction is proven in this section via analysis of the power series expansion of $\sqrt{\frac{-c}{a}}$. The backward direction, reserved for the following section of the paper, involves a modular arithmetic argument.

Remark 2. Though both directions can be proven through the power series method alone, the arithmetic approach is included for variety purposes.

The statement of Theorem 1.1 is equivalent to the claim that $f(n)$ has a root modulo 2^l for all $l \in \mathbb{N}$. Indeed, the congruence equation $f(n) \equiv 0 \bmod 2^l$ has a solution for all $l \in \mathbb{N}$ if and only if $\sqrt{\frac{-c}{a}} \in \mathbb{Q}_2$. In turn, $\sqrt{\frac{-c}{a}} \in \mathbb{Q}_2$ if and only if $\left\|\sqrt{\frac{-c}{a}}\right\|_2$ is finite.

The 2-adic norm of $\sqrt{\frac{-c}{a}}$ is

$$\left\|\sqrt{\frac{-c}{a}}\right\|_2 = 2^{-\nu_2\left(\sqrt{-c/a}\right)}.$$

Yet

$$\begin{aligned}\nu_2\left(\sqrt{\frac{-c}{a}}\right) &= \nu_2(\sqrt{-4^i \cdot b/a}) \\ &= \nu_2\left(2^i\sqrt{\frac{-b}{a}}\right) \\ &= i + \nu_2\left(\sqrt{\frac{-b}{a}}\right).\end{aligned}$$

Hence,

$$\left\|\sqrt{\frac{-c}{a}}\right\|_2 = 2^{-i}\cdot 2^{-\nu_2\left(\sqrt{\frac{-b}{a}}\right)}.$$

Therefore, to prove that $\left\|\sqrt{\frac{-c}{a}}\right\|_2$ is finite, one must show that $\nu_2\left(\sqrt{\frac{-b}{a}}\right)$ is large, and thus that the power series expansion of $\sqrt{\frac{-b}{a}}$ converges in $\mathbb{Q}_2$.

Remark 3. When c is odd, $i = 0$ and b is odd. When c is even, one of the following cases applies: either $i \geq 1$ and b may be even or odd, or $i = 0$ and b is divisible by at most 2. (If b were divisible by a greater power of 2, it would be possible to factor 4 from b, thus increasing the exponent i). However, i does not come into consideration for the power series method, which solely depends on b.

Proof. The power series expression of $\sqrt{\dfrac{-b}{a}}$ is written as follows:

$$\sqrt{\frac{-b}{a}} = \sum_{k=0}^{\infty} \frac{\left(\frac{1}{2}\right)_k \cdot (\frac{b}{a}+1)^k}{k!} = \sum_{k=0}^{\infty} \frac{(-1)^k(1)(3)\dots(2k-1)(\frac{a+b}{a})^k}{2^k k!}.$$

By sub-additivity of the 2-adic norm,

$$\begin{aligned}\left\|\sum_{k=0}^{\infty}\frac{(-1)^k(1)(3)\dots(2k-1)(a+b)^k}{2^k a^k k!}\right\|_2 &\leq \left\|\sum_{k=0}^{k_0-1}\frac{(-1)^k(1)(3)\dots(2k-1)(a+b)^k}{2^k a^k k!}\right\|_2 \\ &+ \left\|\sum_{k=k_0}^{\infty}\frac{(-1)^k(1)(3)\dots(2k-1)(a+b)^k}{2^k a^k k!}\right\|_2\end{aligned}$$

for any $k_0 \in \mathbb{N}$. Therefore, to prove convergence of the series in $\mathbb{Q}_2$, it is enough to show that the right-hand side of the inequality is bounded above by a constant. Indeed, terms with a finite 2-adic norm converge in $\mathbb{Q}_2$.

For $k = 0$, the summand is odd. For all $k \geq 1$, the summand is even, due to the factor $\frac{(a+b)}{2}$ which is even for all such terms. Indeed, $\nu_2(a+b) \geq 3$, from the theorem statement. Hence, the finite sum

$$\sum_{k=0}^{k_0-1} \frac{2^{4k}}{(2k)!}\cdot\left(\frac{-4\cdot(k\cdot 2^{m+1}+1)+(2k+1)}{2k+1}\right)(1)(1+2^m)\dots((2k-1)\cdot 2^m+1)$$

is odd, and thus

$$\nu_2\left(\sum_{k=0}^{k_0-1}\frac{(-1)^k(1)(3)\dots(2k-1)(a+b)^k}{2^k a^k k!})\right)=0,$$

which implies that

$$\left\|\sum_{k=0}^{\infty}\frac{(-1)^k(1)(3)\dots(2k-1)(a+b)^k}{2^k a^k k!}\right\|_2=\frac{1}{2^0}=1.$$

It remains to show that

$$\left\|\sum_{k=k_0}^{\infty}\frac{(-1)^k(1)(3)\dots(2k-1)(a+b)^k}{2^k a^k k!}\right\|_2$$

is bounded, which is equivalent to proving that

$$\nu_2\left(\sum_{k=k_0}^{\infty}\frac{(-1)^k(1)(3)\dots(2k-1)(a+b)^k}{2^k a^k k!}\right)\geq N$$

for all $N\in\mathbb{N}$.

Note that

$$\nu_2\left(\sum_{k=k_0}^{\infty}\frac{(-1)^k(1)(3)\dots(2k-1)(a+b)^k}{2^k a^k k!}\right)\geq\inf\left\{\nu_2\left(\frac{(-1)^k(1)(3)\dots(2k-1)(a+b)^k}{2^k a^k k!}\right)\right\}_{k\geq k_0}.$$

The expression $\nu_2\left(\frac{(-1)^k(1)(3)\dots(2k-1)(a+b)^k}{2^k a^k k!}\right)$ can be reduced to

$k\nu_2(a+b)+s_2(k)-2k$, where $s_2(k)$ is the sum of the binary coefficients of k. This new expression follows from the properties $\nu_2(h!)=h-s_2(h)$ $(h\in\mathbb{N})$ and $s_2(2^l\cdot k)=s_2(k)$, for all $l\in\mathbb{N}$.

Thus, for all $k\in\mathbb{N}, s_2(k)\geq 0$,

$$\inf\{k\nu_2(a+b)+s_2(k)-2k\}_{k\geq k_0}\geq\inf\{k\nu_2(a+b)-2k\}_{k\geq k_0}=k_0\cdot\nu_2(a+b)-2k_0.$$

Since $a+b\equiv 0 \bmod 8$, $\nu_2(a+b)\geq 3$. Hence, $k_0\nu_2(a+b)-2k_0\geq 3k_0-2k_0=k_0$.

For every $N\in\mathbb{N}$, there exists $k_0\in\mathbb{N}$ such that $0\leq N\leq k_0$. Hence, for every $N\in\mathbb{N}$, there exists k_0 such that $\nu_2\left(\frac{(-1)^k(1)(3)\dots(2k-1)(a+b)^k}{2^k a^k k!}\right)\geq N$.

Therefore, for every such pair $\{k_0, N\}$,

$$\left\| \sum_{k=k_0}^{\infty} \frac{(-1)^k (1)(3)\dots(2k-1)(a+b)^k}{2^k a^k k!} \right\|_2 = \frac{1}{2^m} \leq \frac{1}{2^N}$$

where $m = \nu_2 \left(\sum_{k=k_0}^{\infty} \frac{(-1)^k (1)(3)\dots(2k-1)(a+b)^k}{2^k a^k k!} \right)$.

This yields the global inequality

$$\left\| \sum_{k=0}^{\infty} \frac{(-1)^k (1)(3)\dots(2k-1)(a+b)^k}{2^k a^k k!} \right\|_2 \leq 1 + \frac{1}{2^N}.$$

Furthermore,

$$\left\| \sum_{k=0}^{\infty} \frac{(-1)^k (1)(3)\dots(2k-1)(a+b)^k}{2^k a^k k!} \right\|_2 \geq 0.$$

Then, as $N \to \infty$,

$$0 \leq \left\| \sum_{k=0}^{\infty} \frac{(-1)^k (1)(3)\dots(2k-1)(a+b)^k}{2^k a^k k!} \right\|_2 \leq 1. \qquad \square$$

Remark 4. This proof for the "if" direction holds the same for the roots of any polynomial $f(n) = an^r + c$ modulo $2^l, l \geq 1$, where $a = 1$, $r = 2^m, m \geq 1$, and $c \equiv -1 \bmod 2^{m+2}$. However, analysis of polynomials of higher degree is beyond the scope of this paper.

The following section proves the reverse direction.

5 Arithmetic analysis of $\nu_2(f(n))$

The argument is first applied to polynomials $f(n) = an^2 + c$ for which a and c are odd, and is later extended to polynomials for which a is odd and c is even.

5.1 2-adic valuation of $f(n) = an^2 + c$, a odd, c odd

When c is odd, c is of the form $c = 4^0 \cdot b = 1 \cdot b$, where b is an odd integer. Therefore, the congruence $a + c \equiv 0 \bmod 8$, which appears in the proof, is equivalent to the congruence $a + b \equiv 0 \bmod 8$ in the statement of Theorem 1.1. Here begins the proof of Theorem 1.1 for the second direction of the statement.

Proof. Consider the 2-adic expansion of a solution n for $an^2 + c \equiv 0 \bmod 2^l$, $n = x_0 2^0 + x_1 2^1 + \cdots + x_{l-1} 2^{l-1}, x_j \in \{0, 1\}$. As n cannot be even (cf. section 1.4), $x_0 = 1$.

To find x_1, solve the congruence $a(x_0 + 2x_1)^2 + c \equiv 0 \bmod 2^l$ at $l = 2$. Since $x_0 = 1$, this yields

$$\begin{aligned} a(1 + 2x_1)^2 + c &\equiv 0 \bmod 2^2 \\ a + c &\equiv 0 \bmod 2^2. \end{aligned}$$

Note that when simplifying the term $(1+2x_1)^2$, the factors $4x_1$ and $4x_1^2$ vanish modulo 2^2.

This results in the following conditions on a and c and the possible values for x_1.

a mod 4	c mod 4	Number of Solutions	x_1
1	1	0	none
3	1	2	$0, 1$
1	3	2	$0, 1$
3	3	0	none

The subsequent step consists in studying the congruence equation for $l = 3$: $a(x_0 + 2x_1 + 4x_2)^2 + c \equiv 0 \bmod 2^3$. For this, it is necessary to consider the cases $x_1 = 0$ and $x_1 = 1$ separately. Setting $x_1 = 0$ yields following congruence equation:

$$\begin{aligned} a(1 + 2(0) + 4x_2)^2 + c &\equiv 0 \bmod 2^3 \\ a + c &\equiv 0 \bmod 2^3. \end{aligned}$$

The terms $8x_2$ and $16x_2^2$ obtained from the simplification of $(1 + 4x_2)^2$ are divisible by 8, and thus vanish modulo 2^3.

Setting $x_1 = 1$ yields the following congruence equation:

$$\begin{aligned} a(1 + 2(1) + 4x_2)^2 + c &\equiv 0 \bmod 2^3 \\ a + c &\equiv 0 \bmod 2^3. \end{aligned}$$

Once again, the terms $24x_2$ and $16x_2^2$ obtained from the simplification of $(3 + 4x_2)^2$ are divisible by 8, and thus vanish modulo 2^3.

Therefore, for $f(n) = an^2 + c$, where a and c are odd, $\nu_2(f(n)) \geq 3$ only holds if $a + c \equiv 0 \bmod 8$. □

This concludes the proof for $f(n)$ where a and c are odd. A similar proof is used for $f(n) = an^2 + c$ where a is odd and c is even.

5.2 2-adic valuation of $f(n) = an^2 + c$, a odd, c even

For even c, the factor b in the expression $c = 4^i \cdot b$, $i \geq 0$, may be either even or odd. When b is odd, $c \equiv 0 \bmod 8$ for $i \geq 2$ and $c \equiv 4 \bmod 8$ for $i < 2$. When b is even, b must be divisible by at most 2 (otherwise, it is possible to factor additional powers of 4 from b). In this case, $c \equiv 0 \bmod 8$ for $i \geq 1$ and $c \equiv 4 \bmod 8$ for $i = 0$. Therefore, when c is even, it must satisfy the congruences $c \equiv 0 \bmod 8$ or $c \equiv 4 \bmod 8$. This property is consistent with the restrictions posed on c in the proof below.

Proof. Starting at $l = 2$, one would like to find x_1 such that $a(x_0 + 2x_1)^2 + c \equiv 0 \bmod 2^2$. From section 1.4, $x_0 = 0$, which yields the congruence equation:

$$\begin{aligned} a(2x_1)^2 + c &\equiv 0 \bmod 2^2 \\ c &\equiv 0 \bmod 2^2. \end{aligned}$$

The conditions on a and c can be refined as follows.

a mod 4	c mod 4	Number of Solutions	x_1
1	0	2	$0, 1$
3	0	2	$0, 1$
1	2	0	none
3	2	0	none

The next step, where $l = 3$, is finding x_2 such that the congruence $a(x_0 + 2x_1)^2 + c \equiv 0 \bmod 2^2$ holds. For this, it is necessary to consider the cases $x_1 = 0$ and $x_1 = 1$ separately. Setting $x_1 = 0$ yields the following congruence:

$$\begin{aligned} a(4x_2)^2 + c &\equiv 0 \bmod 2^3 \\ c &\equiv 0 \bmod 2^3. \end{aligned}$$

Now, setting $x_1 = 1$ yields

$$\begin{aligned} a(2 + 4x_2)^2 + c &\equiv 0 \bmod 2^3 \\ 4a + c &\equiv 0 \bmod 2^3. \end{aligned}$$

Yet, from the analysis for $l = 2$, $a \equiv 1 \bmod 2$ and $c \equiv 0 \bmod 4$. The resulting cases $c \equiv 0 \bmod 8$ and $c \equiv 4 \bmod 8$ are considered seperately.

Case 1: $c \equiv 0 \bmod 8$
The congruence $4a + c \equiv 0 \bmod 2^3$ becomes $4a \equiv 0 \bmod 2^3$, which implies that $a \equiv 0 \bmod 2$. Yet, from the initial statement, $a \equiv 1 \bmod 2$, so this is a contradiction.

Case 2: $c \equiv 4 \bmod 8$
The congruence $4a + c \equiv 0 \bmod 2^3$ becomes $4a + 4 \equiv 0 \bmod 2^3$, which implies that $a \equiv 1 \bmod 2$. This is consistent with the initial statement, hence the condition $c \equiv 4 \bmod 8$ is valid.

This yields two classes of polynomials $f(n) = an^2 + c$ which have roots in $\mathbb{Q}_2$:

- $\{f(n) \mid c \equiv 0 \bmod 8, a \equiv 1 \bmod 2\}$
- $\{f(n) \mid 4a + c \equiv 0 \bmod 8, a \equiv 1 \bmod 2, c \equiv 4 \bmod 8\}$

□

A few applications of the theorem are provided below.

Example 5.1. Let $f(n) = n^2 + 7$. In this case, $c = 7$ can be written as $c = 4^0 \cdot 7$. 1 and 7 satisfy $1 + 7 \equiv 0 \bmod 8$, and $\gcd(1, 7) = 1$ Therefore, $n = \pm\sqrt{-7/1} = \pm\sqrt{-7}$ exist in $\mathbb{Q}_2$.

Example 5.2. Let $f(n) = 3n^2 + 40$. The coefficient $c = 40$ can be expressed as $c = 4^1 \cdot 10$. Since $3 + 10 = 13 \not\equiv 0 \bmod 8$, $f(n)$ has no roots in $\mathbb{Q}_2$.

A few noteworthy results regarding the coefficients a and c arose during the study, and have been verified for approximately fifty examples. These results derived from the main theorem for this study, and are summarized in the following corollary:

Corollary 5.1. *Let $f(n) = an^2 + c$, where $c = m^2$, $m \in \mathbb{Z}$. Then $f(n)$ has a root in $\mathbb{Q}_2$ if $a \equiv -1 \bmod 8$ and $c \equiv 0, 1, 4 \bmod 8$.*

6 Additional Results and Future Goals

A few additional results were discovered alongside the central research, and are stated below. New possible

6.1 Analysis of $\{\nu_2(f(n))\}$, $f(n) = an^2 + c$, for $c = m^2$, $m \in \mathbb{Z}$

As an alternative method for determining which polynomials $f(n) = an^2 + c$ have 2-adic roots, one may seek to recover coefficients a and c which satisfy the equality $n = \sqrt{\frac{2^l k_l - c}{a}}$. This method is elaborated further in the proposition and proof below.

Proposition 6.1. *Let $l \in \mathbb{N}$. If there exists an $n \in \mathbb{N}$ such that $f(n) = an^2 + c \equiv 0 \bmod 2^l$, then there exists a $k_l \in \mathbb{N}$ such that $\sqrt{\frac{2^l k_l - c}{a}} \in \mathbb{N}$, or equivalently $\frac{2^l k_l - c}{a} = m^2, m \in \mathbb{Z}$.*

Proof. Suppose $f(n) = an^2 + c$ has a root in $\mathbb{Q}_2$. Then the congruence $an^2 + c \equiv 0 \bmod 2^l$ must hold for all l. Equivalently, $an^2 + c = 2^l k_l, k_l \in \mathbb{N}$. Rearranging this identity yields the following:

$$\begin{aligned} an^2 + c &= 2^l k_l \\ n &= \sqrt{\frac{2^l k_l - c}{a}}. \end{aligned}$$

Since $n \in \mathbb{N}$, it follows that $\sqrt{\frac{2^l k_l - c}{a}}$ must be in $\mathbb{N}$. □

6.1.1 Modular properties of perfect squares

Determining a and c which satisfy $n = \sqrt{\frac{2^l k_l - c}{a}}$ such that $n \in \mathbb{N}$, is equivalent to determining a and c which satisfy $n^2 = \frac{2^l k_l - c}{a}$ such that $n^2 \in \mathbb{N}$. In other words, it is equivalent to determining a and c for which $\frac{2^l k_l - c}{a}$ is a perfect square. Therefore, it is useful to consider congruence properties of perfect squares, which may then be applied to $\frac{2^l k_l - c}{a}$. An essential congruence property of perfect squares is cited in the following proposition:

Proposition 6.2. *Let $n = m^2$ be a perfect square. For n even, $n \equiv 0 \bmod 4$. For n odd, $n \equiv 1 \bmod 4$.*

As $f(n)$ is studied modulo 2^l, for l arbitrarily large, one may extend the congruences of perfect squares to higher moduli, namely to 2^l such that $l > 2$.

For instance, $n = m^2$ satisfies the congruences $n \equiv 0 \bmod 8$ or $n \equiv 4 \bmod 8$ when n is even. When n is odd, $n \equiv 1 \bmod 8$.

6.1.2 2-adic tree analysis for $f(n) = an^2 + c$, revisited

The existence of a 2-adic root of $f(n) = an^2 + c$ may be visited by studying both the identity $an^2 + c = 2^l k_l$, $l \geq 1$ and $k_l \in \mathbb{N}$, and the 2-adic tree of $f(n)$. In order for the tree of $an^2 + c$ to continue beyond l, there must exist a $k_l \in \mathbb{N}$ such that $an^2 + c = 2^l k_l$.

Example 6.1. **(2-adic tree of $f(n) = n^2 + 1$)**
In this case, $a = c = 1$. At level $l = 1$ of the 2-adic tree of $n^2 + 1$, $\nu_2(n_1^2 + 1) \geq 1$ where the continuing branch is denoted by $n_1 \equiv 1 \bmod 2$. To analyze the tree at level $l = 2$, one may attempt to recover n_2 such that $n_2^2 = \frac{2^l k_l - c}{a}$ as follows:

$$\begin{aligned} n_2^2 &= \frac{2^l k_l - c}{a} \\ &= 2^2 k_2 - 1 \\ &\equiv -1 \bmod 4 \\ &\equiv 3 \bmod 4. \end{aligned}$$

Since no perfect square has a residue of 3 modulo 4, $f(n)$ yields no roots modulo 2^l for $l > 1$. Consequently, the branch of the tree terminates at level $l = 1$, which indicates that $\nu_2(n_1^2 + 1) = 1, n_1 \equiv 1 \bmod 2$.

Example 6.2. 2-adic tree of $f(n) = n^2 + 7$
In this case, $a = 1$ and $c = 7$. At level $l = 1$ of the tree, $\nu_2(n_1^2 + 1) \geq 1$, where the continuing branch is denoted by $n_1 \equiv 1 \bmod 2$. To analyze the tree at level $l = 2$, one may attempt to recover n_2 such that $n_2^2 = \frac{2^l k_l - c}{a}$ as follows,

$$\begin{aligned} n_2^2 &= \frac{2^l k_l - c}{a} \\ &= 2^2 x - 7 \\ &\equiv -7 \bmod 4 \\ &\equiv 1 \bmod 4. \end{aligned}$$

Since a perfect square $n = m^2$ may satisfy the congruence $n \equiv 1 \bmod 4$, there exists a root for $n_2^2 \equiv 1 \bmod 4$.

From Proposition 6.2, it is possible to determine which polynomials $f(n) = an^2 + c$ yield finite 2-adic trees. It is also possible to determine which polynomials of this type yield infinite 2-adic trees which exhibit aperiodic and irregular branching patterns. Corollaries 6.1 and 6.2 summarize these results.

Corollary 6.1. *A tree will be finite and of height r if there exists an $r \in \mathbb{N}$ such that for $l > r$, no solutions exist for $n_l^2 = \frac{2^l k_l - c}{a}$. In other words, for $l > r$, $\sqrt{\frac{2^l k_l - c}{a}} \notin \mathbb{N}$.*

Corollary 6.2. *Assume there exists $n_l \in \mathbb{Z}$, such that $an_l^2 + c \equiv 0 \bmod 2^l$. If the next level of the tree continues, there exists at least one solution $n_{l+1} \equiv n_l + d(2^l) \bmod 2^{l+1}, d \in \{0, 1\}$ such that $n_{l+1}^2 = \frac{2^{l+1} k_{l+1} - c}{a}$ for some $k_{l+1} \in \mathbb{N}$. Furthermore, if the tree continues infinitely, k_{l+1} is even for all $l \in \mathbb{N}$.*

6.2 2-adic roots of general quadratic polynomials $f(n) = an^2 + bn + c$

A future topic of interest which derives from the current study is the behavior of quadratic polynomials in $\mathbb{Z}[x]$, $f(n) = an^2 + bn + c$ where $a, b, c \in \mathbb{Z}$, such that $f(n) \equiv 0 \bmod 2^l$ has solutions for all $l \in \mathbb{N}$. To explore this question, one may characterize and classify the coefficients a, b, c of $f(n)$. The coefficients a, b, and c are to be chosen such that the general roots of $f(n)$, $\frac{-b \pm \sqrt{b^2-4ac}}{2a}$, are in $\mathbb{Q}_2$. In other words, a, b, and c are chosen such that the corresponding series expansion $\displaystyle\sum_{k=0}^{\infty} \frac{(\frac{1}{2})_k \times (\alpha^2+1)^k}{k!}$, where $\alpha = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$ the standard quadratic polynomial root, converges in $\mathbb{Q}_2$.

Remark 5. The power series expansion of the general root can be rewritten as

$$\sum_{k=0}^{\infty} \left[\frac{(-1)^k (2k)!}{(k!)^2 2^{4k} a^{3k}} \times ((-b \pm \sqrt{b^2-4ac})^2 + 4a^2)^k \right].$$

One cannot easily determine which values of a, b, and c cause the series to converge in $\mathbb{Q}_2$. For instance, when considering values of $a \in 2\mathbb{Z}+1$ and arbitary values of b and c, each term of the summand yields a 2-adic valuation $\geq S_2(k) - 3k$, but further restricting b and c may yield a convergent series.

7 Acknowledgments

This work was carried out during the 2014 Mathematical Sciences Research Institute Undergraduate Program (MSRI-UP) which is funded by the National Science Foundation (grant No. DMS-1156499) and the National Security Agency (grant No. H-98230-13-1-0262). We would like to thank Dr. Victor Moll, Dr. Herbert Medina, Dr. Eric Rowland as well as Leyda Almodóvar and our fellow MSRI-UP colleagues. The first author wishes to thank Dr. Carola Wenk for helping her to attend MSRI-UP and Dr. Christophe Vignat for introducing her to the world of undergraduate mathematics. The second author would like to extend her gratitude to Dr. Christine Taylor and Dr. Tasho Kaletha, who have made her participation in the MSRI-UP possible. The third author would like to thank Dr. Alden Walker and Jahan Claes for their encouragement and mathematical guidance.

References

[1] J.-P. Allouche, J. Shallit. *Automatic sequences. Theory, applications, generalizations.* Cambridge University Press, Cambridge, 2003. 438–441.

[2] J. P. Allouche and J. Shallit. *The ring of k-regular sequences. Theoret. Comput. Sci*, 98:193-197, 1992.

[3] J. Bell. *p-adic valuations and k-regular sequences. Discrete Math.*, 307:3070-3075, 2007.

[4] D. Birmajer, J. B. Gil, and M. D. Weiner. *On Hensel's roots and a factorization formula in $\mathbb{Z}[[x]]$.* arXiv:1308.2987,2013.

Catalan numbers modulo 2^α

David Cervantes Nava
SUNY Potsdam

Erica Musgrave
Saint Mary's College of California

Gianluca Pane
Brown University

August 2014

Abstract

Catalan numbers, defined by the explicit formula $C(n) = \frac{1}{1+n}\binom{2n}{n}$, have been studied since the eighteenth century due to their frequent appearance in various fields from set theory to combinatorics. For example, $C(n)$ counts the number of permutations of $\{1, 2, \ldots, n\}$ that avoid an three-term increasing subsequence. However, there are few results about the properties of Catalan numbers modulo prime powers. In particular, we examine the number of residues obtained by viewing Catalan numbers modulo powers of 2.

Introduction

We begin with an example. Modulo 4, the following residues are produced: $C(0) = 1 \equiv 1 \bmod 4$, $C(2) = 2 \equiv 2 \bmod 4$, and $C(6) = 132 \equiv 0 \bmod 4$. One may continue to compute such values, but it seems that no amount of computation will find an n such that $C(n) \equiv 3 \bmod 4$. We use the following definitions to distinguish such residues.

Definition 0.1. A residue $b \bmod 2^\alpha$ is *present* if there exists an n such that $C(n) \equiv b \bmod 2^\alpha$. A residue that is not present is called *absent*.

That 3 mod 4 is absent will be proven in Section 1 in addition to other results of a slightly different kind, for example,

$$C(n) \not\equiv 1 \bmod 8 \text{ for } n \geq 1.$$

Definition 0.2. An *eventually absent residue* is a residue $b \bmod 2^\alpha$ for which there exist only finitely many n such that $C(n) \equiv b \bmod 2^\alpha$.

Note that a residue can be both present and eventually absent.

Section 1 contains a number of results for small powers of 2. Section 2 uses these results to exhibit an upper bound on the limit

$$\lim_{\alpha \to \infty} \frac{\#\text{ of present residues mod } 2^\alpha}{2^\alpha}.$$

Section 3, breaks down the search for present residues according to their parity. Section 4 introduces a new approach, which characterizes the residues using 2-adic valuations. Section 5.4 uses this approach to characterize completely the number of residues $\bmod 2^\alpha$ that are congruent to $2 \bmod 8$. Section 7 summarize our results and remaining conjectures, and Section 8 discusses avenues for future progress.

The following notation is used:

1. $C(n)$ denotes the n^{th} Catalan number.

2. $s_p(n)$ denotes the sum of the base-p digits of n.

3. $\nu_p(n)$ denotes the p-adic valuation of n, that is, the exponent of p in the prime factorization of n.

Contents

1 Results for small α

The following recurrences by Xin-Xu (2011) will be used frequently throughout this paper [3].

Recurrence 1.1. $C(2m+1) = C(m) + \sum_{i\geq 1} \binom{2m}{2i} 2^{2i} C(m-i)$

Recurrence 1.2. $C(2m) = \sum_{i\geq 1} \binom{2m-1}{2i-1} 2^{2i-1} C(m-i)$

They are proved simply by induction.

Another useful result, which uses these recurrences, is the following:

Theorem 1.3. *The n^{th} Catalan number $C(n)$ is odd if and only if $n = 2^\alpha - 1$ for some $\alpha \in \mathbb{N}$.*

The proof of Theorem 1.3 is based on the following result by Legendre.

Theorem 1.4. $\nu_p(n!) = \frac{n-s_p(n)}{n-1}$

Proof. It is not difficult to see that

$$\nu_p(n!) = \lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \lfloor n/p^3 \rfloor + \cdots$$

Next, write n in base p:

$$\begin{aligned} \frac{n}{p} &= \frac{a_0}{p} + a_1 + a_2 p + \cdots \\ \frac{n}{p^2} &= \frac{a_0 + a_1 p}{p^2} + a_2 + a_3 p + \cdots \\ \frac{n}{p^k} &= \frac{a_0 + a_1 p + \cdots + a_{k-1} p^{k-1}}{p^k} + a_k + a_{k+1} p + \cdots \end{aligned}$$

Observe that by taking the floor of both sides, the first term fraction on the right-hand side vanishes. Then

$$\begin{aligned}\nu_p(n!) = a_1 + &a_2 p + a_3 p^2 + \cdots + a_r p^{r-1} \\ &+ a_2 + a_3 p + \cdots + a_r p^{r-2} \\ &\qquad + a_3 + \cdots + a_r p^{r-3} \\ &\qquad\qquad \vdots\end{aligned}$$

Or,

$$\begin{aligned}\nu_p(n!) &= a_1 + a_2(p+1) + a_3(p^2+p+1) + \cdots + a_r(\sum_{j=0}^{r-1} p^j) \\ &= \frac{1}{p-1}[a_1(p-1) + a_2(p^2-1) + a_3(p^3-1) + \cdots + a_r(p^r-1)] \\ &= \frac{1}{p-1}[a_1 p + a_2 p^2 + a_3 p^3 + \cdots + a_r p^r - \sum_{j=1}^{r} a_j] \\ &= \frac{1}{p-1}[(n-a_0) - \sum_{j=1}^{r} a_j] \\ &= \frac{n - s_p(n)}{p-1}.\end{aligned}$$

□

Proof of Theorem 1.3. Suppose $n = 2^\alpha - 1$. Then, by definition we have that

$$\begin{aligned}\nu_2\Big(C(2^\alpha - 1\Big) &= \nu_2\left(\frac{1}{2^\alpha}\binom{2^{\alpha+1}-2}{2^\alpha - 1}\right) \\ &= \nu_2\Big((2^{\alpha+1}-2)!\Big) - 2\nu_2\Big((2^\alpha - 1)!\Big) - \nu_2\left(2^\alpha\right) \\ &= 2^{\alpha+1} - 2 - s_2(2^{\alpha+1}-2) - 2\left(2^\alpha - 1 - s_2(2^\alpha - 1)\right) - \alpha \\ &= 2^{\alpha+1} - 2 - s_2\left(2^{\alpha+1}-2\right) - 2^{\alpha+1} + 2 + 2s_2\left(2^\alpha - 1\right) - \alpha \\ &= s_2(2^\alpha - 1) - \alpha \\ &= 0.\end{aligned}$$

Thus, $C(n)$ is odd. Now suppose $C(n)$ is odd.

Then take recurrences 1.1 and 1.2 modulo 2 to obtain:

$$C(2m+1) \equiv C(m) \bmod 2 \tag{1}$$

$$C(2m) \equiv 0 \bmod 2. \tag{2}$$

If n were even, then equivalence (2) shows that $C(n)$ must be even, a contradiction. Therefore, let $n = 2m+1$. In this notation, the first equivalence shows that $C(m)$ must also be odd, so by the inductive hypothesis, $m = 2^\beta - 1$. Then $n = 2m+1 = 2(2^\beta - 1) + 1 = 2^{\beta+1} - 1 = 2^\alpha - 1$. □

We now establish the eventually absent residues mod 4, 8, and 16.

Proposition 1.5. *The n^{th} Catalan number $C(n) \not\equiv 3 \bmod 4$ for any n.*

Proof by induction. Recurrences 1.1 and 1.2 modulo 4 give the following equivalences:

$$C(n) = C(2m+1) \equiv C(m) \bmod 4 \tag{3}$$

$$C(n) = C(2m) \equiv \binom{2m-1}{1} \cdot 2 \cdot C(m-1) \bmod 4 \tag{4}$$

For these recurrences, two base cases are necessary: $C(0) = 1 \equiv 1 \bmod 3$ and $C(1) = 1 \equiv 1 \bmod 3$.

In equivalence (3), $C(m) \not\equiv 3 \bmod 4$ implies $C(n) \not\equiv 3 \bmod 4$ by induction. In equivalence (4), $C(n)$ is even. Therefore $C(n) \not\equiv 3 \bmod 4$. □

Proposition 1.6. *The n^{th} Catalan number $C(n) \not\equiv 1 \bmod 8$ for $n \geq 2$.*

Proof by induction. The following base cases are sufficient for both the even and odd recurrences: $C(2) = 2 \equiv 8 \bmod 8$, $C(3) = 5 \equiv 8 \bmod 8$, and $C(4) = 14 \equiv 6 \bmod 8$. By Theorem 1, n must be odd in order for $C(n)$ to be odd. Let $n = 2m+1$ and use recurrence 1.1 modulo

8 to obtain

$$\begin{aligned} C(2m+1) &\equiv C(m) + \binom{2m}{2} \cdot 2^2 \cdot C(m-1) \bmod 8 \\ &= C(m) + (4m(2m+1))\, C(m-1) \bmod 8. \end{aligned}$$

If m were even, then $C(2m+1) \equiv C(m) \bmod 8$. By the inductive hypothesis, $C(m) \not\equiv 1 \bmod 8$, and so neither is $C(n)$. If m is odd, then Theorem 1.3 shows that $C(m-1)$ is even, and again $C(2m+1) \equiv C(m) \bmod 8$, so $C(n) \not\equiv 1 \bmod 8$. □

Lemma 1.7. $C(2^k - 1) \equiv 13 \bmod 16$ *for* $k \geq 3$.

Proof by induction. If $k = 3$, then $C(2^3 - 1) = C(7) = 449 \equiv 13 \bmod 16$.

Taking recurrence 1.2 modulo 16 gives

$$C(2m+1) \equiv C(m) + 4m(2m-1)C(m-1) \bmod 16.$$

Then, substituting $2m + 1 = 2^k - 1$,

$$C(2^k - 1) \equiv C(2^{k-1} - 1) + 4m(2m-1)C(2^{k-1} - 2) \bmod 16.$$

The inductive hypothesis gives

$$C(2^k - 1) \equiv 13 + 4m(2m-1)C(2^{k-1} - 2) \bmod 16.$$

It suffices to prove $C(2^{k-1} - 2) \equiv 0 \bmod 4$, as then the right term would vanish and then $C(2^k - 1) \equiv 13 \bmod 16$, as desired.

Recurrence 1.1 shows this:

$$\begin{aligned}C(2n) &\equiv \sum_{i\geq 1}\binom{2m-1}{2i-1}2^{2i-1}C(m-i) \bmod 16\\ &\equiv 2(2n-1)C(n-1)+\frac{4}{3}(2n-1)(2n-2)(2n-3)C(n-2) \bmod 16\end{aligned}$$

and $C(2^{k-1}-2)\equiv C(2(2^{k-2}-1))$

$$\equiv 2(2^{k-1}-3)C(2^{k-2}-2)+\frac{4}{3}(2^{k-1}-3)(2^{k-1}-4)(2^{k-1}-5)C(2^{k-2}-3) \bmod 16.$$

Then since $C(2^{k-2}-2)$ is even then $2(2^{k-1}-3)C(2^{k-2}-2)$ is divisible by 4 and $\frac{4}{3}(2^{k-1}-3)(2^{k-1}-4)(2^{k-1}-5)C(2^{k-2}-3)$ is divisible by 4. Thus $C(2^{k-1}-2)$ is divisible by 4. It follows that $C(2^k-1)\equiv 13 \bmod 16$ for $k\geq 3$. □

Proposition 1.8. *The n^{th} Catalan number $C(n)\not\equiv 5 \bmod 16$ for $n\geq 4$.*

Proof. In order for $C(n)\equiv 5 \bmod 16$ then $n=2^k-1$. However, by Lemma 1.7 if $k\geq 3$ then $C(2^k-1)\equiv 13 \bmod 16$. Thus $C(n)\not\equiv 5 \bmod 16$. □

Lemma 1.9. *Suppose $C(m)\equiv C(m+1)\equiv 2 \bmod 4$. Then, $m=2^k$ for some $k\in\mathbb{N}$.*

Proof. Theorem 1.3 shows that the result is equivalent to

$$\nu_2\Big(C(m+1)\Big)=\nu_2\Big(C(m)\Big)=1 \implies \nu_2\Big(C(m-1)\Big)=0.$$

A first-order recurrence for Catalan numbers is

$$C(m+1)=\frac{2(2m+1)}{m+2}C(m). \tag{5}$$

Taking the 2-adic valuation gives

$$1=\nu_2(C(m+1))=\nu_2\left(\frac{2(2m+1)}{m+2}C(m)\right)=\nu_2(2)+\nu_2(2m+1)+\nu_2(C(m))-\nu_2(m+2).$$

It follows that $\nu_2(m+2)=1$. Thus, $m+2=2\alpha$ for some odd integer α. Hence, $m=2(\alpha-1)$ so m is even.

Next, notice that from recurrence (5),

$$C(m+1) = \frac{2(2m+1)(2m-1)}{(m+2)(m+1)} C(m-1).$$

So,

$$\nu_2\Big(C(m+1)\Big) = \nu_2\left(\frac{2(2m+1)\cdot 2(2m-1)}{(m+2)(m+1)} C(m-1)\right).$$

This implies

$$\nu_2\Big(C(m-1)\Big) = \nu_2(C(m+1)) - (2 - \nu_2(m+2)) = 0$$

Therefore, $C(m-1)$ is odd, so m must be of the form $m = 2^k$ for some $k \in \mathbb{N}$. □

Lemma 1.10. *Let $m \geq 2$. Then, $C(2^m) \equiv 6 \bmod 8$.*

Proof. For simplicity, substitute $n = m-1$. We will prove the following,

$$C(2^{n+1}) \equiv 6 \bmod 8 \text{ for } n \geq 1.$$

By Recursion 1.2,

$$C\Big(2(2^n)\Big) = 2\Big(2(2^n) - 1\Big)C(2^n - 1).$$

So,

$$\begin{aligned} C\Big(2(2^n)\Big) &\equiv 2\Big(2(2^n) - 1\Big)C(2^n - 1) \bmod 8 \\ &\equiv 2\Big(2^{n+1} - 1\Big)C(2^n - 1) \bmod 8 \\ &\equiv 10(2^{n+1} - 1) \bmod 8 && \text{(as } C(2^n-1) \text{ is odd and not equivalent to } 3,7 \bmod 8.) \\ &\equiv 2(2^{n+1} - 1) \bmod 8. \end{aligned}$$

Now, it is clear that $2^{n+1} - 1 \equiv 3 \bmod 4$. This implies $2^{n+1} - 1 \equiv 3 \bmod 8$ or $7 \bmod 8$. Moreover, $3 \cdot 2 \equiv 6 \bmod 8$ and $7 \cdot 2 \equiv 6 \bmod 8$. Thus,

$$C\Big(2(2^n)\Big) \equiv 6 \bmod 8.$$

□

Lemma 1.11. *Let $k \geq 2$. Then, $C(2^k+1) \equiv 6 \bmod 8$.*

Proof. Let $k \in \mathbb{N}$. Recursion 1.1 gives

$$\begin{aligned} C(2^k+1) &\equiv C(2^{k-1}) + 4(2^{k-1})(2(2^{k-1})-1)C(2^{k-1}-1) \bmod 8 \\ &\equiv C(2^{k-1}) \bmod 8. \end{aligned}$$

Then Lemma 1.10 imlies $C(2^{k-1}) \equiv 6 \bmod 8$. Thus, $C(2^k+1) \equiv 6 \bmod 8$. □

Proposition 1.12. *The n^{th} Catalan number $C(n) \not\equiv 10 \bmod 16$ for $n \geq 6$.*

Proof. First observe that the result holds for $n = 0, 1, \ldots, 6$. With these base cases, the following may be proven by induction for $n \geq 7$.

Suppose n is even ($n = 2m$). Recurrence 1.2 modulo 16:

$$C(2m) \equiv (2m-1)2C(m-1) + \frac{4}{3}(2m-1)(2m-2)(2m-3)C(m-2) \bmod 16.$$

Suppose $C(n) \equiv 10 \bmod 16$ for some even $n \in \mathbb{N}$. Then

$$(2m-1)2C(m-1) + \frac{4}{3}(2m-1)(2m-2)(2m-3)C(m-2) \equiv 10 \bmod 16,$$

$$6(2m-1)C(m-1) + 4(2m-1)(2m-2)(2m-3)C(m-2) \equiv 14 \bmod 16.$$

Suppose m is odd. Then $C(m-1)$ is even, so $4 \mid 6(2m-1)C(m-1)$ and $4 \mid 4(2m-1)(2m-2)(2m-3)C(m-2)$. But $14 \equiv 2 \bmod 4$. Then $0 \equiv 2 \bmod 4$, a contradiction.

Now suppose m is even. Then $C(m-2)$ is even, and so

$$16 \mid 4(2m-1)(2m-2)(2m-3)C(m-2).$$

Now,

$$6(2m-1)C(m-1) \equiv 14 \bmod 16.$$

By testing out the possible residues for $(2m-1)C(m-1)$ it is clear that this implies

$$(2m-1)C(m-1) \equiv 5 \bmod 8.$$

Since $n \geq 7$, $m \geq 4$,

$$(-1)C(m-1) \equiv 5 \bmod 8,$$

that is,

$$C(m-1) \equiv -5 \bmod 8 \equiv 3 \bmod 8.$$

But no Catalan number is equivalent to 3 mod 4, so this is a contradiction.

Now suppose n is odd ($n = 2m+1$). Consider recurrence 1.1 modulo 16:

$$\begin{aligned} C(2m+1) &\equiv C(m) + 4m(2m-1)C(m-1) \bmod 16 \\ &\equiv 10 \bmod 16. \end{aligned}$$

Since $m-1$ is even, $C(m-1)$ is even. If $4 \mid C(m-1)$, then the second term would disappear and $C(2m+1) \equiv C(m) \equiv 10 \bmod 16$, which is not true by the inductive hypothesis.

Therefore, $C(m-1) \equiv 2 \bmod 4$. Then

$$C(m) + 8m(2m-1) \equiv 10 \bmod 16.$$

It is impossible for $C(m) \equiv 10 \bmod 4$, so $C(m)+8 \equiv 10 \bmod 16$, or $C(m) \equiv 2 \bmod 16$. Thus, $C(m-1) \equiv C(m) \equiv 2 \bmod 4$ and by applying Lemma 1.9, it can be concluded $m-1 = 2^k$ or $m = 2^k+1$, some k. But by Lemma 1.11, $C(2^k+1) \equiv 6 \bmod 8$ for $k \geq 2$, and so this is a contradiction. This completes the proof. □

2 Obtaining an upper bound

We ultimately seek to find the proportion of present residues modulo 2^α as α goes to infinity, that is

$$\lim_{\alpha\to\infty} \frac{\#\text{ of present residues } \bmod 2^\alpha}{2^\alpha}$$

Using the propositions from the previous section, the following upper bound is achieved:

Theorem 2.1. $\lim_{\alpha\to\infty} \dfrac{\#\ \textit{of present residues} \mod 2^\alpha}{2^\alpha} \leq \dfrac{1}{2}$

Proof. First observe the following:

- Modulo 2^α, there are precisely $2^{\alpha-2}$ residues congruent to 3 mod 4.
- Modulo 2^α, there are $2^{\alpha-3}$ residues congruent to 1 mod 8.
- Modulo 2^α, there are $2 \cdot 2^{\alpha-4}$ residues congruent to 5 or 10 mod 16.

Note that we count only the residues that have not been determined to be eventually absent under a smaller modulus. For example, 5 mod 16 $\not\equiv$ 3 mod 4.

Definition 2.2. A *new residue* is an eventually absent residue b mod 2^α such that for $a < \alpha$, b mod 2^a is not eventually absent.

Therefore,

$$\frac{\#\text{ of } \textit{absent} \text{ residues} \mod 2^\alpha}{2^\alpha} \geq \frac{2^{\alpha-2} + (2^{\alpha-3} - 2) + 2 \cdot (2^{\alpha-4} - 1)}{2^\alpha}$$

Letting $\alpha \to \infty$,

$$\frac{2^{\alpha-2} + 2^{\alpha-3} + 2 \cdot 2^{\alpha-4}}{2^\alpha} = \frac{1}{2}$$

□

This bound is strengthened using Rowland's finite automata for Catalan numbers mod 2^α, $\alpha = 1, 2, \ldots, 8$ [2]. The mod 4 automaton has been reproduced below:

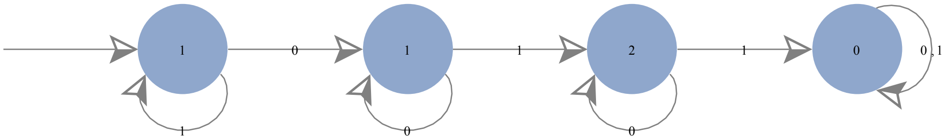


Figure 1: Finite automaton characterizing the residues of Catalan numbers modulo 4.

Example 2.3. One can use this to compute $C(n)$ mod 4 by first writing n in binary form, then reading the digit sequence from right to left. Starting from the top node, one would follow the path corresponding to 0 for every 0 traversed, and the path corresponding to 1 for every 1 traversed. When all the digits are read, the final node will be the residue mod 4.

Observe that 3 does not appear on this diagram; therefore, 3 mod 4 is an absent residue. Eventually absent residues can also be quickly identified. The mod 8 automaton has been reproduced below.

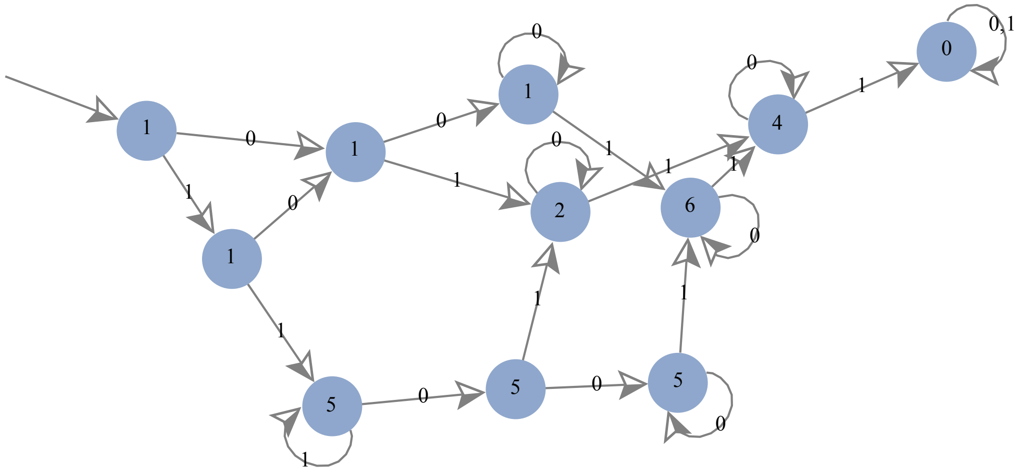


Figure 2: Finite automaton characterizing the residues of Catalan numbers modulo 8.

Note that in this diagram there are only 2 paths to a 1: if $n = 0$ or if $n = 1$. Therefore, 1 mod 8 is an eventually absent residue.

Earlier this year, Rowland and Yassawi produced similar automata for Catalan numbers mod 2^α, $\alpha = 4, 5, \ldots, 8$ [2]. Using this, we calculated the proportion of eventually absent residues and obtained the upper bound $\frac{35}{128} \approx .27$.

Later, we conjecture that all residues congruent to 0 mod 8 are present; that is, at least $\frac{1}{8}$ of residues are present. We therefore place the limit somewhere between .125 and .27.

3 Examining residues mod powers of 2

We now shift from examining absent residues to characterizing the ones that are present. The following table gives the number of present residues modulo 2^α.

α	0	1	2	3	4	5	6	7	8
Residues	1	2	3	6	11	19	34	59	104

There do not appear to be any immediate patterns, so we divide the residues by parity; that is, we examine separately the residues congruent to 1 mod 2 and those congruent to 0 mod 2.

Odd Residues

For odd residues, the pattern is clear.

α	0	1	2	3	4	5	6	7	8
Residues	0	1	1	2	3	4	5	6	7

By Theorem 1.3, the only Catalan numbers congruent to an odd residue will have the form $C(2^a - 1)$. In 2011, Lin proved the following results [1]:

Theorem 3.1 (Lin). *Let $\alpha \geq 2$, the odd congruences $C(2^b - 1) \pmod{2^\alpha}$, remain constant for $b \geq \alpha - 1$ and are distinct for $b = 1, 2, \ldots, \alpha - 1$.*

Corollary 3.2 (Lin). *The sequence of Catalan numbers $\{C(n)\}_{n\in\mathbb{N}}$ when viewed modulo 2^α has exactly $\alpha - 1$ odd residues.*

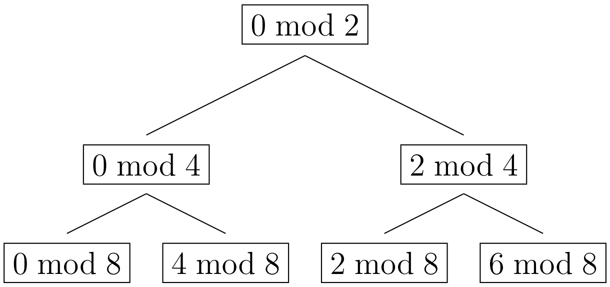
This characterizes exactly the number of odd present residues modulo 2^α.

Even Residues

The following table contains the number of even residues for small α.

α	0	1	2	3	4	5	6	7	8
Residues	1	1	2	4	8	15	29	53	97

There were not any distinguishable patterns here so we proceeded by looking at the tree that divides the number of even residues m according to the residue $m \bmod 2^\alpha$.



The only node on the mod 8 level for which we have a complete characterization is 2 mod 8.

α	0	1	2	3	4	5	6	7	8
Residues	0	0	1	1	2	3	5	6	7

We found that the sequence continues to be linear; in particular, there are $\alpha - 1$ residues of this form modulo 2^α.

The 4 mod 8 and 6 mod 8 nodes had the least discernible patterns. Computation by `Mathematica` was able to extend this tree to the mod 2^9 level, but was only able to provide 4 nonzero terms in the sequence. Therefore, it is difficult to make predictions at this point.

The 0 mod 8 is of interest because it appears to be the fastest growing out of the nodes on its level.

α	0	1	2	3	4	5	6	7	8	...	α
Residues	1	1	1	1	2	4	8	16	32	...	$2^{\alpha-3}$

Here, it appears that every residue of this form is present, and so the following conjecture may be produced:

Conjecture 3.3. Modulo 2^α (for any α), all residues congruent to 0 mod 8 are present.

This conjecture has been tested up to $\alpha = 13$. This result would be quite powerful, because then the proportion of residues that are present must be bounded below by $\frac{2^{\alpha-3}}{2^\alpha} = \frac{1}{8}$. This conjecture may be divided into smaller conjectures, for example,

Proposition 3.4. *There exists an n such that $C(n) \equiv 0 \bmod 2^\alpha$ for any α.*

Before proving this, we first introduce some new notation.

4 A new approach

In this section, we use 2-adic valuations to further classify the even residues.

Definition 4.1. For all $i \in \mathbb{N}$, define $D(i) = \{n \in \mathbb{N} \mid \nu_2(C(n)) = i\}$.

Applying Theorem 1.4 to the explicit formula for the n^{th} Catalan number $\frac{1}{1+n}\binom{2n}{n}$, it follows that

$$D(i) = \{n \in \mathbb{N} \mid s_2(n) - \nu_2(n+1) = 1\}.$$

Proposition 4.2. *For all $i \in \mathbb{N}$, $D(i) \neq \varnothing$.*

Proof. Let $i \in \mathbb{N}$. Consider the integer m with the following base-2 representation:

$$m = \underbrace{1\,1\ldots1\,1}_{\text{exactly } i \text{ \# of 1's}}\ 0\,1_2.$$

Clearly, $s_2(m) = i + 1$. But also, notice that $m + 1$ must be of the form $11\ldots1110_2$ and so, $\nu_2(m+1) = 1$. Hence, it follows that $s_2(m) - \nu_2(m+1) = i$. Thus, $m \in D(i)$. □

Note. This result implies that the collection of $D(i)$'s forms a partition of $\mathbb{N}$.

Corollary 4.3. *For all $i \in \mathbb{N}$, $D(i)$ is an infinite set.*

Proof. Notice that in the proof of Proposition 4.2, the argument holds if one replaces 0 with a finite number of zeros. That is to say,

$$\underbrace{1\,1\ldots1\,1}_{\text{exactly } i \text{ \# of 1's}}\ 0\ \underbrace{0\,0\ldots0\,0}_{\text{finitely many}}\,1_2 \in D(i).$$

□

Proof of Proposition 3.4. Let $\alpha \in \mathbb{N}$. It is clear from the definition that every element of $D(\alpha)$ possesses this property. Furthermore, if $\beta > \alpha$, then so do the elements of $D(\beta)$. □

Next, it is natural to take a closer look at the residues of $C(n) \bmod 2^\alpha$, in particular when n is restricted to $D(i)$'s.

Fix $i \in \mathbb{N}$. Consider the set of residues given by the Catalan numbers corresponding to the elements of $D(i)$ modulo 2^α, denoted by $A_j(i)$ where $j = \alpha - i$. We then get the following table:

Residues of $C(n)$, for $n \in D(i)$:

2^i:	Residues of Catalan numbers:
2^k, $k \leq i$	$\{0\}$
2^{i+1}	$A_1(i)$
2^{i+2}	$A_2(i)$
2^{i+3}	$A_3(i)$
$\vdots$	$\vdots$

Now, from our results above, $A_j(i)$ is nonempty for all $i, j \in \mathbb{N}$ and moreover, these sets do not contain 0. Furthermore, the elements (that is to say, the residues) of $A_j(i)$ must all be multiples of 2^i. This raises the following two conjectures:

Conjecture 4.4. For $i \geq 3$, $A_1(i) \subsetneq A_2(i) \subsetneq A_3(i) \subsetneq \ldots$

Conjecture 4.5. For $i \geq 3$, $|A_j(i)| = 2^j$

Observe that the latter conjecture is equivalent to Conjecture 3.3. In order to prove this, it suffices to show that every residue congruent to $8j \bmod 2^\alpha$ is present. First, notice that according to Proposition 4.2 each $D(i)$ is nonempty. Since 0 is the only residue given by $D(\alpha)$ modulo 2^α, the residues $0 \bmod 2^\alpha$ are present for any α. It also follows from the infinitude of $D(\alpha - 1)$ that the residue $2^{\alpha-1} \bmod 2^\alpha$ is present.

A next step would be to examine the residues of the form $2^{\alpha-2} \bmod 2^\alpha$ and $2^{\alpha-2} + 2^{\alpha-1} \bmod 2^\alpha$. The set $D(\alpha - 2)$ guarantees the existence of one of these residues, however it is still necessary to prove the existence of both. It would therefore be helpful to characterize the elements of $D(i)$ in a way that can identify the residues modulo 2^α. We begin with the following characterization.

Theorem 4.6. *For all $i \in \mathbb{N}$, the elements of $D(i)$ are precisely of the following form,*

$$n = (1\,\chi_1\,1\,\chi_2\,\ldots\,1\,\chi_i\,0\,\chi')_2$$

where each χ_j represents a finite, arbitrary collection of 0's (possibly none), and χ' represents a finite, arbitrary collection of 1's (possibly none).

Proof. Let $i \in \mathbb{N}$. To show that these integers are indeed elements of $D(i)$ is straightforward. So, it suffices to show that every integer in $D(i)$ must necessarily be of this form.

Let $n \in D(i)$. Suppose first that n is even. Then, it follows that $\nu_2(n+1) = 0$ and so it must be the case that $s_2(n) = i$. That is to say, the base-2 representation of n must contain exactly i 1's. Since n is even, n may be expressed as above where χ' is taken to be an empty list. Thus,

$$n = (1\,\chi_1\,1\,\chi_2\,\ldots\,1\,\chi_i\,0\,\chi')_2.$$

Next, suppose n is an odd number. Then, this implies that the base-2 representation of n terminates with finitely many $1's$, say k. However, notice also that the base-2 representation of n cannot contain only 1's. Indeed, for if this were the case, then n would be one less than a power of 2; which in turn would contradict our assumption that $i \neq 0$. Now, more explicitly, n can be expressed as the following

$$n = \left(1\,\ldots\,0\,\underbrace{1\,1\,\ldots\,1\,1}_{k}\right)_2.$$

So, $s_2(n) = k + \ell$ for some positive integer ℓ. But also, by adding 1 to n, it is easy to see that the base-2 representation of $n+1$ will terminate in precisely k number of 0's. Hence, $\nu_2(n+1) = k$. Furthermore, as $n \in D(i)$, it must be the case that

$$s_2(n) - k = i.$$

Thus,

$$k + \ell - k = i \text{ and so } \ell = i.$$

Hence, n must contain i number of 1's, followed by at least one 0, followed by a finite sequence containing finitely many 0's and precisely i number of 1's. This proves the theorem. □

5 2 mod 8

In September 2011, Guoce Xin and Jing-Feng Xu generalized Theorem 3.1 by Hsueh-Yung Lin to include all $C(n)$ where n is odd [3].

Theorem 5.1. *Let $r \geq 1$ and $\alpha \in \mathbb{N}$ with $s_2(\alpha) < r$. Then if $b \geq r - 1 - s_2(\alpha)$, we have $C(2^b(2\alpha+1) - 1 \equiv C(2^{r-1-s_2(\alpha)}(2\alpha+1) - 1) \pmod{2^r}$. Moreover, the congruence classes $C(2^b(2\alpha+1)-1) \pmod{2^r}$, $b = 1, 2, \ldots, r-1-s_2(\alpha)$ are all distinct.*

This theorem is used to characterize the number of residues mod 2^α congruent to 2 mod 8. (see Theorem 5.4.)

α	0	1	2	3	4	5	6	7	8
Residues	0	0	1	1	2	3	5	6	7

Lemma 5.2. *For $n \in \mathbb{N}$, $C(n)$ mod 2^α has at least $\alpha - 4$ residues congruent to* 18 mod 32.

Proof. By Theorem 5.1, the congruence classes $C(2^b \cdot 3 - 1) \pmod{2^r}$, $b = 1, 2, \cdots, r-2$ are distinct. However, note that for $b = 1$ or 2, $C(2^1 \cdot 3 - 1) = C(4) = 14 \not\equiv 18 \bmod 32$ and $C(2^2 \cdot 3 - 1) = C(11) = 58{,}786 \equiv 2 \not\equiv 18 \bmod 32$. Therefore, first consider the case when $b = 3$. Then $C(2^3 \cdot 3 - 1) = C(23) = 343{,}059{,}613{,}650 \equiv 18 \bmod 32$. Now assume $C(2^{b-1} \cdot 3 - 1) \equiv 18 \bmod 32$. Then consider $C(2^b \cdot 3 - 1)$. Taking recursion 1.1 mod 32,

$$\begin{aligned} C(2^b \cdot 3 - 1) \equiv & C(2^{b-1} \cdot 3 - 1) + \binom{2(2^b \cdot 3 - 1)}{2} 4C(2^{b-1} \cdot 3 - 2) \\ & + \binom{2(2^b \cdot 3 - 1)}{4} 16C(2^{b-1} \cdot 3 - 3) \bmod 32. \end{aligned}$$

It follows from Theorem 1.3 that $C(2^b \cdot 3 - 3)$ is even. Therefore the last term disappears. To evaluate the second term, consider

$$\nu_2\left(4C(2^{b-1} \cdot 3 - 2)\right) = 2 + \nu_2\left(C(2^{b-1} \cdot 3 - 2)\right).$$

By Theorem 1.4, it follows that

$$\begin{aligned}\nu_2\left(4C(2^{b-1}\cdot 3-2)\right) &= 2+s_2(2^{b-1}\cdot 3-2)-\nu_2(2^{b-1}\cdot 3-1)\\ &= 2+s_2(2^{b-1}\cdot 3-2).\end{aligned}$$

Note that $2^{b-1}\cdot 3$ has binary representation $11\underbrace{0\cdots 0}_{b-1}$, and so $2^{b-1}\cdot 3-1$ has binary representation $10\underbrace{1\cdots 1}_{b-1}$. Therefore $s_2(2^{b-1}\cdot 3-2)=b-1$, and so $\nu_2(4C(2^{b-1}\cdot 3-2))=b+1\geq 5$ since $b\geq 4$.

The second term also disappears, so

$$C(2^b\cdot 3-1)\equiv C(2^{b-1}\cdot 3-1) \bmod 32.$$

Assuming the inductive hypothesis,

□

Lemma 5.3. *For* $n\in\mathbb{N}$ *and* $\alpha\geq 5$, $C(n) \bmod 2^\alpha$ *has exactly* $\alpha-4$ *residues congruent to* $18 \bmod 32$.

Proof. Suppose $C(n)\equiv 18 \bmod 32$. Then $\nu_2(C(n))=1$ since $\nu_2(18+2^5j)=1$ for any j. Thus, $n\in D(1)$ and therefore has binary expansion $1\chi_1 0\chi'$, where χ_1 is an arbitrary number of zeroes and χ' is an arbitrary number of ones.

If n were even, then χ' must consist of no ones so n is a power of 2. But it follows from Lemma 1.11, $C(2^n)\equiv 6 \bmod 8$ for $n\geq 2$. Observe the following:

- $C(2^0)=1\not\equiv 18 \bmod 32$
- $C(2^1)=2\not\equiv 18 \bmod 32$.

n cannot be a power of 2 and thus n cannot be even.

Thus n is odd and can be expressed as $n=2^b\cdot m-1$, where m is odd. The goal is to prove $C(2^b\cdot m-1)\equiv 18 \bmod 32 \implies m=3$. This would show that in Theorem 5.1, the $r-4$ residues produced for $\alpha=1$ are all that can be produced; that is, no other α produces additional residues congruent to 18 mod 32.

Recall that $2^b \cdot m - 1$ has binary expansion $1\chi_1 0\chi'$. Note that the binary representation of $2^b \cdot m$ is precisely the binary representation of m followed by b zeroes. Then the binary representation of $2^b \cdot m - 1$ is precisely the binary representation of $m - 1$ followed by b ones. Thus, in order for $2^b \cdot m - 1$ to satisfy the form of elements of $D(1)$, it must be that $s_2(m-1) = 1$. Thus m is one more than a power of two: $m = 2^a + 1$.

Writing $C(n)$ as $C(2^b(2^a+1) - 1$, it suffices to prove

$$C(2^b(2^a+1)-1) \equiv C(2^{b+a} + 2^b - 1) \equiv 18 \bmod 32 \Longrightarrow a = 1.$$

Now proceed by induction on b.

First consider the case when $b = 3$ and $a = 2$. Then $C(2^{2+3} + 2^3 - 1) = C(32 + 8 - 1) = C(39) = 6 \bmod 32$. Thus, $a \neq 2$. Now consider the cases for $a \geq 3$, and assume

$$C(2^{a+3} + 2^3 - 1) = C(2^{a+3} + 7) \equiv 18 \bmod 32.$$

Then by recurrence 1.1,

$$C(2^{a+3} + 7) \equiv C(2^{a+2} + 3) + \sum_{i \geq 1} \binom{2(2^{a+2} + 3)}{2i} 2^{2i} C(2^{a+2} + 3 - i) \bmod 32.$$

Note that only the terms in the sum corresponding to $i = 1, 2, 3$ need to be considered because any term corresponding to a higher i will vanish. Therefore, first consider the term where $i = 2$. Note the following:

$$\nu_2(2^4 C(2^{a+2} + 1)) = 4 + s_2(2^{a+2} + 1) - \nu_2(2^{a+2} + 2) = 4 + 2 - 1 = 5.$$

Thus, the term corresponding to $i = 2$ is congruent to 0 mod 32. Next consider when $i = 3$. Then,

$$\nu_2(2^6 C(2^{a+2})) = 6 + s_2(2^{a+2}) - \nu_2(2^{a+2} + 1) = 6 + 1 = 7.$$

Therefore, the term corresponding to $i = 3$ is also congruent to 0 mod 32, so only the first term of the sum does not vanish.

$$\begin{aligned} C(2^{a+3}+7) &\equiv C(2^{a+2}+3) + \sum_{i\geq 1} \binom{2(2^{a+2}+3)}{2i} 2^{2i} C(2^{a+2}+3-i) \\ &\equiv C(2^{a+2}+3) + 4(2(2^{a+2}+3)-1)C(2^{a+2}+2) \bmod 32. \end{aligned}$$

Now consider $C(2^{a+2}+3)$ using recurrence 1.1:

$$C(2^{a+2}+3) \equiv C(2^{a+1}+1) + \sum_{i\geq 1} \binom{2(2^{a+1}+1)}{2i} 2^{2i} C(2^{a+1}+1-i) \bmod 32.$$

Once again it is only necessary to consider the terms corresponding to $i = 1, 2, 3$. First consider when $i = 2$ and notice:

$$\begin{aligned} \nu_2\left(\binom{2(2^{a+1}+1)}{4} 2^4 C(2^{a+1}-1)\right) &= \nu_2\left(\frac{4}{3}(2^{a+1}+1)(2(2^{a+1}+1)-1)(2(2^{a+1}+1)-2\right) \\ &\quad \big(2(2^{a+1}+1)-3)C(2^{a+1}-1)\big) \\ &= \nu_2\left(\frac{4}{3}(2^{a+1}+1)(2^{a+2}+1)(2^{a+2})(2^{a+2}-1)C(2^{a+1}-1)\right) \\ &= 2+a+2 = 4+a \geq 5. \end{aligned}$$

Therefore, this term vanishes. Now consider when $i = 3$ and note:

$$\nu_2(2^6 C(2^{a+2}-1)) = 6 + s_2(2^{a+2}-1) - \nu_2(2^{a+2}) = 6 + a + 2 - a - 2 = 6.$$

Thus, only the first term of the sum is left:

$$C(2^{a+2}+3) \equiv C(2^{a+1}+1) + 2(2(2^{a+1}+1)-1)C(2^{a+1}) \bmod 32.$$

By Lemma 1.10 and Lemma 1.11, $C(2^{a+1}) \equiv 6 \bmod 8$ and $C(2^{a+1}+1) \equiv 6 \bmod 8$ for $a > 1$. Thus,

$$C(2^{a+2}+3) \equiv 6 + 4(2^{a+1}+1)(2(2^{a+1}+1)-1)6 \equiv 6 + 0 \equiv 6 \bmod 8.$$

Now,

$$C(2^{a+3}+7) \equiv 6 + 4(2(2^{a+2}+3)-1)C(2^{a+2}+2) \bmod 8.$$

Since

$$\nu_2(C(2^{a+2}+2)) = s_2(2^{a+2}+2) + \nu_2(2^{a+2}+3) = 2,$$

it follows that $C(2^{a+2}+2) \equiv 0 \bmod 4$ so $C(2^{a+2}+2) \equiv 0 \bmod 8$ or $6 \bmod 8$. Consider both cases:

Let $C(2^{a+2}+2) \equiv 0 \bmod 8$ then

$$C(2^{a+3}+7) \equiv 6 + 4(2(2^{a+2}+3)-1)C(2^{a+2}+2) \equiv 6 + 0 \bmod 8$$

which can not be congruent to $18 \bmod 32$.

Then let $C(2^{a+2}+2) \equiv 6 \bmod 8$ then

$$C(2^{a+3}+7) \equiv 6 + 4(2(2^{a+2}+3)-1)C(2^{a+2}+2) \equiv 6+6 \equiv 12 \equiv 4 \bmod 8.$$

which can not be congruent to $18 \bmod 32$. Thus when $a \geq 2$, $C(2^{a+3}+7) \not\equiv 18 \bmod 32$. Thus a must be 1 in order for $C(2^{a+3}+7) \equiv 18 \bmod 32$.

Now assume that if $C(2^{b+a-1}+2^{b-1}-1) \equiv 18 \bmod 32$ then $a = 1$. Now consider $C(2^{b+a}+2^{b}-1)$ using recurrence 1.1:

$$C(2^{b+a}+2^{b}-1) \equiv C(2^{b+a-1}+2^{b-1}-1) + \sum_{i\geq 1} \binom{2^{b+a}+2^{b}-2}{2i} 2^{2i} C(2^{b+a-1}+2^{b-1}-1-i) \bmod 32.$$

Once again it is only necessary to consider the terms of the sum corresponding to $i = 1, 2, 3$. First consider $i = 1$, then note:

$$\nu_2(2^2 C(2^{b+a-1}+2^{b-1}-2)) = 2 + s_2(2^{b+a-1}+2^{b-1}-2) - \nu_2(2^{b+a-1}+2^{b-1}-1) = 2+b-1 = b.$$

By assumption, $b > 3$, so this term vanishes. Now consider when $i = 2$.

$$\nu_2(2^4 C(2^{b+a-1}+2^{b-1}-3)) = 4 + s_2(2^{b+a-1}+2^{b-1}-3) - \nu_2(2^{b+a-1}+2^{b-1}-2) = 4+b-1-1 = b+2.$$

Therefore, this term also vanishes. Finally consider when $i = 3$.

$$\nu_2(2^6 C(2^{b+a-1}+2^{b-1}-4)) = 2+s_2(2^{b+a-1}+2^{b-1}-4)-\nu_2(2^{b+a-1}+2^{b-1}-3) = 6+b-2 = b+4.$$

Thus every term of the sum vanishes. Therefore,

$$C(2^{b+a} + 2^b - 1) \equiv C(2^{b+a-1} + 2^{b-1} - 1) \equiv 18 \bmod 32$$

which means $a = 1$. Therefore, if $C(2^{b+a} + 2^b - 1) \equiv 18 \bmod 32$ then $a = 1$ for $b \geq 3$. □

Theorem 5.4. *The number of residues modulo* 2^α *congruent to* $2 \bmod 8$ *is given by the formula*

$$f(\alpha) = \begin{cases} \max(0, \alpha - 1) & 0 \leq \alpha \leq 2, \alpha \geq 6 \\ \alpha - 2 & 2 \leq \alpha \leq 5. \end{cases}$$

Proof. Let $f(b, m, \alpha)$ be the number of residues modulo 2^α that are congruent to $b \bmod m$. It follows from Lemma 5.3 that

$$f(18, 32, \alpha) = \max(0, \alpha - 4)$$

since for $\alpha < 5$, there cannot be any residues congruent to $18 \bmod 2^5$.

Rowland and Yassawi's finite automaton for Catalan numbers mod 32 [2] shows that the only n such that $C(n) \equiv 2 \bmod 32$ are:

- 2, when $C(2) = 2 \equiv 2 \bmod 32 \equiv 2 \bmod 64$, and
- 11, when $C(11) = 58,786 \equiv 34 \bmod 64$.

Thus for $2 \geq \alpha \geq 5$, 2 is the only residue congruent to $2 \bmod 32$. And for $\alpha \geq 6$, the only such residues are caused by these two Catalan numbers, and we know they must be distinct, since they have different values mod 64. Therefore,

$$f(2, 32, \alpha) = \begin{cases} 0 & 0 \leq \alpha \leq 2 \\ 1 & 2 \leq \alpha \leq 5 \\ 2 & \alpha \geq 6. \end{cases}$$

Adding these functions, we obtain

$$f(2,16,\alpha) = \begin{cases} 0 & 0 \le \alpha \le 1 \\ 1 & 2 \le \alpha \le 3 \\ \alpha - 1 & 4 \le \alpha \le 5 \\ \alpha - 2 & \alpha \ge 6. \end{cases}$$

However, it follows from Proposition 1.12, and that $C(n) \equiv 10 \bmod 16$ only for $n = 5$, that

$$f(\alpha) = \begin{cases} 0 & 0 \le \alpha \le 3 \\ 1 & \alpha \ge 4 \end{cases}.$$

Adding these functions, we obtain

$$f(\alpha) = f(2,8,\alpha) = \begin{cases} \max(0, \alpha - 1) & 0 \le \alpha \le 2, \alpha \ge 6 \\ \alpha - 2 & 2 \le \alpha \le 5 \end{cases}$$

as desired.

□

6 0 mod 8

At this point, we revisit Conjecture 3.3:

Conjecture. Modulo 2^α (for any α), all residues congruent to 0 mod 8 are present.

We seek to characterize the binary representations of $n \in D(\alpha - i)$ in terms of the residue obtained when viewing $C(n) \bmod 2^\alpha$. For $n \in D(\alpha - 1)$, $C(n) \equiv 2^{\alpha-1} \bmod 2^\alpha$ so there is nothing to characterize. We therefore begin with $n \in D(\alpha - 2)$, where either $C(n) \equiv 2^{\alpha-2}$ or $C(n) \equiv 3 \cdot 2^{\alpha-2} \bmod 2^\alpha$. We then use this characterization to prove some results about $D(\alpha - 2)$.

$\mathbf{D(\boldsymbol{\alpha} - 2)}$

The elements of $D(\alpha-2)$ are either congruent to $2^{\alpha-2}$ or $3\cdot 2^{\alpha-2}$ modulo 2^α. They are able to be characterized simply by the following conjecture:

Conjecture 6.1. Where $n = 1\chi_1 1\chi_2\cdots 1\chi_{\alpha-2}0\chi'$ (Theorem 4.6), $n \in D(\alpha-2)$ satisfies $C(n) \equiv 2^{\alpha-2} \bmod 2^\alpha$ if and only if $\sum \delta(\chi_k)$ is even, where

$$\delta(x) = \begin{cases} 0 & \text{if } x = 0 \\ 1 & \text{if } x \neq 0 \end{cases}$$

This characterization (and those that follow) are based purely on `Mathematica` observations. While these characterizations are not proven, they will help to generate useful conjectures. For example, if n satisfies $\sum \delta(\chi_k) = 0$ and $\chi' = 1$, then by the conjecture, $C(n) \equiv 2^{\alpha-2} \bmod 2^\alpha$. This χ representation corresponds to $n = 2^\alpha - 3$. So we have the following proposition:

Proposition 6.2. *For $\alpha \geq 2$, $C(2^\alpha - 3) \equiv 2^{\alpha-2} \bmod 2^\alpha$.*

If instead $\chi_1 = 1$, $\sum_{k\geq 2}\delta(\chi_k) = 0$ and $\chi' = 1$, then $C(n) \equiv 3\cdot 2^{\alpha-2} \bmod 2^\alpha$. This is equivalent to the following:

Proposition 6.3. *For $\alpha \geq 2$, $C(3\cdot 2^\alpha - 3) \equiv 3\cdot 2^{\alpha-2} \bmod 2^\alpha$.*

We will prove Proposition 6.2; the proof for 6.3 is similar.

Lemma 6.4. *For $i \geq 3$, $3 + s_2(i) + s_2(i+1) + \nu_2(i) \leq 2i$.*

Proof. The worst case for $s_2(i)$ is when $i = 2^a - 1$, for some a, in which case $s_2(i) = a = \log_2(1+i)$. The worst case for $\nu_2(i)$ is when $i = 2^b$, for some b, in which case $\nu_2(i) = b = \log_2(i)$. Therefore,

$$3 + s_2(i) + s_2(i+1) + \nu_2(i) \leq 3 + \log_2(i) + \log_2(i+1) + \log_2(i+2).$$

Note that if $i = 3$, the inequality $3 + \log_2(i) + \log_2(i+1) + \log_2(i+2) \leq 2i$ holds because $2i$ grows faster than the left-hand side. This completes the proof. □

Lemma 6.5. *For $\alpha \geq 2$, $C(2^\alpha - 3) \equiv C(2^{\alpha-1} - 2) \bmod 2^\alpha$.*

Proof. Consider $C(2^\alpha - 3) \bmod 2^\alpha$. Note, $C(2^\alpha - 3) = C(2(2^{\alpha-1} - 2) + 1)$. Then by using recurrence 1.1:

$$C(2(2^{\alpha-1} - 2) + 1) = C(2^{\alpha-1} - 2) + \sum_{i \geq 1} \binom{2(2^{\alpha-1} - 2)}{2i} 2^{2i} C(2^{\alpha-1} - 2 - i) \bmod 2^\alpha.$$

Consider:

$$\begin{aligned} \nu_2(2^{2i} C(2^{\alpha-1} - 2 - i)) &= 2i + \nu_2(C(2^{\alpha-1} - 2 - i)) \\ &= 2i + s_2(2^{\alpha-1} - 2 - i) + \nu_2(2^{\alpha-1} - 1 - i). \end{aligned}$$

Note that the terms where $i > \lceil \frac{\alpha}{2} \rceil$ vanish because then $2^{2i} \equiv 0 \bmod 2$. Since $i \leq \lceil \frac{\alpha}{2} \rceil$, it follows that:

1. $\nu_2(2^{\alpha-1} - 1 - i) = \nu_2(1 + i)$

2. $s_2(2^{\alpha-1} - 2 - i) = s_2(2^{\alpha-1} - 1 - (1 + i)) = \alpha - 1 - s_2(1 + i)$

The first result is straightforward; the last equality is based on the observation that the binary representation of $2^{\alpha-1} - 1$ consists of exactly $\alpha - 1$ 1's, so that by subtracting a number j (in this case $j = 1 + i$) in base 2 of smaller length, the result is achieved by replacing every 1 that appears in j with a 0. For example,

$$\begin{array}{r} 111111111 \\ - \quad 10110 \\ \hline 111101001 \end{array}$$

Observe that the effect this has on the digit sum is to just subtract the number of ones in j. The second fact follows from this point.

This becomes

$$\nu_2\left(2^{2i} C(2^{\alpha-1} - 2 - i)\right) = 2i + \alpha - 1 - s_2(i + 1) - \nu_2(i + 1).$$

By Lemma 6.4,

$$\begin{aligned}2i &\geq 3 + s_2(i) + s_2(i+1) + \nu_2(i+1)\\&\geq 3 + s_2(i+1) + \nu_2(i+1)\\&\geq 1 + s_2(i+1) + \nu_2(i+1).\end{aligned}$$

Now, finally,

$$\begin{aligned}\nu_2\left(2^{2i}C(2^{\alpha-1}-2-i)\right) &= 2i + \alpha - 1 - s_2(i+1) - \nu_2(i+1)\\&\leq \alpha.\end{aligned}$$

Since $i \geq 3$, all but the first two terms of the summation vanish. Now examine the first two terms separately.

The first term of the sum is $2(2^\alpha - 4)C(2^{\alpha-1}-2-1)$. Note:

$$\nu_2(2(2^\alpha-4)C(2^{\alpha-1}-2-1)) = 1 + 2 + s_2(2^{\alpha-1}-3) + \nu_2(2^{\alpha-1}-3) = 3 + \alpha - 3 = \alpha.$$

Thus the first term is congruent to 0 mod 2^α.

The second term is:

$$\binom{2(2^{\alpha-1}-2)}{2}2^4C(2^{\alpha-1}-4).$$

It is sufficient to prove $\nu_2\big(2^4C(2^{\alpha-1}-4)\big) \geq \alpha$.

$$\begin{aligned}\nu_2\big(2^4C(2^{\alpha-1}-4)\big) &= 4 + s_2(2^{\alpha-1}-4) + \nu_2(2^{\alpha-1}-3)\\&= 4 + \alpha - 1 - s_2(3)\\&= 1 + \alpha.\end{aligned}$$

Thus all of the terms in the summation are congruent to 0 mod 2^α and the following can be concluded:

$$C(2^\alpha - 3) \equiv C(2^{\alpha-1} - 2) + \sum_{i\geq 1} \binom{2^\alpha - 4}{2i} 2^{2i} C(2^{\alpha-1} - 2 - i) \bmod 2^\alpha \equiv C(2^{\alpha-1} - 2) \bmod 2^\alpha.$$

□

Proof of Proposition 6.2. Clearly, $C(14) \equiv 8 \bmod 32$.

Assume that for all values $k < \alpha$, $C(2^k - 3) \equiv 2^{k-2} \bmod 2^k$. Now consider $C(2^\alpha - 3)$. Note $\nu_2(C(2^\alpha - 3)) = s_2(2^\alpha - 3) - \nu_2(2^\alpha - 2) = \alpha - 1 - 1 = \alpha - 2$. Thus $C(2^\alpha - 3) \equiv b \cdot 2^{\alpha-2} \bmod 2^\alpha$ where b is a constant and $2 \nmid b$.

Either $b = 1$ or 3 because if $b = 5$ then $5(2^{\alpha-2}) = 4(2^\alpha) + 2^\alpha = 2^\alpha \bmod 2^\alpha$. Thus when $b = 5$ it is the same as when $b = 1$. It can be similarly shown that any other higher powers of b are congruent to either $b = 1$ or $b = 3$.

Now for the sake of contradiction assume $b = 3$ so $C(2^\alpha - 3) \equiv 3(2^{\alpha-2}) \bmod 2^\alpha$. Note that $C(2^\alpha - 3) \equiv C(2^{\alpha-1} - 2) \equiv C(2(2^{\alpha-2} - 1))$. Then use recursion 1.2:

$$\begin{aligned} C(2(2^{\alpha-2} - 1)) &\equiv \sum_{i\geq 1} \binom{2(2^{\alpha-2} - 1) - 1}{2i - 1} 2^{2i-1} C((2^{\alpha-2} - 1) - i) \bmod 2^\alpha \\ &\equiv \sum_{i\geq 1} \binom{2^{\alpha-1} - 3}{2i - 1} 2^{2i-1} C(2^{\alpha-2} - 1 - i). \end{aligned}$$

Now note that $\nu_2(2^{2i-1} C(2^{\alpha-2} - 1 - i)) = 2i - 1 + s_2(2^{\alpha-2} - 1 - i) - \nu_2(2^{\alpha-2} - i) = 2i - 1 + \alpha - 2 - s_2(i) - \nu_2(i)$.

Then by Lemma 6.4 it follows that $2i \geq 3 + s_2(i) - \nu_2(i)$ for $i \geq 3$ so $2i - 1 + \alpha - 2 - s_2(i) - \nu_2(i) \geq \alpha$ for $i \geq 3$. Thus all of the terms except the first two in the summation are congruent to 0 mod 2^α. Therefore,

$$\begin{aligned} C(2(2^{\alpha-2} - 1)) &\equiv \sum_{i\geq 1} \binom{2^{\alpha-1} - 3}{2i - 1} 2^{2i-1} C(2^{\alpha-2} - 1 - i) \bmod 2^\alpha \\ &\equiv 2(2^{\alpha-1} - 3) C(2^{\alpha-2} - 2) \\ &+ \frac{4}{3}(2^{\alpha-1} - 3)(2^{\alpha-1} - 4)(2^{\alpha-1} - 5) C(2^{\alpha-2} - 3) \bmod 2^\alpha. \end{aligned}$$

Now note

$$\begin{aligned}
\nu_2\left(\frac{4}{3}(2^{\alpha-1}-3)(2^{\alpha-1}-4)(2^{\alpha-1}-5)C(2^{\alpha-1}-3)\right) &= 2+2+\nu_2(C(2^{\alpha-1}-3)) \\
&= 4+s_2(2^{\alpha-2}-3)-\nu_2(2^{\alpha-1}-3) \\
&= 4+\alpha-4 \\
&= \alpha.
\end{aligned}$$

Thus the second term also is congruent to 0 mod 2^α. Therefore, we have

$$C(2(2^{\alpha-2}-1)) \equiv 2(2^{\alpha-1}-3)C(2^{\alpha-2}-2).$$

Now by induction, $C(2^{\alpha-2}-2) \equiv 2^{\alpha-3} \bmod 2^{\alpha-1}$ so $C(2^{\alpha-2}-2) \equiv 2^{\alpha-3} \bmod 2^\alpha$ or $C(2^{\alpha-2}-2) \equiv 5(2^{\alpha-3}) \bmod 2^\alpha$. Thus let us consider both cases.

First consider the case where $C(2^{\alpha-2}-2) \equiv 2^{\alpha-3} \bmod 2^\alpha$. Then since it is also assumed above that $C(2^\alpha-3) \equiv 3(2^{\alpha-2}) \bmod 2^\alpha$ then

$$\begin{aligned}
C(2(2^{\alpha-2}-1)) &\equiv 2(2^{\alpha-1}-3)C(2^{\alpha-2}-2) \bmod 2^\alpha \\
3(2^{\alpha-2}) &\equiv 2(2^{\alpha-1}-3)2^{\alpha-3} \bmod 2^\alpha \\
&\equiv 2^{\alpha-2}(2^{\alpha-1}-3) \bmod 2^\alpha \\
&\equiv 2^{\alpha-2}(2^{\alpha-1})-3(2^{\alpha-2}) \bmod 2^\alpha \\
&\equiv -3(2^{\alpha-2}) \bmod 2^\alpha.
\end{aligned}$$

Since $3(2^{\alpha-2}) \neq -3(2^{\alpha-2}) \bmod 2^\alpha$, this is a contradiction. Thus, $C(2^{\alpha-2}-2) \not\equiv 2^{\alpha-3} \bmod 2^\alpha$.

Then let us consider the other case when $C(2^{\alpha-2}-2) \equiv 5(2^{\alpha-3}) \bmod 2^\alpha$. Then

$$\begin{aligned}
C(2(2^{\alpha-2}-1)) &\equiv 2(2^{\alpha-1}-3)C(2^{\alpha-2}-2) \bmod 2^\alpha \\
3(2^{\alpha-2}) &\equiv 2(2^{\alpha-1}-3)5(2^{\alpha-3}) \bmod 2^\alpha \\
&\equiv 5(2^{\alpha-2})(2^{\alpha-1}-3) \bmod 2^\alpha \\
&\equiv 5(2^{\alpha-2})(2^{\alpha-1}) - 15(2^{\alpha-2}) \bmod 2^\alpha \\
&\equiv -15(2^{\alpha-2}) \bmod 2^\alpha \\
&\equiv 2^{\alpha-2} \bmod 2^\alpha.
\end{aligned}$$

Since $3(2^{\alpha-2}) \not\equiv 2^{\alpha-2} \bmod 2^\alpha$, this is a contradiction. Thus, $C(2^{\alpha-2}-2) \not\equiv 5(2^{\alpha-3}) \bmod 2^\alpha$. However, this means neither case is true which is a contradiction. Thus, $C(2^\alpha - 3) \not\equiv 3(2^{\alpha-2}) \bmod 2^\alpha$. Therefore, $C(2^\alpha - 3) \equiv 2^{\alpha-2} \bmod 2^\alpha$. □

The proof that $3 \cdot 2^{\alpha-2} \bmod 2^\alpha$ is present for every α is similar.

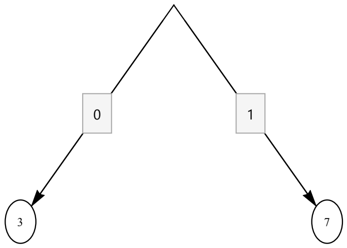
$\mathbf{D(\boldsymbol{\alpha} - 3)}$

The characterization for $D(\alpha - 3)$ is more complicated, mainly because it is affected by the position of the nonzero values among the χ_k. For example, if the nonzero values consist of a 1 and a 2, which χ_k takes on each of these values affects the resulting residue, whereas $D(\alpha - 2)$ it did not matter.

Let $n \in D(\alpha - 3)$. Arbitrary let $\chi' = 0$ so that $n = 1\chi_1 1\chi_2 \dots 1\chi_{\alpha-3}0$. Consider the values $\{\chi_1, \chi_2, \dots, \chi_{\alpha-3}\}$. We examine separately the cases $\sum \chi_k = j$.

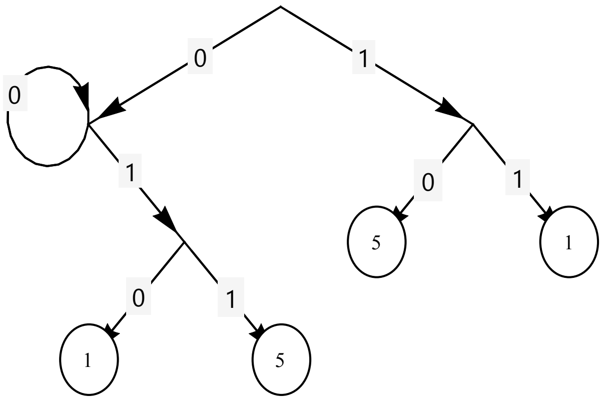
First let $j = 0$. Then, each χ_k must be 0, and so $n = 11\dots10_2$, in which case $C(n) \equiv 2^{\alpha-3} \bmod 2^\alpha$.

Now suppose $\sum \chi_n = 1$. Then there is exactly one $\chi_i = 1$. Now, if $\chi_1 = 1$ then $C(n) \equiv 7 \cdot 2^{\alpha-3} \bmod 2^\alpha$. If $\chi_1 = 0$ and any other $\chi_i = 1$ then $C(n) \equiv 3 \cdot 2^{\alpha-3} \bmod 2^\alpha$. This can be represented by the following automaton.



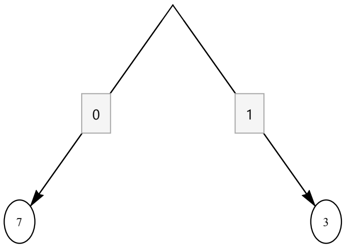
Note: in this automaton (and those that follow), the χ values are read from left to right.

Next, suppose $\sum \chi_n = 2$. This means that either there are distinct indices i, j with $\chi_i = 1$ and $\chi_j = 1$, or there exists an i with $\chi_i = 2$. If there is a $\chi_i = 1$ and $\chi_j = 1$, then there are two options. If $\chi_1 = 1$ and any other $\chi_2 = 1$ then $C(n) \equiv 2^{\alpha-3} \bmod 2^\alpha$. If $\chi_1 = 0$, $\chi_2 = 0$, and any other $\chi_j = 1$ then $C(n) \equiv 5 \cdot 2^{\alpha-3} \bmod 2^\alpha$. There are also other similar conditions that can then be represented by the following automaton.



The structure of this same automaton seems to reappear, so let it be denoted as $A_2(1, 5)$ where the 2 indicates there is one integer that appears twice in $\{\chi_1, \chi_2, \ldots, \chi_{\alpha-3}\}$.

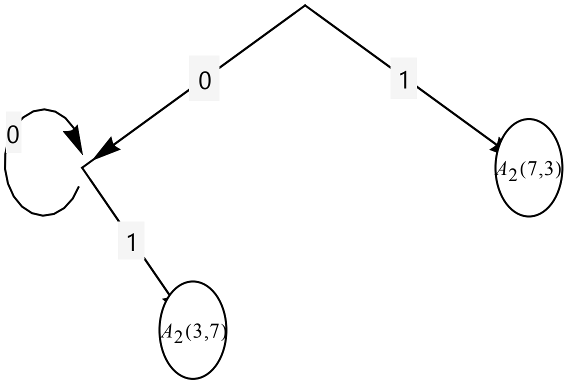
Now if $\sum \chi_n = 2$ and there exists a $\chi_i = 2$, then the following automaton represents the residues attained.



Lastly, consider the case when $\sum \chi_i = 3$. Then, it is clear that there are the following three possibilities:

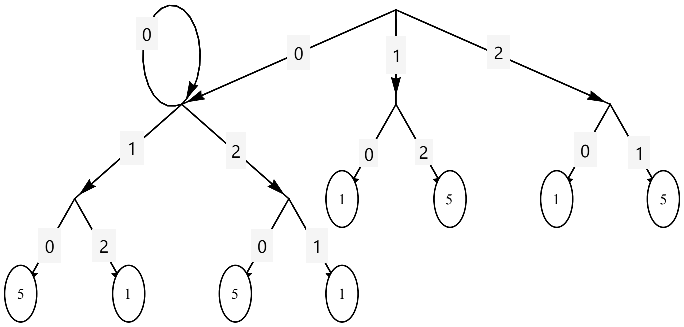
1. there exist distinct i, j, k with $\chi_i, \chi_j, \chi_k = 1$,
2. there exist distinct i, j with $\chi_i = 1$ and $\chi_j = 2$,
3. there exists i with $\chi_i = 3$.

The first case is characterized by the following automaton, $A_3(7, 3)$.



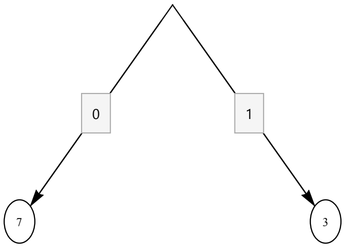
Note that $A_2(7, 3)$ and $A_2(3, 7)$ have similar structure to $A_2(1, 5)$ described above.

The following automaton characterize case 2.

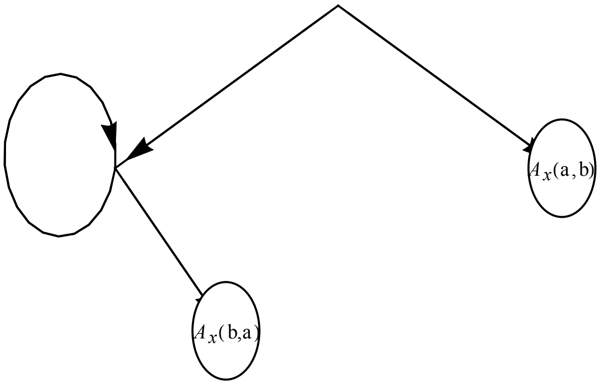


This automaton will be notated as $A_{1,1}(5,1)$ where the 1,1 indicates there are two distinct integers appearing $\{\chi_1, \chi_2, \ldots, \chi_{\alpha-3}\}$ with each appearing only once.

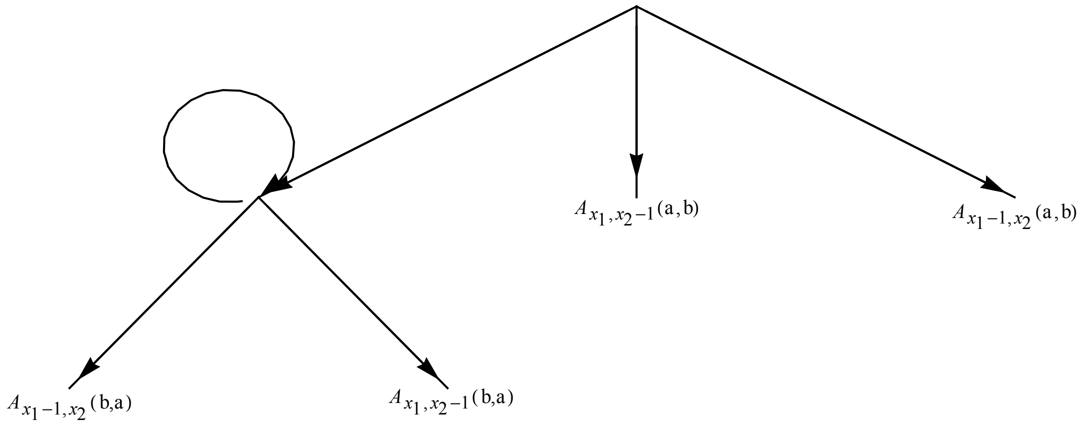
Finally, consider the automaton for case 3.



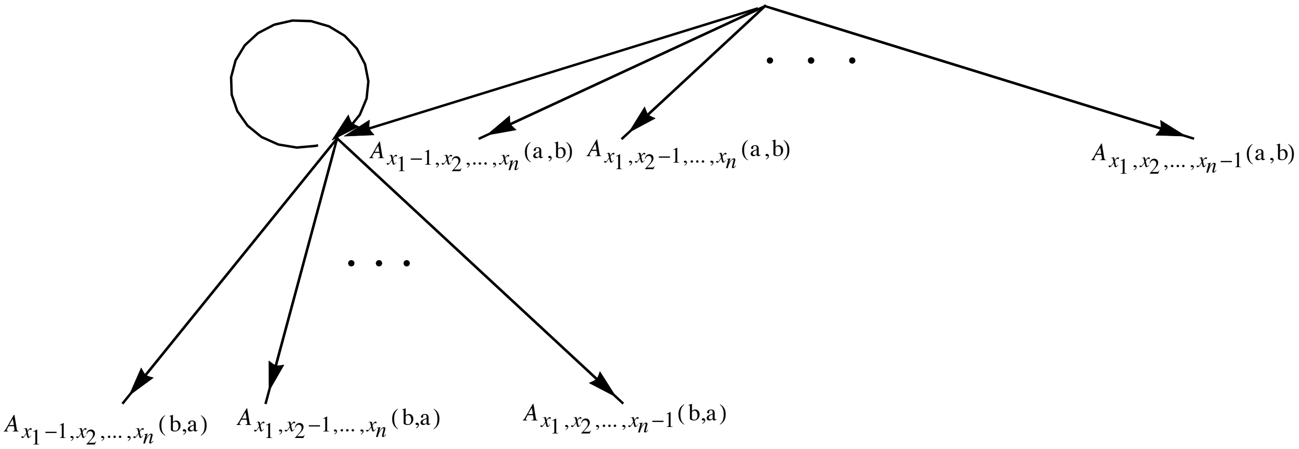
This process can then be continued for higher and higher sums; however, a pattern begins to appear. In order to state this pattern let $A_x(a,b)$ refer to the following automaton where x indicates that one distinct integer appears x times in $\{\chi_1, \chi_2, \ldots, \chi_{\alpha-3}\}$.



Then let $A_{x_1,x_2}(a,b)$ refer to the following auotmaton where x_1, x_2 indicates there are two distince integers in $\{\chi_1, \chi_2, \ldots, \chi_{\alpha-3}\}$ with one integer appearing x_1 times and the other appearing x_2 times.



Therefore, it can be concluded that $A_{x_1,\ldots,x_n}(a,b)$ can represent the general automaton in $D(\alpha-3)$:


$A_{x_1-1,x_2,\ldots,x_n}$(a,b)
$A_{x_1,x_2-1,\ldots,x_n}$(a,b)
$A_{x_1,x_2,\ldots,x_n-1}$(a,b)
$A_{x_1-1,x_2,\ldots,x_n}$(b,a)
$A_{x_1,x_2-1,\ldots,x_n}$(b,a)
$A_{x_1,x_2,\ldots,x_n-1}$(b,a)

By analyzing the above automata and using the δ function used to characterize $D(\alpha-2)$,

$D(\alpha - 3)$ can be characterized as follows:

$$D(\alpha - 3) = \begin{cases} 2^{\alpha-3}, 5 \cdot 2^{\alpha-3} & \sum \delta(\chi_k) \text{ even,} \\ 3 \cdot 2^{\alpha-3}, 7 \cdot 2^{\alpha-3} & \sum \delta(\chi_k) \text{ odd.} \end{cases}$$

This means that each automaton that corresponds to an even $\sum \delta(\chi_k)$ produces the residues $2^{\alpha-3}, 5 \cdot 2^{\alpha-3}$. Similarly, each automaton that corresponds to an odd $\sum \delta(\chi_k)$ produces the residues $3 \cdot 2^{\alpha-3}, 7 \cdot 2^{\alpha-3}$.

It is then logical to generalize this characterization to $D(\alpha - i)$.

$$D(\alpha - i) = \begin{cases} (1 + 4j) \cdot 2^{\alpha-i} & \sum \delta(\chi_k) \text{ even,} \\ (3 + 4j) \cdot 2^{\alpha-i} & \sum \delta(\chi_k) \text{ odd} \end{cases}$$

which leads to the following conjecture:

Conjecture 6.6. For $D(\alpha - i)$ and $n = 1\chi_1 1 \ldots\ 1\chi_{\alpha-3}0$, if $\sum \delta(\chi_k)$ is even then there exists a $C(n) \equiv (1 + 4j)2^{\alpha-i} \bmod 2^\alpha$ for $j = 0, 1, \ldots, i - 2$. If $\sum \delta(\chi_k)$ is odd then $C(n) \equiv (3 + 4j)2^{\alpha-i} \bmod 2^\alpha$ for $j = 0, 1, \ldots, i - 2$.

This conjecture has been tested for $\alpha = 11, 12, 13$ using $n = 1, 2, \ldots, 500,000$. Conjecture 3.3 would follow from this result.

7 Summary

In this paper, we provide some insight into the nature of even residues of Catalan numbers $\bmod\, 2^\alpha$. In particular, we first prove initial results that explicitly characterize some of the absent or eventually absent residues. Together, each of these results regarding the eventually absent residues demonstrates that the number of present residues is bounded above by $\frac{35}{128}$. We then took a different approach to this problem and were able to characterize the Catalan numbers based on their 2-adic valuations. We were able to completely characterize present residues of the form $2 + 8j$. In addition, these characterizations based on 2-adic valuations provided some insight for a possible approach that describes present residues of the form $8j$. This led to a conjecture that has not yet been proven, but it does indicate the number of present residues is bounded below by $\frac{1}{8}$. Therefore, it seems the proportion of present residues falls between .125 and .27.

8 Future work

Conjecture 3.3, which would produce a lower bound of $\frac{1}{8}$, remains to be proven. The most promising path to attempt this proof may be to continue the work in Section 6. This would consist of characterizing the binary representations of elements of $D(\alpha - i)$ and proving that at least one n such that $C(n)$.

Additionally, the $4 \bmod 8$ and $6 \bmod 8$ nodes have yet to be characterized. This can likely be done by using the same methods we have shown; that is, extending the tree until we can classify each leaf as either constant (in the case of an eventually absent residue), linear (e.g. 18 mod 32), or exponential (e.g. 0 mod 8).

9 Acknowledgements

This work was carried out during the 2014 Mathematical Sciences Research Institute Undergraduate Program (MSRI-UP) which is funded by the National Science Foundation (grant No. DMS-1156499) and the National Security Agency (grant No. H-98230-13-1-0262). We would like to thank Dr. Victor Moll, Dr. Herbert Medina, Dr. Eric Rowland, and Leyda Almodóvar.

The first author would like to thank Dr. Victoria Klawitter from SUNY Potsdam for her exceptional encouragement and guidance throughout his academic career.

The second author would like to thank Dr. Ellen Veomett from Saint Mary's College of California for her continuous support and invaluable guidance throughout the last couple years.

The third author would like to thank Dr. David Scribner for fostering his curiosity about math and appetite for solving problems.

References

[1] Hsueh-Yung Lin. “Odd Catalan numbers modulo $2k$”. *Integers*, 12(2):161-165, 2012.

[2] Eric Rowland and Reem Yassawi. “Automatic congruences for diagonals of rational functions”. 2014. `http://arXiv:1310.8635v2`.

[3] Guoce Xin and Jing-Feng Xu. “A short approach to Catalan numbers modulo $2r$”. *The Electronic Journal of Combinatorics*, 18:P177, 2011.

Infinite products and periodic sequences

Hadrian Quan

University of California, Santa Cruz

Fernando Roman

Kansas State University

Michole Washington

Georgia Institute of Technology

August 2014

Abstract

The work discussed here develops methods to evaluate certain infinite products in closed-form. These are finite products of values of the gamma function. Presented here are infinite products of rational functions $R(n)$ raised to the power of some sequence M_n. The sequences satisfy certain regularity conditions as either a ℓ-periodic or k-automatic. Of particular interest is the regular paperfolding sequence considered by J. P. Allouche. Also included are some results on the p-adic valuation of partial products of these types, which also contain some patterns of interest.

1 Introduction

The evaluation of infinite sums and products is a topic of great interest in mathematics. Mathematical constants arising in these evaluations are sometimes unexpected and interesting. For example, the earliest evaluation of an infinite product was produced by J. Wallis in 1655

$$\prod_{n=1}^{\infty} \frac{(2n)(2n)}{(2n-1)(2n+1)} = \frac{\pi}{2}. \tag{1.1}$$

The history of this discovery appears in [9]. A variety of infinite product evaluations including

$$\prod_{n=1}^{\infty}\left(1+\frac{1}{F_{2^n+1}}\right)=\frac{3}{\varphi} \text{ and } \prod_{n=0}^{\infty}\left(1+\frac{1}{L_{2^n+1}}\right)=3-\varphi \tag{1.2}$$

were given by J. Sondow [10]. Here, F_n and L_n are the Fibonacci and Lucas numbers, respectively, defined by the recurrence $x_{n+1}=x_n+x_{n-1}$ with the initial conditions $x_0=1,\ x_1=1$ and $x_0=2,\ x_1=1$, respectively. The golden ratio $\varphi=\frac{1}{2}(\sqrt{5}+1)$ is the limit of F_{n+1}/F_n as $n\to\infty$.

The value of infinite products usually involves classical concepts of analysis. For instance P. Borwein [3] evaluates the function

$$D(x)=\lim_{n\to\infty}\prod_{k=1}^{2n+1}\left(1+\frac{x}{k}\right)^{(-1)^{k+1}k} \tag{1.3}$$

as a generalization of the values

$$\prod_{n=1}^{\infty}\left(1+\frac{2}{n}\right)^{(-1)^{n+1}n}=\frac{\pi}{2e}, \text{ and } \prod_{n=1}^{\infty}\left(1+\frac{2}{n}\right)^{(-1)^{n}n}=\frac{6}{\pi e} \tag{1.4}$$

established by Z.A. Melzak [6]. Some exact evaluations are given in terms of the constant

$$A_1=\exp\left\{\frac{1}{4}-\int_0^{\infty}\frac{e^{-s}}{s^3}\left[1-\frac{s}{2}+\frac{s^2}{12}-\frac{s}{e^s-1}\right]ds\right\} \tag{1.5}$$

and

$$G=\sum_{n=0}^{\infty}\frac{(-1)^n}{(2n+1)^2}. \tag{1.6}$$

For instance

$$D(1)=\frac{A_1^6}{2^{1/6}\sqrt{\pi}} \text{ and } D\left(\frac{1}{4}\right)=\frac{2^{1/6}\sqrt{\pi}A_1^3}{\Gamma(\frac{1}{4})}e^{G/\pi}. \tag{1.7}$$

The question considered here deals with the evaluation of products of the form

$$\prod_{n=0}^{\infty}R(n)^{s(n)}. \tag{1.8}$$

Here R is a rational function and s is a sequence with *regularity properties* (as stated by J.P. Allouche in [1]). Examples of such sequences include *periodic* and *automatic sequences* taking values in the alphabet $\{+1,-1\}$: a sequence $\{s_n : n\geq 0\}$ is k-automatic if the set of subsequences $\{s_{k^jn+l} : n\geq 0\}$ with $j\geq 0, l\in[0,k^j-1]$ is finite. More information about automatic sequences appears in [2].

The arithmetic properties of these products are analyzed in their p-adic valuations. The p-adic number field has been leveraged heavily to further our understanding of the rational numbers. The p-adic valuation of a number is denoted by $\nu_p(n)$ for a fixed prime p and is equal to the exponent of the highest power of p that divides n.

2 Convergence criterion for infinite products

An infinite sum is said to be convergent if the limit of its partial sums exists and is finite; it is said to be divergent if its partial sums are unbounded. In the case of infinite products there are two different types of divergence. If the limit of the partial products exists and is finite, the product is said to converge; if it grows unbounded, the product is said to be divergent; also, if the product is identically zero it is said to diverge to zero rather that converge to zero. This reasoning become clear in lemma 2.1. A strong result about the convergence (or divergence) of infinite products of rational functions is provided in this section. This result implies that if an infinite product converges then it can be evaluated in terms of the gamma function.

First, a well known result, that provides a criterion for divergence of infinite products, is introduced:

Lemma 2.1. *Let* $u : \mathbb{R} \longrightarrow \mathbb{R}$. *If* $\displaystyle\prod_{n=1}^{\infty} u(n)$ *converges then* $\displaystyle\lim_{n \longrightarrow \infty} u(n) = 1$.

Proof. Assume that the product $\displaystyle\prod_{n=1}^{\infty} u(n)$ converges to some real number L, then the quantity $\log L = \log \displaystyle\prod_{n=1}^{\infty} u(n) = \sum_{n=1}^{\infty} \log u(n)$ is finite and well defined; that is to say, the sum $\sum\limits_{n=1}^{\infty} \log u(n)$ converges. Since $\sum\limits_{n=1}^{\infty} \log u(n)$ converges we know that $\lim_{n\rightarrow\infty} \log u(n) = 0$ but since log is an injective function we conclude that $\displaystyle\lim_{n\rightarrow\infty} u(n) = 1$. □

If an infinite product goes to zero, taking its logarithm makes it a divergent infinite sum and thus the terminology "diverging to zero".

Next, the proof of a classical result due to Weierstrass is provided. This result will be constantly used to evaluate infinite products, for the classical formulation refer to [11]:

Lemma 2.2. *Let $u : \mathbb{R} \longrightarrow \mathbb{R}$ be a rational function. If*

$$u(n) = \frac{(n+a_1)(n+a_2)\cdots(n+a_d)}{(n+b_1)(n+b_2)\ldots(n+b_d)} \text{ where } a_j, b_i \notin \{0,-1,-2,-3\ldots\}$$

and

$$\sum_{j=1}^{d} a_j = \sum_{j=1}^{d} b_j$$

then

$$\prod_{n=0}^{\infty} u(n) = \prod_{j=1}^{d} \frac{\Gamma(b_j)}{\Gamma(a_j)}.$$

Proof. To prove this equality first recall Euler's definition of the gamma function

$$\Gamma(z) = \lim_{k\to\infty} \frac{(k+1)^z k!}{z(z+1)\cdots(z+k)} \tag{2.1}$$

then we have

$$\frac{\Gamma(b_1)\cdots\Gamma(b_d)}{\Gamma(a_1)\cdots\Gamma(a_d)} = \lim_{k\to\infty} \prod_{j=1}^{d} k^{b_j-a_j} \prod_{n=0}^{k} \frac{n+a_j}{n+b_j} = \lim_{r\to\infty} \prod_{n=0}^{r} \frac{(n+a_1)\cdots(n+a_d)}{(n+b_1)\cdots(n+b_d)} \tag{2.2}$$

where the last equality comes from the fact that since $a_1 + \cdots + a_d - b_1 - \cdots - b_d = 0$, then the products of $k^{b_j-a_j}$ for $1 \le j \le d$ equals $k^0 = 1$. □

This condition on the sum of the roots and poles seems very restrictive, however if an infinite product of rational functions cannot be evaluated in this way then it diverges:

Theorem 2.1. *Let $u : \mathbb{R} \longrightarrow \mathbb{R}$ be a rational function with no roots or poles in the nonnegative integers and such that $\lim_{n\to\infty} u(n) = 1$. Then $\prod_{n=1}^{\infty} u(n)$ converges if, and only if,*

$$u(n) = \frac{(n+a_1)(n+a_2)\cdots(n+a_d)}{(n+b_1)(n+b_2)\cdots(n+b_d)} \text{ where } \sum_{j=1}^{d} a_j = \sum_{j=1}^{d} b_j. \tag{2.3}$$

Proof. First note that if $u(n) = \frac{(n+a_1)(n+a_2)\cdots(n+a_d)}{(n+b_1)(n+b_2)\cdots(n+b_d)}$, where $\sum_{j=1}^{d} a_j = \sum_{j=1}^{d} b_j$, lemma 2.2 not only asserts that $\prod_{n=1}^{\infty} u(n)$ converges, but it also provides a method of evaluating it in terms of the gamma function.

Hence, the converse (convergence of $\prod_{n=1}^{\infty} u(n)$ implies (2.3)) is proven as follows: Assume that the product does not diverge. If this product converges to some finite value, then by lemma 2.1, $u(n) \to 1$ as $n \to \infty$. Hence, if $u(n)$ is some rational function, it is necessarily of the form $u(n) = \dfrac{P(n)}{Q(n)}$ where $\deg(P) = \deg(Q)$, and the leading coefficients of P and Q are equal. As these polynomials have finite degree, they may be written as products of linear factors over $\mathbb{C}$, i.e.

$$u(n) = \frac{P(n)}{Q(n)} = \frac{(n+a_1)\cdots(n+a_d)}{(n+b_1)\cdots(n+b_d)}$$

for some $a_1, \cdots, a_d, b_1, \cdots, b_d \in \mathbb{C}$. This yields

$$\begin{aligned} u(n) &= \left(1+\frac{a_1}{n}\right)\cdots\left(1+\frac{a_d}{n}\right)\left(1+\frac{b_1}{n}\right)^{-1}\cdots\left(1+\frac{b_d}{n}\right)^{-1} \\ &= 1 + \frac{a_1+\cdots+a_d-b_1-\cdots-b_d}{n} + O\left(\frac{1}{n^2}\right) \\ \implies \prod_{n=1}^{\infty} u(n) &= \prod_{n=1}^{\infty}\left(1+\frac{a_1+\cdots+a_d-b_1-\cdots-b_d}{n}+O\left(\frac{1}{n^2}\right)\right) \end{aligned}$$

and since the harmonic series $\sum_{n=1}^{\infty}\frac{1}{n}$, appearing when the product is expanded diverges, the linear term must equal zero for the product to converge, hence $a_1+\cdots+a_d-b_1-\cdots-b_d = 0$. □

With this criterion one can evaluate infinite products of rational functions. Moreover, given a periodic sequence M_n with elements in $\{1, -1\}$, one can characterize rational functions $R(n)$ for which $\prod_{n=1}^{\infty} R(n)^{M_n}$ converges. Note that for a sequence $M_n \in \{+1,\ -1\}$ and any constant $c \neq 1$, $\lim_{n\to\infty} c^{M_n} \neq 1$. Therefore $\prod_{n}^{\infty} c^{M_n}$ is not defined. Hence throughout this paper it is assumed, unless otherwise indicated, that every rational function has leading coefficient 1; that is, $R(n) = \dfrac{(n+a_1)\cdots(n+a_d)}{(n+b_1)\cdots(n+b_r)}$.

3 Sequences of period 2

To motivate the general results, begin by letting R be a rational function, $M_n = (-1)^n$ and considering $\prod_{n=1}^{\infty} R(n)^{M_n}$. What conditions on R are sufficient and necessary for the convergence of this product? The characterization of all such functions is given in the following

Theorem 3.1. *Let R be a rational function with no roots or poles on the positive integers, then $\prod\limits_{n=0}^{\infty} R(n)^{(-1)^n}$ converges if, and only if $\lim\limits_{n\to\infty} R(n) = 1$.*

Proof. First note the restriction that none of the roots and poles of R are positive integers integers rules out the possibility of products being identically zero or blowing up for some finite index. As for the claim, this can be proven by considering the partial products of $R(n)^{M_n}$:

$$\prod_{n=0}^{N} R(n)^{(-1)^n} = \prod_{n=0}^{\lfloor \frac{N}{2} \rfloor} R(2n) \prod_{n=0}^{\lfloor \frac{N}{2} \rfloor} \frac{1}{R(2n+1)} = \prod_{n=0}^{\lfloor \frac{N}{2} \rfloor} \frac{R(2n)}{R(2n+1)}.$$

Taking limits of both sides as $N \to \infty$ gives us equality of the products $\prod\limits_{n=0}^{\infty} R(n)^{(-1)^n}$ and $\prod_{n=0}^{\infty} \frac{R(2n)}{R(2n+1)}$. By theorem 2.1, the infinite product on the right-hand side converges if, and only if,

$$\frac{R(2n)}{R(2n+1)} = \frac{(n+\alpha_1)(n+\alpha_2)\cdots(n+\alpha_m)}{(n+\beta_1)(n+\beta_2)\cdots(n+\beta_m)} \text{ satisfies } \sum_{j=1}^{m} \alpha_j = \sum_{j=1}^{m} \beta_j.$$

Now R has the form $R(n) = \dfrac{(n+a_1)(n+a_2)\cdots(n+a_d)}{(n+b_1)(n+b_2)\cdots(n+b_r)}$, so that

$$\frac{R(2n)}{R(2n+1)} = \frac{(2n+a_1)(2n+a_2)\cdots(2n+a_d)}{(2n+b_1)(2n+b_2)\cdots(2n+b_r)} \frac{(2n+1+b_1)(2n+1+b_2)\cdots(2n+1+b_r)}{(2n+1+a_1)(2n+1+a_2)\cdots(2n+1+a_d)}.$$

So, $\prod\limits_{n=0}^{\infty} \frac{R(2n)}{R(2n+1)}$ converges if, and only if,

$$\frac{1}{2}\sum_{i=1}^{d} a_i + \frac{1}{2}\sum_{j=1}^{r}(1+b_j) = \frac{1}{2}\sum_{j=1}^{r} b_j + \frac{1}{2}\sum_{i=1}^{d}(1+a_i) \iff \sum_{j=1}^{r} 1 = \sum_{i=1}^{d} 1.$$

This is true if, and only if, $d = r$, but since

$$R(n) = \frac{(n+a_1)(n+a_2)\cdots(n+a_d)}{(n+b_1)(n+b_2)\cdots(n+b_r)}$$

it can be concluded that $d = r$ if, and only if, $R(n) \to 1$ as $n \to \infty$.

□

In what follows, a closed-form formula for the evaluation of these products, is derived. First recall that

$$\prod_{n=0}^{\infty} R(n)^{(-1)^n} = \prod_{n=0}^{\infty} \frac{R(2n)}{R(2n+1)}.$$

Therefore the evaluation of this product is given by

$$\prod_{n=0}^{\infty} R(n)^{(-1)^n} = \prod_{i=1}^{d} \frac{\Gamma\left(\frac{b_i}{2}\right)\Gamma\left(\frac{1+a_i}{2}\right)}{\Gamma\left(\frac{1+b_i}{2}\right)\Gamma\left(\frac{a_i}{2}\right)}, \tag{3.1}$$

where d is the degree of both the numerator and denominator of R. To simplify this expression, use the duplication formula for the gamma function to obtain

$$\Gamma\left(\frac{a_i+1}{2}\right) = \frac{\sqrt{\pi}\Gamma(a_i)}{2^{a_i-1}\Gamma\left(\frac{a_i}{2}\right)} \tag{3.2}$$

that yields

$$\frac{\Gamma\left(\frac{a_i}{2}\right)}{\Gamma\left(\frac{a_i+1}{2}\right)} = \frac{2^{a_i-1}\Gamma^2\left(\dfrac{a_i}{2}\right)}{\sqrt{\pi}\Gamma(a_i)}. \tag{3.3}$$

Hence,

$$\frac{\Gamma\left(\frac{b_i}{2}\right)\Gamma\left(\frac{1+a_i}{2}\right)}{\Gamma\left(\frac{1+b_i}{2}\right)\Gamma\left(\frac{a_i}{2}\right)} = 2^{(b_i-a_i)}\frac{\Gamma^2\left(\frac{b_i}{2}\right)\Gamma(a_i)}{\Gamma^2\left(\frac{a_i}{2}\right)\Gamma(b_i)}. \tag{3.4}$$

Therefore,

$$\prod_{i=1}^{d}\frac{\Gamma\left(\frac{b_i}{2}\right)\Gamma\left(\frac{1+a_i}{2}\right)}{\Gamma\left(\frac{1+b_i}{2}\right)\Gamma\left(\frac{a_i}{2}\right)} = 2^{S(a,b)}\prod_{i=1}^{d}\frac{\Gamma^2(b_i/2)\Gamma(a_i)}{\Gamma^2(a_i/2)\Gamma(b_i)}, \tag{3.5}$$

where $S(a,b) = \sum_{i=1}^{d}(b_i - a_i)$.

Note that there is a total of $2^2 = 4$ different 2-periodic sequences in the symbols -1 and 1. Two of them are trivial, one was discussed above, and the last one is $-(-1)^n = (-1)^{n+1}$. Hence the previous results generalizes to this sequence by just considering reciprocals.

Example 3.1. The product $\prod_{n=1}^{\infty}\left(\frac{n}{n+1}\right)^{(-1)^n}$ can be evaluated noting that $R(n) = \frac{n}{n+1} \to 1$ as $n \to \infty$.

Apply the result to get

$$\prod_{n=1}^{\infty}\left(\frac{n}{n+1}\right)^{(-1)^n} = \prod_{n=0}^{\infty}\left(\frac{n+1}{n+2}\right)^{(-1)^{n+1}} = \left[\prod_{n=0}^{\infty}\left(\frac{n+1}{n+2}\right)^{(-1)^n}\right]^{-1} = \left[2\frac{\Gamma^2(1)\Gamma(1)}{\Gamma^2(1/2)\Gamma(2)}\right]^{(-1)} = \frac{\pi}{2}$$

where the second to last equality follows from lemma 2.2, and the last one follows from properties of the gamma function.

4 Sequences of period 3

Attention is now turned to a sequence of period 3. Define the sequence l_n as

$$l_n = \begin{cases} 1 & \text{if } n \equiv 0 \bmod 3; \\ -1 & \text{otherwise.} \end{cases}$$

Next consider products of the form $\displaystyle\prod_{n=1}^{\infty} R(n)^{l_n}$.

Theorem 4.1. *Let l_n denote the above described sequence, and*

$$R(n) = \frac{(n+a_1)\cdots(n+a_d)}{(n+b_1)\cdots(n+b_r)}$$

be a rational function with no roots or poles in the positive integers. Then $\displaystyle\prod_{n=1}^{\infty} R(n)^{l_n}$ converges if, and only if,

(i) $\lim_{n\to\infty} R(n) = 1$

(ii) $\sum_{i=1}^{d} a_i = \sum_{j=1}^{r} b_j$.

Note that condition (i) implies that $r = d$. These conditions combined imply that no quotient of monomials (excluding trivial case $p(n)/p(n)$) yields convergence of the product in question.

Proof. Taking the same approach as before:

$$\prod_{n=1}^{N} R(n)^{l_n} = \prod_{n=1}^{\lfloor \frac{N}{3} \rfloor} R(3n) \prod_{n=0}^{\lfloor \frac{N}{3} \rfloor} \frac{1}{R(3n+1)} \prod_{n=0}^{\lfloor \frac{N}{3} \rfloor} \frac{1}{R(3n+2)} = \frac{1}{R(1)R(2)} \prod_{n=1}^{\lfloor \frac{N}{3} \rfloor} \frac{R(3n)}{R(3n+1)R(3n+2)}.$$

By taking limit of both sides as $N \to \infty$ we get the equality of the products $\displaystyle\prod_{n=1}^{\infty} R(n)^{l_n}$ and $\displaystyle\frac{1}{R(1)R(2)} \prod_{n=1}^{\infty} \frac{R(2n)}{R(3n+1)R(3n+2)}$, so that the convergence of one is equivalent to the convergence of the other.

Once again, since R is a rational function with leading coefficient 1, one can factor both the numerator and denominator to write it in the form

$$R(n) = \frac{(n+a_1)(n+a_2)\cdots(n+a_d)}{(n+b_1)(n+b_2)\cdots(n+b_r)},$$

so that

$$\frac{R(3n)}{R(3n+1)R(3n+2)}$$
$$= \frac{(3n+a_1)\cdots(3n+a_d)}{(3n+b_1)\cdots(3n+b_r)}\frac{(3n+1+b_1)\cdots(3n+1+b_r)}{(3n+1+a_1)\cdots(3n+1+a_d)}\frac{(3n+2+b_1)\cdots(3n+2+b_r)}{(3n+2+a_1)\cdots(3n+2+a_d)}.$$

By lemma 2.1 it is needed $\lim_{n\to\infty}\frac{R(3n)}{R(3n+1)R(3n+2)} = 1$, therefore it must be that $2d+r = 2r+d \iff d=r$; this gives us condition (i). Now, by theorem 2.1 it is also needed that

$$\frac{1}{3}\sum_{i=1}^{d} a_i + \frac{1}{3}\sum_{j=1}^{r}(1+b_j) + \frac{1}{3}\sum_{j=1}^{r}(2+b_j) = \frac{1}{3}\sum_{i=1}^{d}(1+a_i) + \frac{1}{3}\sum_{i=1}^{d}(2+a_i) + \frac{1}{3}\sum_{j=1}^{r} b_j$$

$$\iff \sum_{j=1}^{r} b_j + 3r = \sum_{i=1}^{d} a_i + 3d,$$

but since $d=r$ this equality holds if, and only if, $\sum_{j=1}^{r} b_j = \sum_{i=1}^{d} a_i$ which explicitly gives us condition (ii). It is clear from this argument that if conditions (i) and (ii) are satisfied then $\prod_{n=1}^{\infty} R(n)^{l_n}$ converges. This completes the proof. □

The product $\prod_{n=0}^{\infty} R(n)^{l_n}$ reduces to evaluating

$$\prod_{n=0}^{\infty}\frac{R(3n)}{R(3n+1)R(3n+2)} = \prod_{n=0}^{\infty}\prod_{i=0}^{d}\frac{\left(n+\frac{a_i}{3}\right)\left(n+\frac{b_i+1}{3}\right)\left(n+\frac{b_i+2}{3}\right)}{\left(n+\frac{b_i}{3}\right)\left(n+\frac{b_i+1}{3}\right)\left(n+\frac{b_i+2}{3}\right)}.$$

The value of this product is given in terms of the gamma function as

$$\prod_{i=1}^{d}\frac{\Gamma\left(\frac{b_i}{3}\right)\Gamma\left(\frac{a_i+1}{3}\right)\Gamma\left(\frac{a_i+2}{3}\right)}{\Gamma\left(\frac{a_i}{3}\right)\Gamma\left(\frac{b_i+1}{3}\right)\Gamma\left(\frac{b_i+2}{3}\right)} \tag{4.1}$$

where d is the degree of the numerator (and denominator) of R. This expression can be simplified using the triplication formula for the gamma function to obtain:

$$\Gamma\left(\frac{a_i+1}{3}\right)\Gamma\left(\frac{a_i+2}{3}\right) = \frac{2\pi\Gamma(a_i)}{3^{a_i-\frac{1}{2}}\Gamma\left(\frac{a_i}{3}\right)}, \tag{4.2}$$

which yields

$$\frac{\Gamma\left(\frac{a_i+1}{3}\right)\Gamma\left(\frac{a_i+2}{3}\right)}{\Gamma\left(\frac{a_i}{3}\right)}=\frac{2\pi\Gamma(a_i)}{3^{a_i-\frac{1}{2}}\Gamma^2\left(\frac{a_i}{3}\right)}. \tag{4.3}$$

Therefore

$$\frac{\Gamma\left(\frac{b_i}{3}\right)\Gamma\left(\frac{a_i+1}{3}\right)\Gamma\left(\frac{a_i+2}{3}\right)}{\Gamma\left(\frac{a_i}{3}\right)\Gamma\left(\frac{b_i+1}{3}\right)\Gamma\left(\frac{b_i+2}{3}\right)}=3^{b_i-a_i}\frac{\Gamma^2\left(\frac{b_i}{3}\right)\Gamma(a_i)}{\Gamma^2\left(\frac{a_i}{3}\right)\Gamma(b_i)}, \tag{4.4}$$

so that

$$\prod_{i=1}^{d}\frac{\Gamma\left(\frac{b_i}{3}\right)\Gamma\left(\frac{a_i+1}{3}\right)\Gamma\left(\frac{a_i+2}{3}\right)}{\Gamma\left(\frac{a_i}{3}\right)\Gamma\left(\frac{b_i+1}{3}\right)\Gamma\left(\frac{b_i+2}{3}\right)}=3^{S(a,b)}\prod_{i=1}^{d}\frac{\Gamma^2\left(\frac{b_i}{3}\right)\Gamma(a_i)}{\Gamma^2\left(\frac{a_i}{3}\right)\Gamma(b_i)}. \tag{4.5}$$

Here $S(a,b)=\sum_{i=1}^{d}(b_i-a_i)$ but condition (ii) on theorem 4.1 forces $S(a,b)=0$. Hence the closed-form formula

$$\prod_{n=0}^{\infty}R(n)^{l_n}=\prod_{i=1}^{d}\frac{\Gamma^2\left(\frac{b_i}{3}\right)\Gamma(a_i)}{\Gamma^2\left(\frac{a_i}{3}\right)\Gamma(b_i)} \tag{4.6}$$

is obtained. Once again, note that there are $2^3=8$ distinct periodic sequences of period 3 in the symbols -1 and 1, however 2 of them are trivial and of the remaining six, three are the negatives of the other three; for example $\overline{\{-1,1,1\}}=-l_n$. Thus, in other to make a general statement on 3-periodic sequences it is only necessary to consider the sequences $l_n,\ s_n=\overline{\{-1,1,-1\}},\ t_n=\overline{\{-1,-1,1\}}$. The problem of characterizing rational functions R for which $\prod\limits_{n=0}^{\infty}R(n)^{l_n}$ was completely solved, so attention is turned to the same question for the sequences s_n and t_n. Characterization of rational functions yielding converging infinite products when raised to these sequences is the same as the characterization of rational functions for the sequence l_n. This can be seen using the same argument as before, after noting that

$$\prod_{n=0}^{\infty}R(n)^{s_n}=\prod_{n=0}^{\infty}\frac{R(3n+1)}{R(3n)R(3n+2)}$$

and

$$\prod_{n=0}^{\infty}R(n)^{t_n}=\prod_{n=0}^{\infty}\frac{R(3n+2)}{R(3n)R(3n+1)}.$$

Applying the same method yields the respective closed-form formulas

$$\prod_{n=0}^{\infty}R(n)^{s_n}=\prod_{t=1}^{d}\frac{\Gamma(a_t)\Gamma^2(\frac{1+b_t}{3})}{\Gamma(b_t)\Gamma^2(\frac{1+a_t}{3})} \tag{4.7}$$

and

$$\prod_{n=0}^{\infty} R(n)^{t_n} = \prod_{t=1}^{d} \frac{\Gamma(a_t)\Gamma^2(\frac{2+b_t}{3})}{\Gamma(b_t)\Gamma^2(\frac{2+a_t}{3})}. \tag{4.8}$$

Thus, theorem 4.1 actually gives a characterization of all rational functions for which $\prod_{n=0}^{\infty} R(n)^{M_n}$ converges, where M_n is any 3-periodic sequence in $\{1, -1\}$.

Example 4.1. Let l_n be as above and put $R(n) = \frac{3+4n+n^2}{4+4n+n^2} = \frac{(n+1)(n+3)}{(n+2)^2}$. None of the roots or poles of R are positive integers, and the conditions of theorem 4.1 are satisfied, hence:

$$\prod_{n=0}^{\infty} \left(\frac{(n+1)(n+3)}{(n+2)^2}\right)^{l_n} = \frac{\Gamma^4(2/3)\Gamma(3)\Gamma(1)}{\Gamma^2(1/3)\Gamma^2(1)\Gamma^2(2)} = \frac{32\pi^4}{9\Gamma^6(1/3)}.$$

This section closes with the following remark. Note that in the proofs of theorems 3.1 and 4.1, issues of convergence were addressed by considering partial products and then taking limits. In general, this argument applies to all proofs of this type. Therefore, in the rest of this paper, the splitting of infinite products is done without addressing issues of convergence; however, the reader should keep in mind the argument on the partial products used previously.

5 Sequences of period 4, a hint to the general case

Sufficient and necessary conditions for convergence of infinite products have been established for sequences of period 2 and 3. These conditions seem to impose some restriction on the rational functions for which the infinite product can be evaluated. However, this pattern does not entirely persist.

Consider the 4-periodic sequence $\overline{\{1, -1, -1, 1\}}$ given by

$$M_n = \begin{cases} 1 & \text{if } n \equiv 0 \text{ or } 3 \bmod 4; \\ -1 & \text{if } n \equiv 1 \text{ or } 2 \bmod 4. \end{cases}$$

Once again, let $R(n) = \dfrac{(n+a_1)\cdots(n+a_d)}{(n+b_1)\cdots(n+b_r)}$ with $a_i, b_j \notin -\mathbb{N}$ and consider the product $\prod_{n=0}^{\infty} R(n)^{M_n}$.

$$\prod_{n=0}^{\infty} R(n)^{M_n} = \prod_{n=0}^{\infty} \frac{R(4n)R(4n+3)}{R(4n+2)R(4n+3)}$$
$$= \prod_{n=0}^{\infty} \prod_{\substack{1\le i\le d\\ 1\le j\le r}} \frac{(4n+a_i)(4n+3+a_i)(4n+1+b_j)(4n+2+b_j)}{(4n+b_j)(4n+3+b_j)(4n+1+a_i)(4n+2+a_i)}.$$

Hence it is known that $\displaystyle\prod_{n=0}^{\infty} R(n)^{M_n}$ converges if, and only if $\displaystyle\lim_{n\to\infty} \frac{R(4n)R(4n+3)}{R(4n+1)R(4n+2)} = 1$ and

$$\sum_{i=1}^{d} a_i + \sum_{i=1}^{d}(a_i+3) + \sum_{j=1}^{r}(b_j+1) + \sum_{j=1}^{r}(b_j+2) = \sum_{j=1}^{r} b_j + \sum_{j=1}^{r}(b_j+3) + \sum_{i=1}^{d}(a_i+1) + \sum_{i=1}^{d}(a_i+2).$$

The first condition is clearly satisfied and the second condition simplifies yielding

$$2\sum_{i=1}^{d} a_i + 2\sum_{j=1}^{r} b_j + 3d + 3r = 2\sum_{j=1}^{r} b_j + 2\sum_{i=1}^{d} a_i + 3r + 3d.$$

The latter is always true; that is to say $\displaystyle\prod_{n=0}^{\infty} R(n)^{M_n}$ converges for every such rational function.

However, considering the sequence

$$M_n = \begin{cases} 1 & \text{if } n \equiv 0 \text{ or } 1 \bmod 4; \\ -1 & \text{if } n \equiv 2 \text{ or } 3 \bmod 4, \end{cases}$$

it is obtained that

$$\prod_{n=0}^{\infty} R(n)^{M_n} = \prod_{n=0}^{\infty} \frac{R(4n)R(4n+1)}{R(4n+2)R(4n+3)}$$
$$= \prod_{n=0}^{\infty} \prod_{\substack{1\le i\le d\\ 1\le j\le r}} \frac{(4n+a_i)(4n+1+a_i)(4n+2+b_j)(4n+3+b_j)}{(4n+b_j)(4n+1+b_j)(4n+2+a_i)(4n+3+a_i)}.$$

This converges if, and only if $\displaystyle\lim_{n\to\infty} \frac{R(4n)R(4n+1)}{R(4n+2)R(4n+3)} = 1$ and

$$\sum_{i=1}^{d} a_i + \sum_{i=1}^{d}(a_i+1) + \sum_{j=1}^{r}(b_j+2) + \sum_{j=1}^{r}(b_j+3) = \sum_{j=1}^{r} b_j + \sum_{j=1}^{r}(b_j+1) + \sum_{i=1}^{d}(a_i+2) + \sum_{i=1}^{d}(a_i+3).$$

Once again the first condition is clearly satisfied and the second one simplifies:

$$2\sum_{i=1}^{d} a_i + 2\sum_{j=1}^{r} b_j + d + 5r = 2\sum_{j=1}^{r} b_j + 2\sum_{i=1}^{d} a_i + r + 5d \iff r = d.$$

So that $\prod_{n=0}^{\infty} R(n)^{M_n}$ converges if, and only if $\lim_{n\to\infty} R(n) = 1$.

In the following section these results are generalized and proven for any periodic sequence.

6 Periodic sequences, the general case

In this section, a characterization of rational functions R for which $\prod_{n=0}^{\infty} R(n)^{M_n}$ converges, where M_n is a periodic sequence of period ℓ for some $\ell \in \mathbb{N}$, is established.

Theorem 6.1. *Let* $R(n) = \dfrac{(n+a_1)\cdots(n+a_d)}{(n+b_1)\cdots(n+b_r)}$ *be a rational function with* $a_s,\ b_t \notin -\mathbb{N}$ *for* $1 \le s \le d$, $1 \le t \le r$, *and let* M_n *be a periodic sequence of period* ℓ *in* $\{1, -1\}$. *Define* $M^+ = \{\ i\ :\ M_i = 1 \text{ and } 0 \le i \le \ell - 1\}$ *and* $M^- = \{\ j\ :\ M_j = -1 \text{ and } 0 \le j \le \ell - 1\}$.

Case 1: If $|M^+| \neq |M^-|$, *then* $\prod_{n=0}^{\infty} R(n)^{M_n}$ *converges if, and only if*

(i) $\lim_{n\to\infty} R(n) = 1$

(ii) $\sum_{m=1}^{d} a_m = \sum_{m=1}^{r} b_m$.

Case 2: If $|M^+| = |M^-|$ *but* $\sum_{i\in M^+} i \neq \sum_{j\in M^-} j$, *then* $\prod_{n=0}^{\infty} R(n)^{M_n}$ *converges if, and only if* $\lim_{n\to\infty} R(n) = 1$.

Case 3: $|M^+| = |M^-|$, *and* $\sum_{i\in M^+} i = \sum_{j\in M^-} j$, *then* $\prod_{n=0}^{\infty} R(n)^{M_n}$ *converges for every such rational function* R.

Note that if ℓ is odd then Case 1 always applies and Case 3 is only attainable when $\ell = 4r$ for some $r \in \mathbb{N}$.

Proof.

Assume $|M^+| \neq |M^-|$, and let $R_1(n) = \dfrac{R(\ell n + j_1)\cdots R(\ell n + j_{|M^+|})}{R(\ell n + i_1)\cdots R(\ell n + i_{|M^-|})}$ such that

$$\prod_{n=0}^{\infty} R(n)^{M_n} = \prod_{n=0}^{\infty} R_1(n),$$

where $j_s, i_t \in \{0, 1, \cdots \ell - 1\}$. Without lost of generality assume $|M^-| < |M^+|$, then

$$R_1(n) = \frac{R(\ell n + j_1)\cdots R(\ell n + j_{|M^-|})\cdots R(\ell n + j_{M^+})}{R(\ell n + i_1)\cdots R(\ell n + i_{|M^-|})}.$$

By Lemma 2.1, it is necessary to have $\lim\limits_{n\to\infty} R_1(n) = 1$ but since

$$\lim_{n\to\infty} \frac{R(\ell n + j_1)\cdots R(\ell n + j_{|M^-|})}{R(\ell n + i_1)\cdots R(\ell n + i_{|M^-|})} = 1 \text{ for any rational function } \ R,$$

it is needed that

$$\lim_{n\to\infty} R(\ell n + j_{|M^-|+1})\cdots R(\ell n + j_{|M^+|}) = 1,$$

but this true if, and only if, $\lim\limits_{n\to\infty} R(n) = 1$ which gives condition (i) on Case 1. Note that this also implies that $d = r$. Now, the evaluation of this product reduces to

$$\prod_{n=0}^{\infty} R(n)^{M_n} = \prod_{n=0}^{\infty}\prod_{t=1}^{d} \frac{(\ell n + j_1 + a_t)\cdots(\ell n + j_{|M^+|} + a_t)(\ell n + i_1 + b_t)\cdots(\ell n + i_{|M^-|} + b_t)}{(\ell n + j_1 + b_t)\cdots(\ell n + j_{|M^+|} + b_t)(\ell n + i_1 + a_t)\cdots(\ell n + i_{|M^-|} + a_t)},$$

which, by Theorem 2.1, we know converges if, and only if

$$\sum_{s=1}^{l}\sum_{t=1}^{d}(a_t + j_s) + \sum_{s=1}^{m}\sum_{t=1}^{d}(b_t + i_s) = \sum_{s=1}^{l}\sum_{t=1}^{d}(b_t + j_s) + \sum_{s=1}^{m}\sum_{t=1}^{d}(a_t + i_s)$$

which simplifies to

$$|M^+|\sum_{t=1}^{d} a_t + |M^-|\sum_{t=1}^{d} b_t + d\sum_{s=1}^{|M^+|} j_s + d\sum_{s=1}^{|M^-|} i_s = |M^+|\sum_{t=1}^{d} b_t + |M^-|\sum_{t=1}^{d} a_t + d\sum_{s=1}^{|M^-|} i_s + d\sum_{s=1}^{|M^+|} j_s$$

$$\iff (|M^+| - |M^-|)\sum_{t=1}^{d} a_t = (|M^+| - |M^-|)\sum_{t=1}^{d} b_t \iff \sum_{t=1}^{d} a_t = \sum_{t=1}^{d} b_t,$$

which is precisely condition (ii) on Case 1. This completes the proof of the first case.

Next, if it is assumed that $|M^+| = |M^-| = m$, then $R_1(n) = \dfrac{R(\ell n + j_1)\cdots R(\ell n + j_m)}{R(\ell n + i_1)\cdots R(\ell n + i_m)}$ so that $\lim_{n\to\infty} R_1(n) = 1$ for any rational function R.

Now, the evaluation of this product also reduces to

$$\prod_{n=0}^{\infty} R(n)^{M_n} = \prod_{n=0}^{\infty}\prod_{\substack{1\le t\le d\\ 1\le s\le r}} \frac{(\ell n + j_1 + a_t)\cdots(\ell n + j_m + a_t)(\ell n + i_1 + b_s)\cdots(\ell n + i_m + b_s)}{(\ell n + j_1 + b_s)\cdots(\ell n + j_m + b_s)(kn + i_1 + a_t)\cdots(kn + i_m + a_t)},$$

which converges if, and only if

$$\sum_{k=1}^{m}\sum_{t=1}^{d}(a_t+j_k)+\sum_{k=1}^{m}\sum_{s=1}^{r}(b_s+i_k)=\sum_{k=1}^{m}\sum_{s=1}^{r}(b_s+j_k)+\sum_{k=1}^{m}\sum_{t=1}^{d}(a_t+i_k),$$

which simplifies to

$$m\sum_{t=1}^{d}a_t+m\sum_{s=1}^{r}b_s+d\sum_{k=1}^{m}j_k+r\sum_{k=1}^{m}i_k=m\sum_{s=1}^{r}b_s+m\sum_{t=1}^{d}a_t+r\sum_{k=1}^{m}j_k+d\sum_{k=1}^{m}i_k$$

$$\iff (d-r)\sum_{k=1}^{l}j_k=(d-r)\sum_{k=1}^{l}i_k. \tag{6.1}$$

Note that $\sum_{k=1}^{l}j_k=\sum_{j\in M^+}j$ and $\sum_{k=1}^{l}i_k=\sum_{i\in M^-}i$, so that if $\sum_{j\in M^+}j\neq\sum_{i\in M^-}i$ then (6.1) is true if, and only if $d=r$ which is true if, and only if, $\lim_{n\to\infty}R(n)=1$. This proves case 2.
On the other hand, if $\sum_{j\in M^+}j=\sum_{i\in M^-}i$, then (6.1) is always true. This proves case 3 and completes the proof. □

In the interest of completeness, a closed-form evaluation for these products is provided in the following

Theorem 6.2. *Let* $R(n)=\dfrac{(n+a_1)\cdots(n+a_d)}{(n+b_1)\cdots(n+b_r)}$ *be such that* $a_s,b_t\notin-\mathbb{N}$*,* M_n *a* ℓ*-periodic sequence,* $M^+=\{j|M_j=1,\ \ 0\le j\le\ell-1\}$*,* $S(a,b)=\sum_{t=1}^{l}b_t-\sum_{s=1}^{d}a_s$*, and assume* $\prod_{n=0}^{\infty}R(n)^{M_n}$ *converges; then*

$$\prod_{n=0}^{\infty}R(n)^{M_n}=\ell^{S(a,b)}(2\pi)^{(\frac{d-r}{2})(\ell-1)}\prod_{\substack{1\le s\le d\\1\le t\le r}}\frac{\Gamma(a_s)}{\Gamma(b_t)}\prod_{j\in M^+}\frac{\Gamma^2\left(\frac{b_t+j}{\ell}\right)}{\Gamma^2\left(\frac{a_s+j}{\ell}\right)}. \tag{6.2}$$

Proof. Splitting the product by its residues modulo k we can rewrite the product first as

$$\prod_{n=0}^{\infty}R(n)^{M_n}=\prod_{n=0}^{\infty}\prod_{\substack{i\in M^+\\j\in M^-}}\frac{R(\ell n+j)}{R(\ell n+l)}$$

by noting that the terms with residues in M^- are being raised to the power of negative one, and become inverted. Using lemma 2.2, we can re-express this infinite product as a product of values of the gamma function.

$$\prod_{n=0}^{\infty}\prod_{\substack{i\in M^+\\ j\in M^-}}\frac{R(\ell n+i)}{R(\ell n+j)}$$

$$=\prod_{n=0}^{\infty}\prod_{\substack{i\in M^+\\ j\in M^-}}\frac{\left(n+\frac{a_1+i}{\ell}\right)\cdots\left(n+\frac{a_d+i}{\ell}\right)\left(n+\frac{b_1+j}{\ell}\right)\cdots\left(n+\frac{b_l+j}{\ell}\right)}{\left(n+\frac{b_1+i}{\ell}\right)\cdots\left(n+\frac{b_l+i}{\ell}\right)\left(n+\frac{a_1+j}{\ell}\right)\cdots\left(n+\frac{a_d+j}{\ell}\right)} \tag{6.3}$$

$$=\prod_{\substack{i\in M^+\\ j\in M^-}}\frac{\Gamma\left(\frac{b_1+i}{\ell}\right)\cdots\Gamma\left(\frac{b_l+i}{\ell}\right)\Gamma\left(\frac{a_1+j}{\ell}\right)\cdots\Gamma\left(\frac{a_d+j}{\ell}\right)}{\Gamma\left(\frac{a_1+i}{\ell}\right)\cdots\Gamma\left(\frac{a_d+i}{\ell}\right)\Gamma\left(\frac{b_1+j}{\ell}\right)\cdots\Gamma\left(\frac{b_l+j}{\ell}\right)}. \tag{6.4}$$

Now, using the Gauss Multiplication formula

$$(2\pi)^{\frac{\ell-1}{2}}\ell^{(1/2-\ell z)}\Gamma(\ell z)=\Gamma(z)\Gamma\left(z+\frac{1}{\ell}\right)\Gamma\left(z+\frac{2}{\ell}\right)\cdots\Gamma\left(z+\frac{\ell-1}{\ell}\right) \tag{6.5}$$

with $z=\dfrac{a_s}{k}$ or $z=\dfrac{b_t}{k}$ the above simplifies to

$$\begin{aligned}(2\pi)^{\frac{\ell-1}{2}}\ell^{(1/2-\ell a_s)}\Gamma(a_s)&=\Gamma\left(\frac{a_s}{\ell}\right)\Gamma\left(\frac{a_s+1}{\ell}\right)\Gamma\left(\frac{a_s+2}{\ell}\right)\cdots\Gamma\left(\frac{a_s+(\ell-1)}{\ell}\right)\\ &=\Gamma\left(\frac{a_s+i_1}{\ell}\right)\Gamma\left(\frac{a_s+i_2}{\ell}\right)\cdots\Gamma\left(\frac{a_s+i_{|M^+|}}{\ell}\right)\Gamma\left(\frac{a_s+j_1}{\ell}\right)\cdots\Gamma\left(\frac{a_s+j_{|M^-|}}{\ell}\right)\end{aligned}$$

where the last equality follows because $|M^+|+|M^-|=\ell$, and every residue mod ℓ appears on the right hand side exactly once. Dividing both sides by the terms containing $i\in M^+$ yields

$$\prod_{j\in M^-}\Gamma\left(\frac{a_s+j}{\ell}\right)=\frac{(2\pi)^{\frac{\ell-1}{2}}\ell^{(1/2-a_s)}\Gamma(a_s)}{\prod\limits_{i\in M^+}\Gamma\left(\frac{a_s+i}{\ell}\right)}\text{ for all } s=1,...,d \tag{6.6}$$

and similarly

$$\prod_{j\in M^-}\Gamma\left(\frac{b_t+j}{\ell}\right)=\frac{(2\pi)^{\frac{\ell-1}{2}}\ell^{(1/2-b_t)}\Gamma(b_t)}{\prod\limits_{i\in M^+}\Gamma\left(\frac{b_t+i}{\ell}\right)}\text{ for all } t=1,...,r. \tag{6.7}$$

Substituting (6.6) and (6.7) into (6.4) for every s and t yields

$$\frac{(2\pi)^{(\frac{\ell-1}{2})d}\ell^{(1/2-a_1-a_2\cdots-a_d)}}{(2\pi)^{(\frac{\ell-1}{2})r}\ell^{(1/2-b_1-b_2-\cdots-b_r)}}\prod_{\substack{1\le s\le d\\1\le t\le r}}\frac{\Gamma(a_s)}{\Gamma(b_t)}\prod_{j\in M^+}\frac{\Gamma^2\left(\frac{b_t+j}{\ell}\right)}{\Gamma^2\left(\frac{a_s+j}{\ell}\right)}$$

$$=(2\pi)^{(\frac{d-r}{2})(\ell-1)}\ell^{S(a,b)}\prod_{\substack{1\le s\le d\\1\le t\le r}}\frac{\Gamma(a_s)}{\Gamma(b_t)}\prod_{j\in M^+}\frac{\Gamma^2\left(\frac{b_t+j}{\ell}\right)}{\Gamma^2\left(\frac{a_s+j}{\ell}\right)}. \qquad \square$$

7 Infinite products and the paper folding sequence

Recall that the regular paper folding sequence can be defined by the recurrence $t_{2n} = (-1)^n, t_{2n+1} = t_n$ and $t_0 = 1$. In [1], J.P. Allouche gives a closed-form evaluation of the product $\prod_{n=1}^{\infty}\left(\frac{2n}{2n+1}\right)^{t_n}$ in terms of the gamma function. Moreover, he generalizes his result to a wider class of rational functions. Here, the results from previous sections are used (specifically the closed-form formula obtained in section 3) to take a different approach to the product $\prod_{n=1}^{\infty} R(n)^{t_n}$ where $R(n) = \frac{an+b}{cn+d}$ to reproduce the result of [1]. It is known that $a = c \neq 0$ is a necessary condition for the convergence of the product in question, hence let R be as above with $a = c$ and t_n be the regular paper folding sequence, then

$$\prod_{n\ge0}\left(\frac{an+b}{cn+d}\right)^{t_n} = \prod_{n\ge0}\left(\frac{2an+b}{2cn+d}\right)^{(-1)^n}\prod_{n\ge0}\left(\frac{2n+(a+b)}{2n+(c+d)}\right)^{t_n}$$

$$= 2^{\frac{d}{2c}-\frac{b}{2a}}\frac{\Gamma^2(\frac{d}{4c})\Gamma(\frac{b}{2a})}{\Gamma^2(\frac{b}{4a})\Gamma(\frac{d}{2c})}\prod_{n\ge0}\left(\frac{2n+(a+b)}{2n+(c+d)}\right)^{t_n}$$

$$= 2^{\frac12(\frac{d}{c}-\frac{b}{a})}\frac{\Gamma^2(\frac{d}{4c})\Gamma(\frac{b}{2a})}{\Gamma^2(\frac{b}{4a})\Gamma(\frac{d}{2c})}\prod_{n\ge0}\left(\frac{4an+(a+b)}{4n+(c+d)}\right)^{(-1)^n}\prod_{n\ge0}\left(\frac{4an+3a+b}{4cn+3c+d}\right)^{t_n}$$

$$= 2^{\frac12(\frac{d}{c}-\frac{b}{a})}\frac{\Gamma^2(\frac{d}{4c})\Gamma(\frac{b}{2a})}{\Gamma^2(\frac{b}{4a})\Gamma(\frac{d}{2c})}2^{\frac14(\frac{d}{c}-\frac{b}{a})}\frac{\Gamma^2(\frac{c+d}{8c})\Gamma(\frac{a+b}{4a})}{\Gamma^2(\frac{a+b}{8a})\Gamma(\frac{c+d}{4c})}\prod_{n\ge0}\left(\frac{4an+3a+b}{4cn+3c+d}\right)^{t_n} = \cdots$$

Iterating this process N times yields

$$2^{(\frac{d}{c}-\frac{b}{a})\sum\limits_{k\ge1}\frac{1}{2^k}}\prod_{k=2}^{N}\frac{\Gamma^2(\frac14-\frac{d-c}{c2^k})\Gamma(\frac12+\frac{b-a}{a2^{k-1}})}{\Gamma^2(\frac14+\frac{b-a}{2^k})\Gamma(\frac12+\frac{d-c}{c2^{k-1}})}\prod_{n=0}^{\infty}\left(\frac{2^Nan+a(2^N-1)+b}{2^Ncn+c(2^N-1)+d}\right)^{t_n}. \qquad (7.1)$$

Without lost of generality one may assume that $c > 0$. It is claimed that

$$\lim_{N\to\infty}\prod_{n=0}^{\infty}\left(\frac{2^N an + a(2^N-1)+b}{2^N cn + c(2^N-1)+d}\right)^{t_n} = 1. \tag{7.2}$$

To show this, it suffices to prove that $\dfrac{2^N an + a(2^N-1)+b}{2^N cn + c(2^N-1)+d} \to 1$ uniformly as $N \to \infty$, to be able to obtain

$$1 = \prod_{n=0}^{\infty}\left(\lim_{N\to\infty}\frac{2^N an + a(2^N-1)+b}{2^N cn + c(2^N-1)+d}\right)^{t_n} = \lim_{N\to\infty}\prod_{n=0}^{\infty}\left(\frac{2^N an + a(2^N-1)+b}{2^N cn + c(2^N-1)+d}\right)^{t_n}.$$

But this result is almost immediate. Let $\epsilon > 0$ be given. Then $\exists\ K \in \mathbb{N}$ such that for all $r \geq K$ we have

$$\left|\frac{2^r an + a(2^r-1)+b}{2^r cn + c(2^r-1)+d} - 1\right| = \left|\frac{b-d}{2^r cn + c(2^r-1)+d}\right| \leq \frac{b-d}{2^r+d-1} \leq \epsilon$$

for all n.

Hence, as we let $N \to \infty$ we have the equality

$$\prod_{n=0}^{\infty}\left(\frac{an+b}{cn+d}\right)^{t_n} = 2^{\frac{d}{c}-\frac{b}{a}}\prod_{k=2}^{\infty}\frac{\Gamma^2(\frac{1}{4}-\frac{d-c}{c2^k})\Gamma(\frac{1}{2}+\frac{b-a}{a2^{k-1}})}{\Gamma^2(\frac{1}{4}+\frac{b-a}{2^k})\Gamma(\frac{1}{2}+\frac{d-c}{c2^{k-1}})}. \tag{7.3}$$

Here, a closed-form expression for the value of this product is not known, however, in some particular cases this product can be computed in closed-form. In particular, if $2ad = c(b+a)$ a telescoping product is obtained, and the product can be evaluated in closed-form. Now, since $a = c$ without lost of generality one may assume a priori with that R has the form $\dfrac{n+b}{n+d}$; in which case $2ad = c(b+a) \iff d = \dfrac{b+1}{2}$. This is precisely the class of functions for which Allouche gave a closed-form expression for the evaluation of their infinite products. Indeed, setting $a = c = 1$ and $d = \dfrac{1+b}{2}$ in (7.3), expanding partial product and taking the limit, Allouche's closed-form expresion

$$\prod_{n=0}^{\infty}\left(\frac{n+b}{n+\frac{b+1}{2}}\right)^{t_n} = 2^{\frac{1-b}{2}}\frac{\Gamma^2(1/4)\Gamma(b/2)}{\sqrt{\pi}\Gamma^2(b/4)} \tag{7.4}$$

is obtained.

In the particular case of the product $\displaystyle\prod_{n=0}^{\infty}\left(\frac{2n+1}{2n+2}\right)^{t_n}$,

$$\prod_{n=0}^{\infty}\left(\frac{2n+1}{2n+2}\right)^{t_n} = \sqrt{2}\prod_{k=2}^{\infty}\frac{\Gamma^2(\frac{1}{4})\Gamma(\frac{1}{2}-\frac{1}{2^k})}{\Gamma^2(\frac{1}{4}-\frac{1}{2^{k+1}})\Gamma(\frac{1}{2})}. \tag{7.5}$$

Now, noting that

$$\prod_{k=2}^{\infty} \frac{\Gamma(\frac{1}{2}-\frac{1}{2^k})}{\Gamma(1/2)} = \prod_{k=1}^{\infty} \frac{\Gamma(\frac{1}{2}-\frac{1}{2^{k+1}})}{\Gamma(\frac{1}{2})} \tag{7.6}$$

and using Knar's formula [4]

$$\Gamma(1+z) = 2^{2z} \prod_{k=1}^{\infty} \pi^{-1}\Gamma\left(\frac{1}{2}+\frac{z}{2^k}\right), \tag{7.7}$$

with $z = -1/2$, yields

$$\prod_{k=2}^{\infty} \frac{\Gamma(\frac{1}{2}-\frac{1}{2^k})}{\Gamma(\frac{1}{2})} = 2\sqrt{\pi}. \tag{7.8}$$

Therefore

$$\sqrt{2}\prod_{k=2}^{\infty} \frac{\Gamma^2(\frac{1}{4})\Gamma(\frac{1}{2}-\frac{1}{2^k})}{\Gamma^2(\frac{1}{4}-\frac{1}{2^{k+1}})\Gamma(\frac{1}{2})} = 2\sqrt{2\pi}\prod_{k=2}^{\infty} \frac{\Gamma^2(\frac{1}{4})}{\Gamma^2(\frac{1}{4}-\frac{1}{2^{k+1}})}. \tag{7.9}$$

What follows was an attempted approach to evaluate the previous product. In addition to this simplification, it is known that by definition of the infinite product, the right-hand side of (7.5) is equivalent to

$$\sqrt{2}\lim_{N\to\infty}\prod_{k=2}^{N} \frac{\Gamma^2(\frac{1}{4})\Gamma(\frac{1}{2}-\frac{1}{2^k})}{\Gamma^2(\frac{1}{4}-\frac{1}{2^{k+1}})\Gamma(\frac{1}{2})}. \tag{7.10}$$

Note that in equation (7.10) the sum of arguments of the gammas on the numerator equals the sum of the arguments of the gammas in the denominator. This hints to where this finite products of gammas might be coming from. Making use of lemma 2.2 we get

$$\sqrt{2}\lim_{N\to\infty}\prod_{k=2}^{N} \frac{\Gamma^2(\frac{1}{4})\Gamma(\frac{1}{2}-\frac{1}{2^k})}{\Gamma^2(\frac{1}{4}-\frac{1}{2^{k+1}})\Gamma(\frac{1}{2})} = \sqrt{2}\lim_{N\to\infty}\prod_{n=0}^{\infty}\prod_{k=2}^{N} \frac{(n+\frac{1}{2})(n+\frac{1}{4}-\frac{1}{2^{k+1}})^2}{(n+\frac{1}{4})^2(n+\frac{1}{2}-\frac{1}{2^k})}. \tag{7.11}$$

Now, the product $\prod_{k=2}^{\infty} \frac{(n+\frac{1}{2})(n+\frac{1}{4}-\frac{1}{2^{k+1}})^2}{(n+\frac{1}{4})^2(n+\frac{1}{2}-\frac{1}{2^k})}$ converges, if and only if

$$\sum_{k=2}^{\infty} \log\left(\frac{(n+\frac{1}{2})(n+\frac{1}{4}-\frac{1}{2^{k+1}})^2}{(n+\frac{1}{4})^2(n+\frac{1}{2}-\frac{1}{2^k})}\right)$$

converges. It is not hard to see, by comparison test, that this series converges. Moreover

$$\left|\prod_{k=2}^{N+1}\frac{(n+\frac{1}{2})(n+\frac{1}{4}-\frac{1}{2^{k+1}})^2}{(n+\frac{1}{4})^2(n+\frac{1}{2}-\frac{1}{2^k})}-\prod_{k=2}^{N}\frac{(n+\frac{1}{2})(n+\frac{1}{4}-\frac{1}{2^{k+1}})^2}{(n+\frac{1}{4})^2(n+\frac{1}{2}-\frac{1}{2^k})}\right| \tag{7.12}$$

$$=\prod_{k=2}^{N}\frac{(n+\frac{1}{2})(n+\frac{1}{4}-\frac{1}{2^{k+1}})^2}{(n+\frac{1}{4})^2(n+\frac{1}{2}-\frac{1}{2^k})}\left|\left(\frac{(n+\frac{1}{2})(n+\frac{1}{4}-\frac{1}{2^{N+2}})^2}{(n+\frac{1}{4})^2(n+\frac{1}{2}-\frac{1}{2^{N+1}})}-1\right)\right|, \tag{7.13}$$

as $N\to\infty$ the factor on the right goes to zero independently of n whereas the product over k converges. Hence, by Cauchy criterion, this product converges uniformly, obtaining the equality

$$\prod_{n=0}^{\infty}\left(\frac{2n+1}{2n+2}\right)^{t_n}=\sqrt{2}\prod_{k=2}^{\infty}\frac{\Gamma^2(\frac{1}{4})\Gamma(\frac{1}{2}-\frac{1}{2^k})}{\Gamma^2(\frac{1}{4}-\frac{1}{2^{k+1}})\Gamma(\frac{1}{2})}=\sqrt{2}\prod_{n=0}^{\infty}\prod_{k=2}^{\infty}\frac{(n+\frac{1}{2})(n+\frac{1}{4}-\frac{1}{2^{k+1}})^2}{(n+\frac{1}{4})^2(n+\frac{1}{2}-\frac{1}{2^k})}. \tag{7.14}$$

Note that the function

$$\Phi_R(x):=\prod_{k=2}^{\infty}\frac{(x+\frac{1}{2})(x+\frac{1}{4}-\frac{1}{2^{k+1}})^2}{(x+\frac{1}{4})^2(x+\frac{1}{2}-\frac{1}{2^k})}, \tag{7.15}$$

associated to the rational function $R(n)=\frac{2n+1}{2n+2}$, has infinitely many zeros accumulating to $x=-1/4$ which is a pole of Φ_R. On the other hand, it also has infinitely many poles accumulating to $-1/2$ which is a zero of Φ_R. However, for $x\geq 0$ this function is well-behaved, in fact $\lim_{x\to\infty}\Phi_R(x)=1$. Nevertheless, this complicated function might explain some of the underlying difficulties on the evaluation of $\prod_{n=0}^{\infty}\left(\frac{2n+1}{2n+2}\right)^{t_n}$.

8 A special class of automatic sequences

A generalization of the result in [1] is provided in this section. A closed-form formula for evaluation of infinite products of certain rational functions raised to the power of certain class of automatic sequence is also given at the end of this section.

Theorem 8.1. *Let* $R(n) = \dfrac{n+b}{n+d}$ *where* $b, d \in \mathbb{R}^+$ *and let* M_n *be a* k*-automatic sequence satisfying the following recurrence*

$$\begin{cases} M_{kn} = q_0(n) \\ M_{kn+1} = q_1(n) \\ \vdots \\ M_{kn+k-2} = q_{k-2}(n) \\ M_{kn+k-1} = M_n, \end{cases} \tag{8.1}$$

where each $q_i(n)$ *is a* $(2L)^{\alpha_i}$*-periodic sequence, for some* $L \in \mathbb{Z}^+$ *and some power* $\alpha_i \in \mathbb{N}$ *corresponding to* $q_i(n)$*. Additionally, assume that* $|q_i^+| = |q_i^-|$ *for all* $0 \le i \le k-2$*. Then* $\prod_{n=0}^{\infty} R(n)^{M_n}$ *converges. Moreover, if* $d = \dfrac{b+k-1}{k}$ *the product can be evaluated in closed-form given by*

$$\prod_{n=0}^{\infty} R(n)^{M_n} = \prod_{i=0}^{k-2} \left[(2L)^{\frac{\alpha_i(1-b)}{k}} \frac{\Gamma(\frac{b+i}{k})}{\Gamma(\frac{i+1}{k})} \prod_{j \in q_i^+} \frac{\Gamma^2\left(\frac{i+1}{(2L)^{\alpha_i}k} + \frac{j}{(2L)^{\alpha_i}}\right)}{\Gamma^2\left(\frac{b+i}{(2L)^{\alpha_i}k} + \frac{j}{(2L)^{\alpha_i}}\right)} \right]. \tag{8.2}$$

Note that the paperfolding sequence is one such sequence, with $k = 2$, $q_0(n) = (-1)^n$, $L = 1$ and $\alpha_0 = 1$. In this case, $R(n) = \dfrac{n+b}{n+\frac{b+1}{2}}$ and (8.2) simplifies to the result of Allouche, (7.4).

Proof. The argument proceeds by splitting $R(n)$ into the first $k-2$ terms and raising these to their respective periodic powers $q_i(n)$. Then,

$$\begin{aligned} \prod_{n=0}^{\infty} R(n)^{M_n} &= \prod_{n=0}^{\infty}\prod_{i=0}^{k-2} R(kn+i)^{q_i(n)} \prod_{n=0}^{\infty} R(kn+k-1)^{M_n} \\ &= \prod_{n=0}^{\infty}\prod_{i=0}^{k-2} \left(\frac{kn+i+b}{kn+i+d}\right)^{q_i(n)} \prod_{n=0}^{\infty}\prod_{i=0}^{k-2} R(k^2n + k(i+1) - 1)^{q_i(n)} \prod_{n=0}^{\infty} R(k^2n + k^2 - 1)^{M_n} \\ &= \prod_{n=0}^{\infty}\prod_{i=0}^{k-2} \left(\frac{kn+i+b}{kn+i+d}\right)^{q_i(n)} \prod_{n=0}^{\infty}\prod_{i=0}^{k-2} \left(\frac{k^2n + k(i+1) - 1 + b}{k^2n + k(i+1) - 1 + d}\right)^{q_i(n)} \prod_{n=0}^{\infty} R(k^2n + k^2 - 1)^{M_n}, \end{aligned}$$

and after N iterations this becomes

$$= ... = \prod_{\beta=1}^{N}\prod_{n=0}^{\infty}\prod_{i=0}^{k-2}\left(\frac{k^{\beta}n+k^{\beta-1}(i+1)-1+b}{k^{\beta}n+k^{n-1}(i+1)-1+d}\right)^{q_i(n)} \underbrace{\prod_{n=0}^{\infty}\left(\frac{k^{N}n+k^{N}-1+b}{k^{N}n+k^{N}-1+d}\right)^{M_n}}_{\text{F(N,n)}}.$$

It can be easily check (as done in (7.2)) that $F(N,n)$ goes to 1 as $N \to \infty$. So that the preceding triple product contributes entirely to this equality. Letting $N \to \infty$, this simplifies to

$$\prod_{n=0}^{\infty} R(n)^{M_n} = \prod_{\beta=1}^{\infty}\prod_{n=0}^{\infty}\prod_{i=0}^{k-2}\left(\frac{k^{\beta}n+k^{\beta-1}(i+1)-1+b}{k^{\beta}n+k^{n-1}(i+1)-1+d}\right)^{q_i(n)}. \tag{8.3}$$

Isolating the infinite product

$$\prod_{n=0}^{\infty}\prod_{i=0}^{k-2}\left(\frac{k^{\beta}n+k^{\beta-1}(i+1)-1+b}{k^{\beta}nk^{\beta-1}(i+1)-1+d}\right)^{q_i(n)}, \tag{8.4}$$

and noting that finite and infinite products can be interchanged, yields

$$\prod_{i=0}^{k-2}\prod_{n=0}^{\infty}\left(\frac{k^{\beta}n+k^{\beta-1}(i+1)-1+b}{k^{\beta}nk^{\beta-1}(i+1)-1+d}\right)^{q_i(n)}. \tag{8.5}$$

For each fixed i in (8.5), theorem 6.2 can be applied to

$$\prod_{n=0}^{\infty}\left(\frac{k^{\beta}n+k^{\beta-1}(i+1)-1+b}{k^{\beta}n+k^{\beta-1}(i+1)-1+d}\right)^{q_i(n)}. \tag{8.6}$$

Here the function in consideration is $\dfrac{k^{\beta}n+k^{\beta-1}(i+1)-1+b}{k^{\beta}n+k^{\beta-1}(i+1)-1+d}$, which has a single root at $\dfrac{b+k^{\beta-1}(i+1)-1}{k^{\beta}}$ and a single pole at $\dfrac{d+k^{\beta-1}(i+1)-1}{k^{\beta}}$. The sequence in play is $q_i(n)$ which is $(2L)^{\alpha_i}$-periodic. Note also that in this case the degrees in the numerator and denominator are both 1, and $S(b,d) = \dfrac{d-b}{k^{\beta}}$. Therefore, using (6.2), (8.6) reduces to

$$(2L)^{\alpha_i \frac{d-b}{k^{\beta}}} \frac{\Gamma(\frac{b+k^{\beta-1}(i+1)-1}{k^{\beta}})}{\Gamma(\frac{d+k^{\beta-1}(i+1)-1}{k^{\beta}})} \prod_{j\in q_i^{+}} \frac{\Gamma^2(\frac{d+k^{\beta-1}(i+1)-1+jk^{\beta}}{(2L)^{\alpha_i}k^{\beta}})}{\Gamma^2(\frac{b+k^{\beta-1}(i+1)-1+jk^{\beta}}{(2L)^{\alpha_i}k^{\beta}})}, \tag{8.7}$$

so that (8.4) reduces to

$$\prod_{i=0}^{k-2}\left[(2L)^{\alpha_i \frac{d-b}{k^{\beta}}} \frac{\Gamma(\frac{b+k^{\beta-1}(i+1)-1}{k^{\beta}})}{\Gamma(\frac{d+k^{\beta-1}(i+1)-1}{k^{\beta}})} \prod_{j\in q_i^{+}} \frac{\Gamma^2(\frac{d+k^{\beta-1}(i+1)-1+jk^{\beta}}{(2L)^{\alpha_i}k^{\beta}})}{\Gamma^2(\frac{b+k^{\beta-1}(i+1)-1+jk^{\beta}}{(2L)^{\alpha_i}k^{\beta}})}\right]. \tag{8.8}$$

Hence, the product in question becomes

$$\prod_{n=0}^{\infty} R(n)^{M_n} = \prod_{\beta=1}^{\infty}\prod_{i=0}^{k-2}\left[(2L)^{\alpha_i \frac{d-b}{k^\beta}} \frac{\Gamma(\frac{b+k^{\beta-1}(i+1)-1}{k^\beta})}{\Gamma(\frac{d+k^{\beta-1}(i+1)-1}{k^\beta})} \prod_{j\in q_i^+} \frac{\Gamma^2(\frac{d+k^{\beta-1}(i+1)-1+jk^\beta}{(2L)^{\alpha_i}k^\beta})}{\Gamma^2(\frac{b+k^{\beta-1}(i+1)-1+jk^\beta}{(2L)^{\alpha_i}k^\beta})}\right]. \tag{8.9}$$

Once again, interchanging finite and infinite products yields

$$\prod_{n=0}^{\infty} R(n)^{M_n} = \prod_{i=0}^{k-2}\prod_{\beta=1}^{\infty}\left[(2L)^{\alpha_i \frac{d-b}{k^\beta}} \frac{\Gamma(\frac{b+k^{\beta-1}(i+1)-1}{k^\beta})}{\Gamma(\frac{d+k^{\beta-1}(i+1)-1}{k^\beta})} \prod_{j\in q_i^+} \frac{\Gamma^2(\frac{d+k^{\beta-1}(i+1)-1+jk^\beta}{(2L)^{\alpha_i}k^\beta})}{\Gamma^2(\frac{b+k^{\beta-1}(i+1)-1+jk^\beta}{(2L)^{\alpha_i}k^\beta})}\right]. \tag{8.10}$$

Now, $\prod_{\beta=1}^{\infty}(2L)^{\alpha_i \frac{d-b}{k^\beta}} = (2L)^{\alpha_i \frac{d-b}{k-1}}$ so that (8.10) becomes

$$\prod_{i=0}^{k-2}(2L)^{\alpha_i \frac{d-b}{k-1}} \prod_{\beta=1}^{\infty}\left[\frac{\Gamma(\frac{b+k^{\beta-1}(i+1)-1}{k^\beta})}{\Gamma(\frac{d+k^{\beta-1}(i+1)-1}{k^\beta})} \prod_{j\in q_i^+} \frac{\Gamma^2(\frac{d+k^{\beta-1}(i+1)-1+jk^\beta}{(2L)^{\alpha_i}k^\beta})}{\Gamma^2(\frac{b+k^{\beta-1}(i+1)-1+jk^\beta}{(2L)^{\alpha_i}k^\beta})}\right]. \tag{8.11}$$

The goal is now to find sufficient conditions for the closed-form evaluation of the infinite product on (8.11). A simple way in which this product can be evaluated in closed-form is if it is a telescoping product. Note that if $\dfrac{d+k^{\beta-1}(i+1)-1}{k^\beta} = \dfrac{b+k^\beta(i+1)-1}{k^\beta+1}$ it would also be true that $\dfrac{d+k^{\beta-1}(i+1)-1+jk^\beta}{(2L)^{\alpha_i}k^\beta} = \dfrac{b+k^\beta(i+1)-1+jk^{\beta+1}}{(2L)^{\alpha_i}k^{\beta+1}}$, and the product would indeed be a telescoping product. Now,

$$\begin{aligned} \frac{d+k^{\beta-1}(i+1)-1}{k^\beta} &= \frac{b+k^\beta(i+1)-1}{k^\beta+1} \\ \iff d &= \frac{b+k^\beta(i+1)-1}{k} - k^{\beta-1}(i+1)-1 \\ \iff d &= \frac{b+k-1}{k}. \end{aligned}$$

Making this substitution, the product in question becomes

$$\prod_{i=0}^{k-2}(2L)^{\frac{\alpha_i(1-b)}{k}} \prod_{\beta=1}^{\infty}\left[\frac{\Gamma(\frac{b+k^{\beta-1}(i+1)-1}{k^\beta})}{\Gamma(\frac{b+k^{\beta}(i+1)-1}{k^{\beta+1}})} \prod_{j\in q_i^+} \frac{\Gamma^2(\frac{b+k^{\beta}(i+1)-1+jk^{\beta+1}}{(2L)^{\alpha_i}k^{\beta+1}})}{\Gamma^2(\frac{b+k^{\beta-1}(i+1)-1+jk^\beta}{(2L)^{\alpha_i}k^\beta})}\right]. \tag{8.12}$$

It is now easily seen that the infinite product telescopes. In fact

$$\prod_{\beta=1}^{\infty}\left[\frac{\Gamma(\frac{b+k^{\beta-1}(i+1)-1}{k^\beta})}{\Gamma(\frac{b+k^{\beta}(i+1)-1}{k^{\beta+1}})} \prod_{j\in q_i^+} \frac{\Gamma^2(\frac{b+k^{\beta}(i+1)-1+jk^{\beta+1}}{(2L)^{\alpha_i}k^{\beta+1}})}{\Gamma^2(\frac{b+k^{\beta-1}(i+1)-1+jk^\beta}{(2L)^{\alpha_i}k^\beta})}\right]$$

$$= \lim_{N\to\infty} \frac{\Gamma(\frac{b+i}{k})}{\Gamma(\frac{d+k^{N-1}(i+1)-1}{k^N})} \prod_{j\in q_i^+} \frac{\Gamma(\frac{d+k^{N-1}(i+1)-1+jk^N}{(2L)^{\alpha_i}k^N})}{\Gamma(\frac{b+i+jk}{(2L)^{\alpha_i}k})}$$

$$= \frac{\Gamma(\frac{b+i}{k})}{\Gamma(\frac{i+1}{k})} \prod_{j\in q_i^+} \frac{\Gamma^2(\frac{i+1}{(2L)^{\alpha_i}k} + \frac{j}{2^{\alpha_i}})}{\Gamma^2(\frac{b+i}{(2L)^{\alpha_i}k} + \frac{j}{2^{\alpha_i}})}. \tag{8.13}$$

Substituting this last expression into (8.12) yields (8.2) and completes the proof. □

Remarks on theorem 8.2.

- The condition that each $q_i(n)$ has even period, at first sight, seems unnecessary. However, If some $q_i(n)$ had odd period then it would fall in *case* (i) of theorem 6.1, so that $\prod_{n=0}^{\infty}\left(\frac{k^\beta n + k^{\beta-1}(i+1)-1+b}{k^\beta n + k^{\beta-1}(i+1)-1+d}\right)^{q_i(n)}$ converges if, and only if, $b = d$. Hence the conclusion would be false.

- This result can be generalized to any rational function of the form $R(n) = \frac{(n+a_1)\cdots(n+a_d)}{(n+b_1)\cdots(n+b_d)}$ where $a_i, b_j \notin -\mathbb{N}$. In this case, the condition would be that to each a_i corresponds a unique b_j such that $b_j = \frac{a_i+k-1}{k}$. Without lost of generality, the denominator of R can be rearranged in such a way that $R(n) = \frac{(n+a_1)\cdots(n+a_d)}{(n+\frac{a_1+k-1}{k})\cdots(n+\frac{a_d+k-1}{k})}$. Then, the closed-forms formula is obtained by means of $\prod_{n=0}^{\infty} R(n)^{M_n} = \prod_{m=1}^{d}\prod_{n=0}^{\infty}\left(\frac{n+a_i}{n+\frac{a_i+k-1}{k}}\right)^{M_n}$.

9 Preliminaries on p-adic valuations

The introduction briefly described what a p-adic valuation is, here, this topic is explored further.

Definition 9.1. The p-adic valuation of a number is denoted by $\nu_p(n)$ for a fixed prime p and is equal to the exponent of the highest power of prime p that n is divisible by.

Example 9.1. The 3-adic valuation of 45 is equal to the highest power of 3 that 45 is divisble by. The number 45 expressed as a list of it's prime factors produces $\{3, 3, 5\}$. Since there are two 3's the 3-adic valuation of 45 is 2,

$$\nu_3(45) = 2 \tag{9.1}$$

In relation to the purpose of this report, the p-adic valuations of the partial products of the previously discussed infinite products, may reveal some unknowns. For example, when evaluating the 2-adic valuation of

$$\prod_{n=1}^{N}\left(\frac{n}{n+1}\right)^{(-1)^n} \tag{9.2}$$

it was reasonable to infer that the partial products are never integers when $N \geq 2$. When looking at the 2-adic valuations as N got larger the outputs were either negative or 0 thus implying rational numbers.

Proposition 9.1. *The partial products of Equation* (9.2) *are never integers when* $N \geq 2$*.*

Proof. Suppose $N \geq 2$ and consider the finite product

$$\prod_{n=1}^{N}\left(\frac{n}{n+1}\right)^{(-1)^n}. \tag{9.3}$$

Case 1: When $n \in 2k$, $a_n = \frac{2k}{2k+1}$.

Case 2: When $n \in 2k+1$, $a_n = \frac{2k+2}{2k+1}$.

In both cases the denominators of a_n is odd whereas the numerator is even thus Equation 9.3 is equal to $\frac{p}{q}$ where $p \in 2\mathbb{Z}$ and $q \notin 2\mathbb{Z}$. Hence $\frac{p}{q} \notin \mathbb{Z}$. □

Discoveries of these sort aid the thorough comprehension of partial products of rational functions raised to certain sequences. The nature of the alternating sequence is an elementary case therefore this report will analyze the characteristics related to the paperfolding sequence.

10 p-adic valuations of paper folding partial products

The difficulties with $\prod_{n=1}^{\infty}\left(\frac{2n+1}{2n+2}\right)^{t_n}$, where t_n is the paperfolding sequence, were discussed in Section 7 in comparison to the simpler evaluation of $\prod_{n=1}^{\infty}\left(\frac{2n}{2n+1}\right)^{t_n}$ as seen in [1]. In addition to studying the behavior of the Φ_R function (Section 7), it is worthwhile to investigate the p-adic properties of the two aformentioned products' partials, $\prod_{n=1}^{N}\left(\frac{2n}{2n+1}\right)^{t_n}$ and

$\prod_{n=1}^{N}\left(\frac{2n+1}{2n+2}\right)^{t_n}$, as the p-adic metric is an extension of rational number qualities. These properties were studied using *Mathematica* 9.0.1 Software.

Preliminarily the two products' p-adic valuations were evaluated along with statistical measures on the data points. *Prod* and *Prod1* represent the partial products, respectively. The resulting grid appeared as such for the first two p-adic valuations:

{

2 Prime	Prod	Prod1
Mean	999.105	-38.3401
Median	997.	-38.
Variance	333 109.	160.167
Skewness	-0.00180552	0.014431
StandardDev	577.156	577.156

,

3 Prime	Prod	Prod1
Mean	-2.0225	7.29607
Median	-2.	7.
Variance	41.4279	37.6562
Skewness	-0.157954	-0.084667
StandardDev	6.43645	6.43645

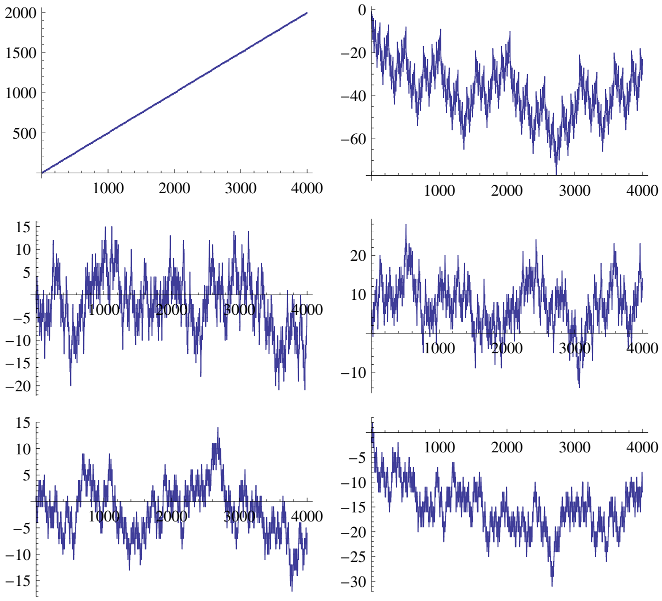
}

An initial observation shows how the means and medians for each product are extremely close in value. Even though the variances are different between the products, the standard deviations are equal. Next we see tables for different primes, together with their respective plots,

2 Prime	Prod	Prod1
Mean	999.105	-38.3401
Median	997.	-38.
Variance	333 109.	160.167
Skewness	-0.00180552	0.014431
StandardDev	577.156	577.156

3 Prime	Prod	Prod1
Mean	-2.0225	7.29607
Median	-2.	7.
Variance	41.4279	37.6562
Skewness	-0.157954	-0.084667
StandardDev	6.43645	6.43645

5 Prime	Prod	Prod1
Mean	-1.69225	-15.1318
Median	-2.	-15.
Variance	25.2789	23.9669
Skewness	0.0337012	0.170986
StandardDev	5.02781	5.02781



The initial obervations from the primes 2 and 3 hold for the primes 5, 7, 11, and 13 as well. A pattern is more apparent now with the given plots. The left plots represent

$$\nu_p\left(\prod_{n=1}^{4000}\left(\frac{2n}{2n+1}\right)^{t_n}\right) \text{ for all prime } p. \tag{10.1}$$

The data clusters stagger about the x-axis continuously, excluding prime 2. Prime 2 exhibits different qualities because the numerator will always be an even value therefore the 2-adic valuation will always be positive. In contrast the right plots, representing

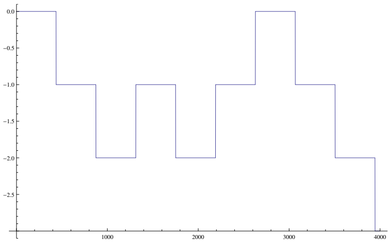
$$\nu_p\left(\prod_{n=1}^{4000}\left(\frac{2n+1}{2n+2}\right)^{t_n}\right) \text{ for all prime } p, \tag{10.2}$$

display inconsistent trends among the shown primes. In particular, primes 2, 5, and 13 have most of their data points below the x-axis. There seems to be a pattern among certain primes that evaluate mostly negative p-adic valuations. When the plots are extended to the first 20 prime numbers the prime values 29, 37, 53, and 61 exhibit the same p-adic trait as 2, 5, and 13. Querying the sequence $\{2, 5, 13, 29, 37, 53, 61\}$ in The On-line Encyclopedia of Integer Sequences revealed that this is a sequence of prime numbers congruent to $\{2, 5\}$ mod 8 [8]. It was then necessary to evaluate certain primes in the sequence on Equation 10.2.

Example 10.1. $877 \equiv 5 \bmod 8$ since $877 - 5 = 872$ and 872 is a multiple of 8. The plot of

$$\nu_{877}\left(\prod_{n=1}^{4000}\left(\frac{2n+1}{2n+2}\right)^{t_n}\right) \tag{10.3}$$

is shown below:



As expected the 877-adic values are less than 0.

Now that there is a list of primes exhibiting a notable effect onto Equation 10.2 the concept of "mostly negative" has to be quantified. Meaning the p-adic valuations of these special primes on the function produced values that were "mostly" less than 0. This paper will define "mostly" as a percentage cutoff. Next, a table of several primes congruent to 5 modulo 8, together with the respective percentage of values of N for which the p-adic valuation of the products is negative.

This was evaluated for

$$\nu_p\left(\prod_{n=1}^{50000}\left(\frac{2n+1}{2n+2}\right)^{t_n}\right) \tag{10.4}$$

for the first 79 primes, p, where $p \equiv \{2, 5\}$ mod 8.

p	%	p	%	p	%	p	%
2	100	373	99	853	42	1453	96
5	100	389	98	877	93	1493	89
13	100	397	99	941	98	1549	93
29	100	421	97	997	91	1597	98
37	100	461	91	1013	95	1613	84
53	96	509	100	1021	99	1621	89
61	100	541	95	1061	99	1637	99
101	100	557	99	1069	98	1669	90
109	100	613	99	1093	87	1693	99
149	100	653	95	1109	44	1709	95
157	100	661	95	1117	99	1733	80
173	99	677	98	1181	99	1741	83
181	96	701	100	1213	99	1789	99
197	87	709	78	1229	80	1861	80
229	94	733	100	1237	51	1877	89
269	98	757	99	1277	99	1901	95
277	84	773	89	1301	71	1933	91
293	100	797	97	1373	99	1949	99
317	98	821	80	1381	89	1973	79
349	100	829	97	1429	95		

There are only three prime values yielding a percentage less than 70%, which are 853, 1109, and 1237, with percentages of 42, 44, and 51, respectively. Beyond those exceptions, the other 76 primes resulted in percentages greater than 70%. Conclusively, the p-adic valuations of $\prod_{n=1}^{N} \left(\frac{2n+1}{2n+2} \right)^{t_n}$ are characterized when p is congruent to $\{2, 5\}$ mod 8.

11 Closing remarks

The main result, theorem 8.2 has allowed the closed form evaluation of many new types of k-automatic products. However these results hold only when the periods of the periodic components of these sequences are powers of a fixed even number. It is conjectured that this method of proof cannot be generalized to periods which are powers of an odd number. The conclusion of theorem 6.1 imposes the condition that the sum of the roots and the sum of the poles are equal. With this restrictive condition it is reasonable to believe that thess infinite products cannot telescope in any case other than the trivial.

In the attempt to develop closed form expressions for k-automatic products, the algorithm developed in theorem 8.2 is suited for k-automatic sequences which decompose into periodic components. Other automatic sequences, such as the Rudin-Shapiro sequence, [7], have no periodic subsequence and will require new approaches.

In section 7 there is an equivalent representation of the product $\prod_{n=0}^{\infty}\left(\frac{2n+1}{2n+2}\right)^{t_n}$ where t_n is the regular paper folding sequence. The representation

$$\prod_{n=0}^{\infty}\left(\frac{2n+1}{2n+2}\right)^{t_n} = 2\sqrt{2\pi}\prod_{k=2}^{\infty}\frac{\Gamma^2(1/4)}{\Gamma^2(\frac{1}{4}-\frac{1}{2^{k+1}})} \tag{11.1}$$

is closely related to the product

$$\prod_{k=2}^{\infty}\frac{\Gamma(\frac{1}{2}-\frac{1}{2^k})}{\Gamma(1/2)} = 2\sqrt{\pi} \tag{11.2}$$

which was evaluated using Knar's formula [4]. It remains an open question to evaluate this product in closed form. It is suspected that if there is a solution to this question, it will rely on the generalized Knar's formula given by J. Logsdon in [5].

In section 10 the p-adic valuations of the partial products $\prod_{n=0}^{N}\left(\frac{2n+1}{2n+2}\right)^{t_n}$ were studied. It was seen that for primes of the form $p \equiv 5 \bmod 8$, the valuations of these partial products were mostly negative. It is conjecture that for $p \equiv 5 \bmod 8$ there exist an integer M such that, for all $N \geq M$, $\nu_p\left(\prod_{n=0}^{N}\left(\frac{2n+1}{2n+2}\right)^{t_n}\right) \leq 0.$

12 Acknowledgments

The authors would like to thank Dr. Victor Moll, Dr. Herbert Medina, Dr. Eric Rowland, Leyda Almodóvar and the MSRI-UP staff for their help and support during this project.

The first author would like to thank Dr. Richard Mitchell and Professor Viktor Ginzburg of the University of California, Santa Cruz for all the support and instruction they have given.

The second author would like to thank Professor David Auckly, Professor Virginia Naibo and Professor Dan Volok for all of their guidance and support.

The third author would like to thank Sonya Jackson, Professor Kirsten Wickelgren, and Christy Lock for their unparalleled support, commitment, and guidance.

This work was conducted during the 2014 Mathematical Sciences Research Institute Undergraduate Program (MSRI-UP) which is funded by the National Science Foundation (grant No. DMS-1156499) and the National Security Agency (grant No. H-98230-13-1-0262).

References

[1] J.P. Allouche. Paperfolding infinite products and the gamma function. *arXiv preprint arXiv:1406.7407*, 2014.

[2] J.P. Allouche and J. Shallit. *Automatic sequences: theory, applications, generalizations.* Cambridge University Press, 2003.

[3] P. Borwein and W. Dykshoorn. An interesting infinite product. *J. Math. Anal. Appl.*, 179(1):203–207, 1993.

[4] A. Erdélyi, W. Magnus, F. Oberhettinger, and F. G. Tricomi. *Higher transcendental functions. Vol. II.* Robert E. Krieger Publishing Co., Inc., Melbourne, Fla., 1981. Based on notes left by Harry Bateman, Reprint of the 1953 original.

[5] J. Logsdon. A generalization of Knar's formula. *Int. J. Pure Appl. Math.*, 61(4):375–379, 2010.

[6] Z. A. Melzak. Infinite products for π e and π/e. *Amer. Math. Monthly*, pages 39–41, 1961.

[7] M. Mendès France. The Rudin-Shapiro sequence, Ising chain, and paperfolding. In *Analytic number theory (Allerton Park, IL, 1989)*, volume 85 of *Progr. Math.*, pages 367–382. Birkhäuser Boston, Boston, MA, 1990.

[8] OEIS. The On-Line Encyclopedia of Integer Sequences, Sequence A045366. Electronically at http://oeis.org.

[9] T. J. Osler. The tables of John Wallis and the discovery of his product for π. *Math. Gazette*, 94(531):430–437, 2010.

[10] J. Sondow. Evaluation of Tachiya's algebraic infinite products involving Fibonacci and Lucas numbers. *arXiv preprint arXiv:1106.4246*, 2011.

[11] E. T. Whittaker and G. N. Watson. *A course of modern analysis.* Cambridge university press, 1927.

On p-adic valuations of the generalized Fibonacci sequences

Joseph Chavoya California State University Fullerton

Alphonso Lucero Iowa State University

Sean Reynolds University of Chicago

August 2014

Abstract

We study the p-adic valuations of generalized Fibonacci sequences, focusing on the particular sequence given by $S_n = F_n + 2L_n$, where F_n and L_n are the Fibonacci and Lucas sequences, respectively. Analyzing this sequence, we create a closed form formula for certain p, as well as formulate conjectures regarding sequences appearing from studying $\nu_p(S_n)$.

1 Introduction

The Fibonacci and Lucas numbers are well-known sequences given by a second order recurrence that share many identities. Only the initial conditions differ. The Fibonacci numbers, F_n, start with $(0, 1)$ and the Lucas numbers, L_n, with $(2, 1)$. These two initial conditions form a basis for $\mathbb{Z}^2$.

Definition 1.1. Linear combinations of these two sequences, that is, the sequences of the form $f_n = aF_n + bL_n$, are called here *generalized Fibonacci sequences*, denoted by f_n. These satisfy $f_n = f_{n-1} + f_{n-2}$ with the initial conditions $(f_0, f_1) = a(0, 1) + b(2, 1)$.

In order to properly study the powers of primes that divide these generalized Fibonacci numbers and the properties that arise from them, we make extensive use of the p-adic valuation.

Definition 1.2. The *p-adic valuation* of an integer n, denoted by $\nu_p(n)$, is the highest power of p that divides n.

The *p-adic metric*, denoted $\mid \cdot \mid_p$, of a number x is defined such that $\mid x \mid_p = p^{-\nu_p(x)}$. In particular, define $\mid 0 \mid_p = 0$ for all primes p.

Proposition 1.3 (Properties of $\nu_p(n)$)**.** *For a prime p and integers a, b*

$$\nu_p(ab) = \nu_p(a) + \nu_p(b).$$

If $\nu_p(a) \neq \nu_p(b)$,

$$\nu_p(a+b) = \min(\nu_p(a), \nu_p(b)).$$

Wall [7] shows that the Fibonacci sequence is periodic modulo m for all $m \in \mathbb{N}$. Furthermore, he shows that any natural number is a factor of some Fibonacci number.

Theorem 1.4 (Wall)**.** *For every $m \in \mathbb{N}$, $F_n \bmod m$ forms a periodic sequence.*

Theorem 1.5 (Wall)**.** *For every $m \in \mathbb{N}$, there exists an index n such that $F_n \equiv 0 \bmod m$.*

The p-adic valuations of the Fibonacci and Lucas numbers are well understood. The next result appears in Lengyel [6].

Theorem 1.6 (Lengyel)**.** *Let*
$\alpha(p) =$ *the smallest n such that $F_n \equiv 0 \bmod p$,*
$\pi(p) =$ *the period length of F_n modulo p, and*
$\eta(p) = \nu_p(F_{\alpha(p)})$.

Then, for $p \neq 2$ or 5,

$$\nu_p(F_n) = \begin{cases} \nu_p(n) + \eta(p) & n \equiv 0 \bmod \alpha(p) \\ 0 & \textit{otherwise}, \end{cases}$$

and

$$\nu_p(L_n) = \begin{cases} \nu_p(n) + \eta(p) & \pi(p) \neq 4\alpha(p) \textit{ and } n \equiv \frac{\alpha(p)}{2} \bmod \alpha(p) \\ 0 & \textit{otherwise.} \end{cases}$$

For $p = 2$,

$$\nu_2(F_n) = \begin{cases} 0 & n \equiv 1,2 \bmod 3 \\ 1 & n \equiv 3 \bmod 6 \\ \nu_2(n) + 2 & n \equiv 0 \bmod 6, \end{cases} \quad \textit{and} \quad \nu_2(L_n) = \begin{cases} 0 & n \equiv 1,2 \bmod 3 \\ 2 & n \equiv 3 \bmod 6 \\ 1 & n \equiv 0 \bmod 6. \end{cases}$$

Finally, for $p = 5$,

$$\nu_5(F_n) = \nu_5(n) \text{ and } \nu_5(L_n) = 0.$$

Bloom [1] provides a characterization of the period length of generalized Fibonacci sequences modulo m.

Theorem 1.7 (Bloom)**.** *If a generalized Fibonacci sequence f_n has a term f_N such that $m \mid f_N$, then the period of $f_n \bmod m$ is equal to the period of $F_n \bmod m$.*

However, little is known about the p-adic valuations of the generalized Fibonacci numbers. Given that any generalized Fibonacci sequence can be expressed as $f_n = aF_n + bL_n$, we expect there to be similar results regarding their p-adic valuation. In the next section, we apply identities for F_n and L_n and Proposition 1.3 in order to explicitly calculate $\nu_p(aF_n + bL_n)$.

2 Formulas for generalized Fibonacci sequences

Using the identity $L_n = F_{n-1} + F_{n+1}$, the following is true:

Theorem 2.1.

$$aF_n + bL_n = \begin{cases} 2aF_{n+1} & \text{if } a = b \\ (2a+k)F_{n+1} + kF_{n-1} & \text{if } a < b \\ (2b)F_{n+1} + lF_n & \text{if } a > b. \end{cases}$$

where $k = b - a$ and $l = a - b$.

Proof. Case 1: If $a = b$, then

$$\begin{aligned} aF_n + bL_n &= aF_n + aL_n \\ &= aF_n + aF_{n-1} + aF_{n+1} \\ &= aF_{n+1} + aF_{n+1} \\ &= 2aF_{n+1}, \end{aligned}$$

as needed.

Case 2: If $a < b$, then $b = a + k$ for some $k \in \mathbb{Z}$ and

$$\begin{aligned}
aF_n + bL_n &= aF_n + (a+k)L_n \\
&= aF_n + (a+k)F_{n-1} + (a+k)F_{n+1} \\
&= aF_n + (a)F_{n-1} + (a)F_{n+1} + kF_{n-1} + kF_{n+1} \\
&= aF_{n+1} + (a)F_{n+1} + kF_{n-1} + kF_{n+1} \\
&= 2aF_{n+1} + kF_{n-1} + kF_{n+1} \\
&= (2a+k)F_{n+1} + kF_{n-1},
\end{aligned}$$

as needed.

Case 3: If $a > b$, then $a = b + l$ for some $l \in \mathbb{Z}$ and

$$\begin{aligned}
aF_n + bL_n &= (b+l)F_n + bL_n \\
&= bF_n + bF_{n-1} + bF_{n+1} + lF_n \\
&= bF_{n+1} + bF_{n+1} + lF_n \\
&= 2bF_{n+1} + lF_n,
\end{aligned}$$

as needed. □

Example 2.2. If $a = b = 1$, then

$$\begin{aligned}
F_n + L_n &= F_n + L_n \\
&= F_n + F_{n-1} + F_{n+1} \\
&= F_{n+1} + F_{n+1} \\
&= 2F_{n+1}.
\end{aligned}$$

Example 2.3. If $a = 2$ and $b = 1$, it follows that

$$\begin{aligned}
2F_n + L_n &= F_n + F_{n-1} + F_{n+1} + F_n \\
&= F_{n+1} + F_{n+1} + F_n = 2F_{n+1} + F_n.
\end{aligned}$$

(Note that for this particular example, it follows that $2F_{n+1} + F_n = F_{n+2} + F_{n+1} = F_{n+3}$).

Making this observation, it is possible to represent the p-adic valuations of generalized Fibonacci sequences using the well-known p-adic valuation of the Fibonacci sequences.

Corollary 2.4.

$$\nu_p(aF_n+bL_n) = \begin{cases} \nu_p(2aF_{n+1}) & \text{if } a = b \\ \min(\nu_p((2a+k)F_{n+1}), \nu_p(kF_{n-1})) & \text{if } a < b \text{ and } \nu_p((2a+k)F_{n+1}) \neq \nu_p(kF_{n-1}) \\ \min(\nu_p((2b)F_{n+1}), \nu_p(lF_n)) & \text{if } a > b \text{ and } \nu_p((2b)F_{n+1}) \neq \nu_p(lF_n). \end{cases}$$

where $k = b - a$ and $l = a - b$.

Note that this representation only provides clear insight in very few cases, i.e. $a = b$.

Example 2.5. If $a = b$, then

$$\nu_2(aF_n + bL_n) = \nu_2(2aF_{n+1}) = \nu_2(aF_{n+1}) + 1.$$

3 Reduction Modulo Powers of Primes

Proving formulas for p-adic valuations for generalized Fibonacci sequences required a technique called *Reduction Modulo Powers of Primes.* Taking a sequence modulo powers of p for some prime p, is enough to determine the p-adic valuation of the sequence. This technique relied on 3 principles:

Proposition 3.1. *The Fibonacci second order recurrence holds under modular arithmetic.*

Proposition 3.2. *All generalized Fibonacci sequences are periodic modulo m, for all natural numbers m.*

Proposition 3.3. *For an integer x and a prime p, $x \equiv 0 \bmod p^n$ and $x \not\equiv 0 \bmod p^{n+1}$ imply $\nu_p(x) = n$.*

Consider $\{f_n\}$ modulo p. If there are indices n where $f_n \not\equiv 0 \bmod p$, then $\nu_p(f_n) = 0$. Similarly, $\{f_n\}$ is reduced modulo p^2 and indices where p^2 does not divide f_n but p divides f_n are found, and consequently, $\nu_p(f_n) = 1$. This process is repeated until $f_n \not\equiv 0 \bmod p^k$ for all $n \in \mathbb{N}$. From Proposition 3.1 and Proposition 3.2, it can be concluded that this process will hold for all indices n. An illustration of this technique is provided in the proof of the following theorem.

Theorem 3.4. *Let $S_n = F_n + 2L_n$,*

$$\nu_2(S_n) = \begin{cases} 0 & n \equiv 1, 2 \bmod 3 \\ 1 & n \equiv 3 \bmod 6 \\ 2 & n \equiv 0 \bmod 6. \end{cases}$$

Proof. By Proposition 3.1, the recursion formula $S_n = S_{n-1} + S_{n-2}$ holds modulo m, for all $m \in \mathbb{N}$. Now consider S_n mod 2^α.

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13
S_n	4	3	7	10	17	27	44	71	115	186	301	487	788	1275
S_n mod 2	0	1	1	0	1	1	0	1	1	0	1	1	0	1
S_n mod 2^2	0	3	3	2	1	3	0	3	3	2	1	3	0	3
S_n mod 2^3	4	3	7	2	1	3	4	7	3	2	5	7	4	3

When $\alpha = 1$ notice that if $n \equiv 1$ or 2 mod 3, then $S_n \not\equiv 0$ mod 2, and by Proposition 3.3, $\nu_2(S_n) = 0$. For $\alpha = 2$, notice that if $n \equiv 3$ mod 6, $\nu_2(S_n) = 1$ by Proposition 3.3. Finally, when $\alpha = 3$, it is clear that $\nu_2(S_n) = 2$ for $n \equiv 0$ mod 6 since 2^3 does not divide any term of S_n.

Now, because the recursion formula is maintained, it is clear that there is periodicity, and so the sequence will repeat modulo m if any two terms repeat consecutively. For S_n modulo 2 the period is 3, modulo 2^2 the period is 6, and modulo 2^3 the period is 12. □

4 2-adic Valuations

Based off of Theorem 1.6, the 2-adic valuations of Fibonacci and Lucas numbers are special cases in which an explicit formula for $\nu_2(F_n)$ and $\nu_2(L_n)$ can be determined. This is shown in the fact that $\nu_2(L_n)$ is 0,1, or 2 depending on n. In order to determine $\nu_2(aF_n + bL_n)$, a and b must be known to apply Theorem 1.6 to get a formula for $\nu_2(aF_n + bL_n)$. In the following theorem's we present specific cases of a and b where an explicit formula for $\nu_2(aF_n + bL_n)$ could be determined. Note that in all of these theorems, we relate $\nu_2(aF_n + bL_n)$ to $\nu_2(L_n)$. For other values of a and b, $\nu_2(aF_n + bL_n)$ is unknown.

In choosing arbitrary values for a, b, $\nu_2(aF_n + bL_n)$ was calculated and the following pairs of (a, b) gave explicit formulas similar to $\nu_2(L_n)$:

$(1,2)$	$(3,2)$	$(4,1)$	$(5,1)$
$(1,3)$	$(3,5)$	$(4,3)$	$(5,2)$
$(1,6)$	$(3,6)$	$(4,5)$	$(5,3)$
$(1,7)$	$(3,7)$	$(4,7)$	$(5,6)$
$(1,9)$	$(3,9)$	$(4,9)$	$(5,10)$
$(1,10)$	$(3,10)$	$(4,11)$	$(5,13)$.

For the column where $a = 4$ and b odd, the following theorem was developed.

Theorem 4.1. *For odd, positive integer b and $k \geq 2$*

$$\nu_2(2^k F_n + bL_n) = \nu_2(L_n) = \begin{cases} 0 & n \equiv 1, 2 \bmod 3 \\ 2 & n \equiv 3 \bmod 6 \\ 1 & n \equiv 0 \bmod 6. \end{cases}$$

Proof. Consider $\{2^k F_n + bL_n\}$ modulo powers of 2.

n	0	1	2	3	4	5	6	7	8	9	10	11
$2^k F_n$ mod 2	0	0	0	0	0	0	0	0	0	0	0	0
bL_n mod 2	0	1	1	0	1	1	0	1	1	0	1	1
$2^k F_n + bL_n$ mod 2	0	1	1	0	1	1	0	1	1	0	1	1

Since $2^k F_n$ is a multiple of 2, $2^k F_n \equiv 0 \bmod 2$. Also, $b \equiv 1 \bmod 2$ so bL_n mod 2 has the same periodic structure as L_n mod 2. Therefore, for $n \equiv 1, 2 \bmod 2$, $\nu_2(2^k F_n + bL_n) = 0$. For this section choose $b \equiv 3 \bmod 4$. When $b \equiv 1 \bmod 4$, the coming results follow similarly.

n	0	1	2	3	4	5	6	7	8	9	10	11
$2^k F_n$ mod 4	0	0	0	0	0	0	0	0	0	0	0	0
L_n mod 4	2	1	3	0	3	3	2	1	3	0	3	3
bL_n mod 4	2	3	1	0	1	1	2	3	1	0	1	1
$2^k F_n + bL_n$ mod 4	2	3	1	0	1	1	2	3	1	0	1	1

Since $2^k F_n$ is a multiple of 4, $2^k F_n \equiv 0 \bmod 4$. From the table for $n \equiv 0 \bmod 6$, $\nu_2(2^k F_n + bL_n) = 1$. Now all that is left to check is $2^k F_n + bL_n$ mod 8 for $n \equiv 3 \bmod 6$.

For this section choose $b \equiv 3 \bmod 8$. When $b \equiv 1, 5, 7 \bmod 8$, the following results follow similarly. Also, if $k \geq 3$, then $2^k F_n \equiv 0 \bmod 8$ and the result would follow trivially, so assume $k = 2$.

n	0	1	2	3	4	5	6	7	8	9	10	11
$F_n \bmod 8$	0	1	1	2	3	5	0	5	5	2	7	1
$2^k F_n \bmod 8$	0	4	4	0	4	4	0	4	4	0	4	4
$L_n \bmod 8$	2	1	3	4	7	3	2	5	7	4	3	7
$bL_n \bmod 8$	6	3	1	4	5	1	6	7	5	4	1	5
$2^k F_n + bL_n \bmod 8$	6	7	5	4	1	5	6	3	1	4	5	1

Again, the concern is only for $n \equiv 3 \bmod 6$. Here it is observable that $2^k F_n + bL_n$ is not equivalent to 0 mod 8. So $\nu_2(2^k F_n + bL_n) \leq 2$ for all n. Thus the formula for $\nu_2(2^k F_n + bL_n)$ holds.

□

Theorem 4.2. *For $a \in \mathbb{Z}$,*

$$\nu_2(aF_n + 2L_n) = \begin{cases} \nu_2(L_n) + 1 & a \equiv 0 \bmod 8 \\ \nu_2(L_{n+3}) & a \equiv 1 \bmod 2 \\ \nu_2(L_{n+1}) + 2 & a \equiv 10 \bmod 32 \\ \nu_2(bL_{n+2}) + 2 & a \equiv 14 \bmod 32 \\ \nu_2(L_{n+4}) + 2 & a \equiv 18 \bmod 32 \\ \nu_2(L_{n+5}) + 2 & a \equiv 22 \bmod 32. \end{cases}$$

Note that for $a \equiv 2, 4, 6, 12, 20, 24, 26, 28,$ or $30 \bmod 32$, $\nu_2(aF_n + 2L_n)$ is indeterminate, and must be evaluated on a case-by-case basis.

Example 4.3. Taking $a = 3$, it follows that $\nu_2(3F_n + 2L_n) = \nu_2(L_{n+3})$.

Example 4.4. Taking $a = 10$, it follows that $\nu_2(10F_n + 2L_n) = \nu_2(4L_{n+1})$.

Example 4.5. Taking $a = 2$, it follows from Corollary 2.4 that

$$\nu_2(aF_n + 2L_n) = \nu_2(2F_n + 2L_n) = \nu_2(4F_{n+1}) = \nu_2(F_{n+1}) + 2.$$

Theorem 4.6. *For $b \in \mathbb{Z}$,*

$$\nu_2(F_n + bL_n) = \begin{cases} \nu_2(L_{n+3}) & b \equiv 2 \bmod 4 \\ \nu_2(L_{n-1}) + 1 & b \equiv 3 \bmod 16 \\ \nu_2(L_{n-2}) + 1 & b \equiv 9 \bmod 16 \\ \nu_2(L_{n+2}) + 1 & b \equiv 7 \bmod 16 \\ \nu_2(L_{n+1}) + 1 & b \equiv 13 \bmod 16. \end{cases}$$

This theorem partially characterizes the 2-adic valuations of generalized Fibonacci sequences of the form $F_n + bL_n$. These particular values for b were chosen because they reveal an explicit formula. All of these formulas are related to $\nu_2(L_n)$. We suspect that the other values of b mod 16 will have explicit formulas related to $\nu_2(F_n)$ but it could not be determined in general.

5 3-adic Valuations

Some results from the specific case $S_n = F_n + 2L_n$ have been simple to extend to all generalized Fibonacci sequences f_n, and are presented as such.

Theorem 5.1. *There does not exist a generalized Fibonacci sequence f_n such that $\nu_3(f_n) = 0$ for all n.*

Proof. We begin by reducing $f_n = aF_n + bL_n$ modulo 3.

Note $L_2 = 3$, so if $a \equiv 0 \bmod 3$, the proof is complete.

If $b \equiv 0 \bmod 3$, then the proof is complete, as it is well-known that every natural number is a factor of some Fibonacci number.

We are now left with 4 cases, in particular $(a, b) = (1, 1), (1, 2), (2, 1),$ and $(2, 2)$.

$$(1, 1) \text{ and } (2, 1) : F_3 + L_3 = 2 + 4 = 6.$$

$$(1, 2) \text{ and } (2, 1) : F_1 + 2L_1 = 1 + 2 = 3.$$

□

Given Lengyel's formulas for $\nu_p(F_n)$ and $\nu_p(L_n)$, similar behavior is expected from the sequence $\nu_p(S_n)$, and so we look at it in relation to $\nu_p(n)$. Curiously, there are too many zero terms between the non-zero terms, and so remove remove them as follows.

Definition 5.2. For simplicity, we define $\{\nu_p^*(S_l)\} = \{\nu_p(S_n) \mid \nu_p(S_n) \neq 0\}$. Similarly, $\{\nu_p^*(l)\} = \{\nu_p(n) \mid \nu_p(n) \neq 0\}$.

Example 5.3. The case for $p = 3$: $\nu_3(S_n) \neq 0$ for $n \equiv 1 \bmod 4$, which can be see by examining the period modulo 4 and noticing that the only zero terms in $\nu_3(S_n) \bmod 4$ are when $n \equiv 1 \bmod 4$, and so the sequence $\{\nu_3^*(S_l)\}$ consists of every term in $\{\nu_3(S_n)\}$ where the index is congruent to 1 modulo 4.

Comparing the graphs of $\nu_3^*(S_l)$ and $\nu_3^*(l)$ it becomes evident that the latter is a shifted version of the former, up to some degree of accuracy.

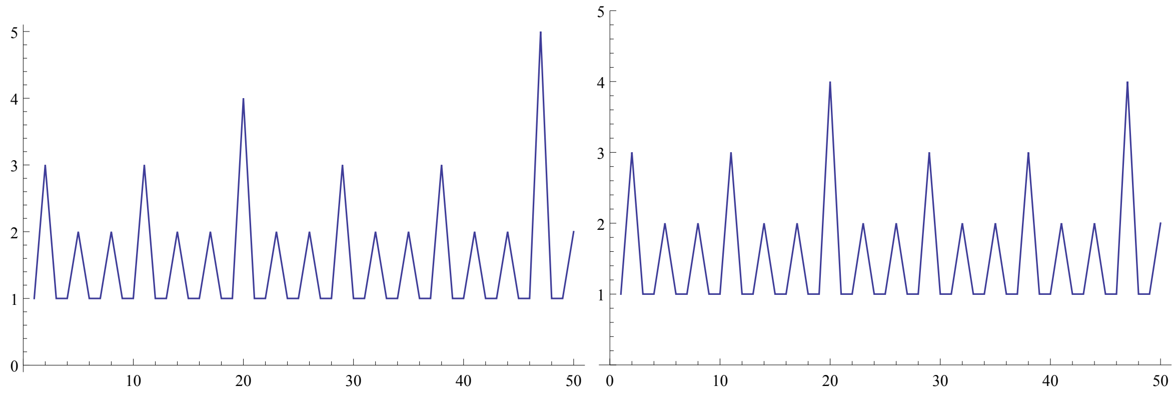


Figure 1: On the left, the first 50 terms of the sequence $\{\nu_3^*(S_l)\}$. On the right, the first 50 terms of the sequence $\{\nu_3^*(l + 23)\}$.

Notice that both of the preceding graphs are precisely equal, except for the 47^{th} term, which is off by 1. More factors can be found that yield increasingly higher accuracy, the first few of which, ignoring multiplicity, are 23, 1805, 174578, 351725. Interestingly, 351725 is accurate up to at least the first 2 million terms in the sequence.

Conjecture 5.4. Fix a prime $p \neq 2$ such that $\nu_p(S_n) \neq 0$. Then, for all $m \in \mathbb{N}$, there exists some K_m such that $\nu_p^*(S_l) = \nu_p^*(l + K_m)$ for all $l \leq m$.

The base-3 expansions of those first terms mentioned are as follows:

$$\begin{aligned} 23 &= 212_3 \\ 1805 &= 2110212_3 \\ 174578 &= 22212110212_3 \\ 351725 &= 122212110212_3. \end{aligned}$$

These seem to be converging to some 3-adic number.

Now considering shifting factors that return the same accuracy, it can be seen that the numbers 23, 104, and 266 all share an accuracy of 46 non-zero terms. Considering all shifting factors that return an accuracy of at least 46 non-zero terms, we see that there appears to be trend in how accurate a particular shifting factor is.

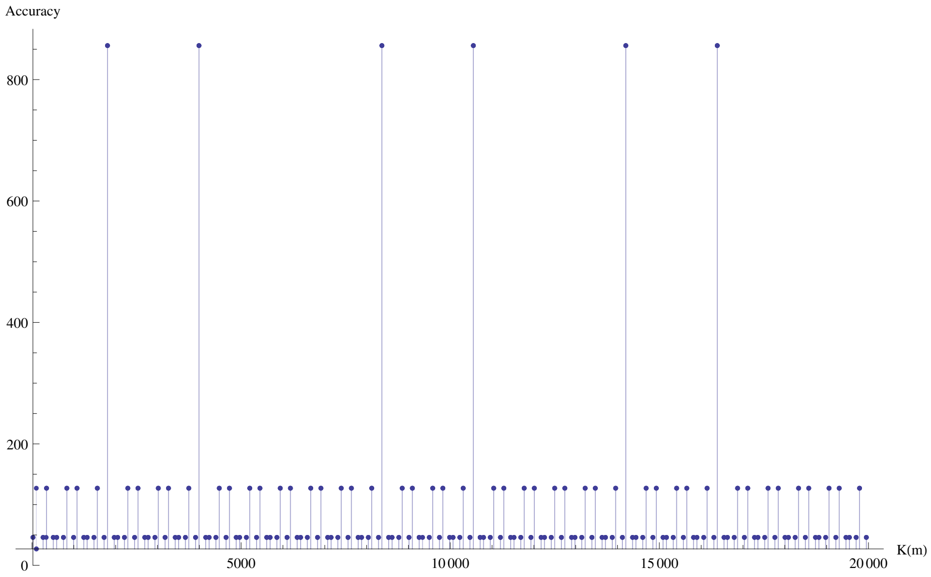


Figure 2: Here we mark the x-axis with the shifting factors of the generalized Fibonacci sequence $F_n + 2L_n$, while the y-axis denotes the accuracy of the shift.

In the figure above, it becomes clear that all shifting factors between 0 and 20,000 repeat the same accuracies, namely 46, 127, and 870. Note that beyond 20,000, these numbers continue to show a similar pattern (differing only by a slow growth), but become increasingly more difficult to compute. Though the idea has not undergone much testing, this trend contributes to the belief that the values of K_m can be determined using a closed-form formula.

Conjecture 5.5. Consider the sequence $\{K_m\}$. If $p = 3$, then $K_m \to c$, where c is some 3-adic number, as $m \to \infty$.

This begs the question: why is 3 special? This leads into the next conjecture.

Conjecture 5.6. (1) Existence of n_i

For all natural numbers i, there exists an n_i such that $3^i \mid S_{n_i}$.

(2) Convergence under 3-adic Metric

$n_i \to \gamma$ as $i \to \infty$ for some 3-adic number γ.

Attempted proofs for Conjecture 5.6 are as follows.

5.6.1 Binet's formulas for F_n and L_n:

Binet's formulas are as follows:

$$F_n = \frac{\varphi^n - (-\varphi)^{-n}}{\sqrt{5}} \text{ and } L_n = \varphi^n + (-\varphi^{-n}), \text{where } \varphi = \frac{1+\sqrt{5}}{2}.$$

We show that $\sqrt{5} \notin \mathbb{Q}_3$.

First, if $\sqrt{5}$ was in $\mathbb{Z}_3$, then $x^2 \equiv 5 \equiv 2 \bmod 3$. Consideration of $x \equiv 0, 1, 2 \bmod 3$ shows that there are no solutions. So, $\sqrt{5} \notin \mathbb{Z}_3$.

Now, if it were an element of $\mathbb{Q}_3$, then one would see $\nu_3(x^2) = 2\nu_3(x) < 0$. However, notice that $\nu_3(x^2) = \nu_3(5) = 0$, thus providing a contradiction.

As such, Binet's formulas could not be used since there was no ability to discuss $\frac{1+\sqrt{5}}{2}$.

5.6.2 Periods of F_n and L_n Modulo 3^i:

It is known that F_n and L_n are periodic modulo m for any integer m. The goal was to find an index n_i such that $F_n + 2L_n \equiv 0 \bmod 3^i$ for any i, which is equivalent to saying $\{n_i\}$ exists. However, the index where the linear combination yielded a zero modulo powers of 3 could not be determined. Therefore it was not definitive that there exists zeros of $F_n + 2L_n \bmod 3^i$.

5.6.3 The Identity $L_n = F_n + 2F_{n-1}$:

Using the well-known formula above, we have

$$\begin{aligned} S_n &= F_n + 2L_n \\ &= F_n + 2(F_{n+1} + F_{n-1}) \\ &= F_n + 2(F_n + F_{n-1} + F_{n-1}) \\ &= 3F_n + 4F_{n-1}. \end{aligned}$$

Taking the 3-adic valuation of both sides yields

$$\begin{aligned} \nu_3(S_n) &= \nu_3(3F_n + 4F_{n-1}) \\ &= \min(\nu_3(F_n) + 1, \nu_3(F_{n-1})) \text{ if } \nu_3(F_n) + 1 \neq \nu_3(F_{n-1}). \end{aligned}$$

It is well-known that any 3 consecutive Fibonacci numbers are pairwise coprime, and so it is clear that if $3 \mid F_n$, then $3 \nmid 4F_{n-1}$, and thus one can only show that there exist indices such that $\nu_3(S_n) = 0$.

Theorem 5.7. *If the sequence $\{n_i\}$ exists and converges to some 3-adic number γ, then $S_\gamma = 0$ in the 3-adics.*

Proof. By definition, S_γ is infinitely divisible by 3, which is precisely 0 in the 3-adics. □

Theorem 5.8. *Suppose that sequences $\{n_j\}$ and $\{n_k\}$ exist where n_j is the first index such that $3^j \mid S_{n_j}$, and n_k is the first index such that $\nu_3(S_{n_k}) \geq k$. Both of these sequences converge to the same limit as $\{n_i\}$, some 3-adic number γ.*

Proof. It is clear that in the limiting case, both S_{n_j} and S_{n_k} are infinitely divisible by 3. Thus, in the 3-adics, they are equivalent to 0, and thus it is clear that they must also converge to γ. □

Theorem 5.9. *Suppose that one can always find a shifting factor K_m for $p = 3$, then the sequence n_i exists and converges to γ.*

Proof. It is clear that $\nu_3^*(n)$ can be made arbitrarily large by considering powers of 3. So, by considering terms $n = 3^j - K_m$, notice that $\nu_3^*(S_n) = j$ for some arbitrary j. However, $\nu_3^*(S_n)$ is just the removal of the zero terms from $\nu_3(S_n)$, and so $\nu_3(S_n)$ can clearly be made arbitrarily large, and thus, by Theorem 5.8, the proof is complete. □

6 Prime Characterizations

It is well-known that no Lucas number is divisible by 5, and so $\nu_5(L_n) = 0$. Primes that return a p-adic valuation for the sequence $S_n = F_n + 2L_n$ can also be found, and a partial list is as follows.

Theorem 6.1. *If* $p \in \{13, 19, 29, 37, 41, 47, 53, 61, 89, 97, 107\}$*, then* $\nu_p(S_n) = 0$.

Proof. For all $p \in \{13, 19, 29, 37, 41, 47, 53, 61, 89, 97, 107\}$, $S_n \bmod p$ is periodic with period according to the following table.

p	13	19	29	37	41	47	53	61	89	97	107
$\pi(p)$	28	18	14	76	40	32	108	60	44	196	72

Calculating $\nu_p(S_n)$ up to $n = \pi(p)$ shows that because none of the terms are 0, $\nu_p(S_n) \leq 0$, and thus $\nu_p(S_n) = 0$. □

What remains curious are the primes that always return a p-adic valuation of 0. Checking first few terms in the On-Line Encyclopedia of Integer Sequences (OEIS) [5], it became clear that those primes had a particularly interesting property: either $5^q p \pm 6$ was prime for some q, or $p = 5^q p_0 \pm 6$ for some q and some other prime p_0.

However, it became clear that this seemed to be true for any prime p, which leads to the following conjecture.

Conjecture 6.2. If $p \geq 5$ is prime, then at least one of the following holds for some $q \in \mathbb{N}$.

1. At least one of $5p^q \pm 6$ is prime, or
2. p is of the form $p = 5p_0^q \pm 6$ for some other prime p_0.

This has been tested for the first 10 million primes. Curiously, most of the exponents q are quite small, indeed less than 10. Only few, comparatively, require exponents much higher.

It appears as though this can be extended to the following:

Conjecture 6.3. Given primes p_0 and $\tilde{p}$ such that $\tilde{p} \pm 1$ and p_0 are relatively prime, so $(\tilde{p} \pm 1, p_0) = 1$, then there exists some integer $q \geq 0$ such that

$$\tilde{p}^q p_0 \pm (\tilde{p} \pm 1)$$

is prime. Furthermore, every prime can be expressed in this form for some p_0 and $\tilde{p}$.

7 Completeness of Lucas Numbers

Are there any natural numbers which cannot be expressed in terms of Lucas numbers? If we were to allow multiplicity, then the statement is trivial, as 1 is a Lucas number. What happens if this is disallowed? Brown [2] provides information on sequences which can be used to express every natural number in a non-trivial manner.

Definition 7.1. A sequence $\{b_n\}$ is *complete* if every natural number can be expressed by summing the terms of a subsequence $\{b_{n_i}\}$. That is,

$$k = \sum_{i=0}^{\infty} \delta_i b_i,$$

where $\delta_i = 0$ or 1.

Theorem 7.2 (Brown). *Without loss of generality, assumed the sequence $\{a_n\}$ is nondecreasing. $\{a_n\}$ is complete if, and only if, the following criteria are met:*

1. $a_0 = 1$

2. *The partial sums $s_{k-1} \geq a_k + 1$ for all $k \geq 1$, where $k \in \mathbb{N}$*

Corollary 7.3 (Brown). *If $a_0 = 1$ and $2a_n \geq a_{n+1}$ for all $n \geq 1$, where $n \in \mathbb{N}$, then the sequence $\{a_n\}$ is complete.*

Theorem 7.4. *The Lucas numbers, L_n, are complete.*

Proof. Let $\{L'_n\}$ be the set of Lucas numbers arranged in nondecreasing order. In this case, we can define $L'_n = L'_{n-1} + L'_{n-2}$ for all natural numbers $n \geq 4$.

The first requirement of Corollary 7.3 is clearly true, and so the only trouble is the second requirement. The first cases where the recurrence does not hold follow as such:

$$2L'_0 = 2 = L'_1$$
$$2L'_1 = 4 \geq 3 = L'_2$$
$$2L'_2 = 6 \geq 4 = L'_3.$$

Now, given any natural number $k \geq 4$, it is clear that $L'_k \geq L'_{k-1}$. It follows that

$$L_k \geq L_{k-1}$$
$$2L_k \geq L_{k-1} + L_k$$
$$2L_k \geq L_{k+1}.$$

This, together with the first cases where the recurrence does not hold, proves that the second requirement is satisfied. Now, this shows that $\{L'_n\}$ is complete. However, the ordering on the set does not affect the completeness, and thus it follows that $\{L_n\}$ is complete. □

We have shown that every natural number can be represented by the Lucas numbers, but is there anything interesting about those representations? For the Fibonacci numbers, Zeckendorf [8] was able to provide a characterization of the representations for the Fibonacci sequence.

Theorem 7.5 (Zeckendorf). *Any natural number has a unique representation of the form*

$$n = \sum_{i=0}^{\infty} \varepsilon_i F_i,$$

where $\varepsilon_i = 0$ or 1, and $\varepsilon_i \varepsilon_{i+1} = 0$.

It was later shown by Daykin [4] that the Zeckendorf represenation was also a characterization of the Fibonacci sequence.

Theorem 7.6 (Daykin). *If $\{a_n\}$ is a sequence with unique Zeckendorf representations, then $\{a_n\}$ is strictly increasing and $\{a_n\} = \{F_n\}$.*

What has yet to be seen is whether or not there is a Zeckendorf representation in the Lucas numbers. The proof that these representations do exist follows similarly to the proof of Zeckendorf's Theorem given in [3].

Theorem 7.7. *Every natural number n has a Zeckendorf representation in the Lucas numbers.*

Proof. We proceed by induction. If $n = 1, 2, 3$, or 4, then the representation is clear, as those are all Lucas Numbers. Now, take $k = 5$. Then we have

$$n = 5 = 1 + 4 = L_1 + L_3.$$

Suppose that every natural number $n \leq k$ has a Zeckendorf representation.

Now, for $n = k + 1$, we have two possibilities.

Case 1: If $k + 1$ is a Lucas number, then the proof is complete.

Case 2: If $k + 1$ is not a Lucas number, then there exists some j such that $L_k < k + 1 < L_{j+1}$. Consider $a = k + 1 - L_j$. Because $a < k$, a has a Zeckendorf representation in the Lucas numbers.

$$L_j + a = k + 1$$

$$L_j + a < L_j + L_{j-1}$$

$$a < L_{j-1}.$$

From this, it is clear that the Zeckendorf representation of a in the Lucas numbers does not contain L_{j-1}. As such, the Zeckendorf representation of $k + 1$ is the representation of a in the Lucas numbers plus L_j. Thus, every natural number has a Zeckendorf represenation in the Lucas numbers. □

It is clear from Theorem 7.6 that despite the fact that there is a Zeckendorf representation in the Lucas numbers, it won't be unique. For example, we could take $12 = L_1 + L_5 = L_0 + L_2 + L_4$.

Furthermore, there is no Zeckendorf representation for generalized Fibonacci sequences as we could take $(f_0, f_1) = (1, 3)$, and thus there is no representation of 2.

8 Acknowledgments

This work was carried out during the 2014 Mathematical Sciences Research Institute Undergraduate Program (MSRI-UP) which is funded by the National Science Foundation (grant No. DMS-1156499) and the National Security Agency (grant No. H-98230-13-1-0262).

We would like to thank Dr. Herbert Medina, Dr. Victor Moll, Dr. Eric Rowland, and Asia Wyatt for their invaluable help with our research and work. The first author would like to thank Dr. Scott Annin from California State University Fullerton for the inspiration, knowledge, and support he has provided. The second author would like to thank Dr. Eric Weber from Iowa State University for providing mentorship and support during the author's undergraduate career. The third author would like to thank Dr. Baoping Liu from the University of Chicago for his unyielding support and excellent tutelage.

References

[1] D. M. Bloom, "On Periodicity in Generalized Fibonacci Sequences," *Amer. Math. Monthly* **72** (1965) 557–560.

[2] J. L. Brown, Jr., "Note on Complete Sequences of Integers," *Amer. Math. Monthly* **68** (1961) 243-252

[3] J. L. Brown, Jr., "Zeckendorf's Theorem and Some Applications," *Fibonacci Quart.* **6** (1964) 163–168

[4] D. E. Daykin, "Representation of Natural Numbers as Sums of Generalized Fibonacci Numbers," *J. Lond. Math. Soc.* **35** (1960) 143–160

[5] OEIS Foundation Inc. (2011), The On-Line Encyclopedia of Integer Sequences, `https://oeis.org/A023219`

[6] T. Lengyel, "The Order of the Fibonacci and Lucas Numbers," *Fibonacci Quart.* **33** (1995) 234–239.

[7] D. D. Wall, "Fibonacci Series Modulo m," *Amer. Math. Monthly* **67** (1960) 525–532.

[8] E. Zeckendorf, "Représentation des nombres naturels par une somme des nombres de Fibonacci ou de nombres de Lucas," *Bull. Soc. Roy. Sci. Liège* **41** (1972) 179–182

On p-adic limits of subsequences of the Catalan numbers

Alexandra Michel **Andrew Miller** **Joseph Rennie**

Mills College Amherst College Reed College

August 2014

Abstract

Methods for determining p-adic convergence of sequences which are expressible in terms of products of factorials are established. The Catalan sequence is investigated, using these methods, for p-adically convergent subsequences. An infinite class of convergent subsequences of Catalan numbers is found for every prime, and the limits of these subsequences are evaluated.

1 Introduction

1.1 The p-adic numbers

A student familiar with introductory analysis will be familiar with the construction of $\mathbb{R}$ as a completion of $\mathbb{Q}$. In this construction of $\mathbb{R}$, its elements are defined as equivalence classes of sequences in $\mathbb{Q}$ which are Cauchy convergent with respect to the familiar Euclidean distance metric.

The *p-adic field*, denoted $\mathbb{Q}_p$, is a second completion of $\mathbb{Q}$. Instead of the familiar Euclidean metric, it uses a metric induced by the *p-adic norm*.

Definition 1.1. The *p-adic valuation* of an integer n, denoted $\nu_p(n)$, is defined to be the greatest power of p that divides n. For a rational number $x = \frac{a}{b}$, define $\nu_p(x) = \nu_p(|a|) - \nu_p(|b|)$. The *p-adic norm* of x is defined as $|x|_p = p^{-\nu_p(x)}$.

Example 1.2. $\nu_5(35) = 1$, because only one power of 5 divides 35, and $|35|_5 = 5^{-\nu_5(35)} = 5^{-1} = \frac{1}{5}$. $\nu_5(25) = 2$, so $|25|_5 = 5^{-\nu_5(25)} = 5^{-2} = \frac{1}{25}$.

The p-adic metric is defined as the p-adic norm of the difference of two numbers in $\mathbb{Q}_p$. As noted, the completion of $\mathbb{Q}$ under the p-adic metric yields $\mathbb{Q}_p$. A detailed account of the completion of $\mathbb{Q}$ to $\mathbb{Q}_p$ can be found in [FG].

1.2 Convergence in $\mathbb{Z}_p$

The definition of p-adic convergence is analogous to that of convergence with respect to the Euclidean metric.

Definition 1.3 (p-adic Convergence)**.** Given a sequence $\{a_n\} \in \mathbb{Q}_p$, we say that $\{a_n\}$ *converges p-adically* if for all $k \geq 1$, there exists an $N \in \mathbb{N}$ such that for all m, $n > N$,

$$|a_m - a_n|_p \leq p^{-k}.$$

Example 1.4. In $\mathbb{Q}_p$, $\lim\limits_{n\to\infty} p^n = 0$. This is because as n increases, $\nu_p(p^n) = n$ increases, and thus $|p^n|_p = p^{-n}$ tends to 0.

The sequence $\{p^n + 1\}$, however, tends to 1. This is because $\nu_p(p^n + 1) = 0$ for all n, and thus for all n, $|p^n + 1|_p = p^0 = 1$.

Because elements of combinatorial sequences are natural numbers, to investigate the convergence of the sequences it is superfluous to work in $\mathbb{Q}_p$. Instead, one need only work in the completion of $\mathbb{Z}$ under the p-adic metric; this is a subset of $\mathbb{Q}_p$ called the *p-adic integers* (denoted $\mathbb{Z}_p$). It is well-known that $\mathbb{Z}_p$ is a compact subset of $\mathbb{Q}_p$, which is itself a metric space. Thus, every combinatorial sequence has convergent subsequences in $\mathbb{Z}_p$.

Investigating the convergence of these subsequences with respect to the p-adic metric has a few important advantages. The most important of these is that the p-adic metric satisfies a strong-triangle inequality.

Proposition 1.5 (Strong Triangle Inequality)**.** *For all x, $y \in \mathbb{Q}_p$,*

$$|x - y|_p \leq \max\{|x|_p, |y|_p\}.$$

Using the strong triangle inequality, it can be shown that a sequence converges p-adically if and only if its difference sequence converges.

Proposition 1.6 (Convergence Criterion). *In $\mathbb{Q}_p$, a sequence $\{a_n\}$ converges if and only if the sequence $\{a_{n+1} - a_n\}$ converges.*

For proofs of Proposition 1.5 and Proposition 1.6, see [FG] or [SK].

Finally, we note an equivalent statement of the definition of p-adic convergence.

Proposition 1.7 (Equivalent Definition of p-adic Convergence). *In $\mathbb{Q}_p$, a sequence $\{a_n\}$ converges if and only if for all $k \geq 1$, it is eventually constant modulo p^k. Furthermore, $\{a_n\}$ converges to a limit L if and only if for all $k \geq 1$, it is eventually constant to L modulo p^k.*

Proof. Given $k \geq 1$ and sufficiently large m and n,

$$\begin{aligned} |f(n) - f(m)|_p \leq p^{-k} \quad &\text{if and only if} \quad \nu_p(f(n) - f(m)) \geq k \\ &\text{if and only if} \quad f(n) - f(m) \equiv 0 \pmod{p^k} \\ &\text{if and only if} \quad f(n) \equiv f(m) \pmod{p^k}, \end{aligned}$$

proving the first statement of Proposition 1.7. The proof of the second statement is almost identical. □

Note that it is easy to see that $p^n \to 0$ using Proposition 1.7. Given $k \geq 1$, for all $n > k$, $p^n \equiv 0 \pmod{p^k}$.

1.3 Catalan Numbers

This paper finds p-adic limits of subsequences of the Catalan numbers, C(n). The Catalan numbers are a famous sequence of natural numbers with numerous combinatorial interpretations. For example, they count the number of ways to balance n pairs of parentheses (i.e., such that each open parathesis is closed and each closed parenthesis is opened). For example, 3 pairs of paretheses can be arranged in the following ways.

$$((())),\ ()()(),\ (())(),\ ()(()),\ (()()).$$

Thus, $C(3) = 5$.

The Catalan numbers have a convenient closed form in terms of the central binomial coefficients:

$$C(n) = \frac{1}{n+1}\binom{2n}{n}.$$

We can use this formula to check that $C(3)$ is indeed 5.

$$C(3) = \frac{1}{4}\binom{2\cdot 3}{3} = \frac{6!}{4\cdot 3!^2} = \frac{5\cdot 6}{3!} = 5.$$

Finally, the closed form can be used to derive a recurrence for consecutive Catalan numbers.

$$C(x+1) = \frac{2(2x+1)}{x+2}C(x).$$

2 Finding the p-adic Limit of $C(ap^n)$

In this section,

$$\lim_{n\to\infty} C(ap^n)$$

is determined for all $a \in \mathbb{N}$.[1]

Example 2.1. Data generated in Mathematica suggest that $\{C(2^n)\}$ converges. The following graphic shows the binary expansion of $C(2^n)$ for $n = 1, 2, \ldots, 25$. The i^{th} row and j^{th} column gives the coefficient on 2^{j-1} of $C(2^i)$. Coefficients with value 1 are represented by a black dot, those with value 0 by a white dot.

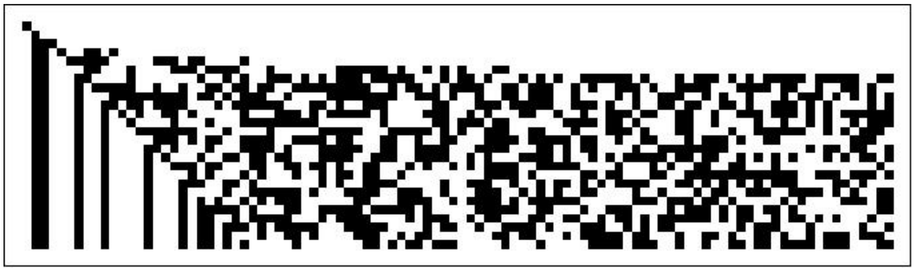


Figure 1: Binary expansions of the first 25 terms of the sequence $C(2^n)$; the power of 2 increases from left to right.

For example, the first row shows the binary representation of $C(1) = 1$. In binary, $1 = 1 + 0\cdot 2 + 0\cdot 2^2 + \cdots$. The coefficient 1 on 2^0 is represented by the black dot in the first

[1] This limit is a p-adic limit, as are all other limits stated in this paper.

column, and the 0 coefficients on the remaining powers of 2 are represented by white dots in the remaining columns.

It is perhaps easiest to see why Figure 1 suggests that $\{C(2^n)\}$ converges by appealing to Proposition 1.6. The binary expansion of $C(2^n) - C(2^{n-1})$ can be obtained by subtracting the $n-1^{st}$ row from the n^{th} row. The resulting binary expansion has a 0 coefficient for all powers of 2 for which the coefficient of $C(2^n)$ agrees with that of $C(2^{n-1})$. As n increases, Figure 1 indicates that the binary expansion of $C(2^n) - C(2^{n-1})$ has a 0 coefficient for an increasingly long string of powers of 2 (starting with 2^0). This indicates that the 2-adic valuation of $C(2^n)-C(2^{n-1})$ is increasing with n, and thus that $|C(2^n)-C(2^{n-1})|$ is tending to 0.

For general a and p, to find the limit of $\{C(ap^n)\}$ it suffices to find the limit of $\{\binom{2ap^n}{ap^n}\}$. This is demonstrated by the following lemma.

Lemma 2.2. *In $\mathbb{Z}_p$, $\lim\limits_{n\to\infty} C(ap^n) = \lim\limits_{n\to\infty} \binom{2ap^n}{ap^n}$.*

Proof. Let $k \geq 1$ be arbitrary. Given $n > k$, note that

$$\left|\frac{1}{ap^n+1}\binom{2ap^n}{ap^n} - \binom{2ap^n}{ap^n}\right|_p < p^{-k} \text{ if and only if } \nu_p\left[\frac{1}{ap^n+1}\binom{2ap^n}{ap^n} - \binom{2ap^n}{ap^n}\right] > k,$$

so it suffices to show the latter. We have

$$\begin{aligned}\nu_p\left[\frac{1}{ap^n+1}\binom{2ap^n}{ap^n} - \binom{2ap^n}{ap^n}\right] &= \nu_p\left[\left(\frac{1}{ap^n+1} - 1\right)\binom{2ap^n}{ap^n}\right] \\ &= \nu_p\left(\frac{ap^n}{ap^n+1}\right) + \nu_p\left[\binom{2ap^n}{ap^n}\right] \\ &\geq n > k,\end{aligned}$$

as desired. □

Thus, the problem of finding the limit of $\{C(ap^n)\}$ can be reduced to that of finding the limit of the sequence of central binomial coefficients $\{\binom{2ap^n}{ap^n}\}$. The elements of this latter sequence can be expressed in terms of the well-known gamma function. On $\mathbb{Z}$, the gamma function is defined to be

$$\Gamma(n) = (n-1)!.$$

We can thus write

$$\binom{2ap^n}{ap^n} = \frac{\Gamma(2ap^n+1)}{(\Gamma(ap^n+1))^2}.$$

But since we are concerned with convergence in $\mathbb{Z}_p$, it will be more useful to write $\binom{2ap^n}{ap^n}$ in terms of a p-adic analog to the gamma function.

Definition 2.3 (p-adic Gamma Function)**.** Let p be prime, and $x \in \mathbb{Z}_p$. The *p-adic gamma function*, $\Gamma_p(x)$, is defined to be the unique continuous p-adic interpolation of the function taking the following values over $\mathbb{N}$.

$$\Gamma_p(n) = (-1)^n \prod_{\substack{k=1 \\ p\nmid k}}^{n-1} k \ \text{ , and } \ \Gamma_p(0) = 1.$$

For a detailed exposition of the p-adic gamma function, including a proof of its existence and uniqueness, see [FG]. The following proposition can be used to prove Lemma 2.5, which expresses $\binom{2ap^n}{ap^n}$ in terms of the p-adic gamma function.

Proposition 2.4. *For all primes p and all $n \in \mathbb{N}$,*

$$n! = \left\lfloor \frac{n}{p} \right\rfloor ! \Gamma_p(n+1)(-1)^{n+1} p^{\left\lfloor \frac{n}{p} \right\rfloor}.$$

Proof. We have

$$\Gamma_p(n+1) = (-1)^{n+1} \prod_{\substack{k=1 \\ p\nmid k}}^{n} k = \frac{(-1)^{n+1}(n)!}{\prod\limits_{\substack{k=1 \\ p|k}}^{n-1} k} = \frac{(-1)^{n+1}(n)!}{p^{\left\lfloor \frac{n}{p} \right\rfloor} \left\lfloor \frac{n}{p} \right\rfloor !}.$$

Solving for $n!$ gives the result. □

Lemma 2.5. *For all primes p and all $a \in \mathbb{N}$,*

$$\binom{2ap^n}{ap^n} = \binom{2a}{a} \prod_{i=1}^{n} \frac{\Gamma_p(2ap^i)}{\Gamma_p(ap^i)^2}.$$

Proof. We first use Proposition 2.4 to express $(ap^n)!$ which gives

$$(ap^n)! = (ap^{n-1})! \Gamma_p(ap^n+1)(-1)^{ap^n+1} p^{ap^{n-1}}. \tag{2.1}$$

This is a first-order recursion on n. It can be used to show via induction that

$$(ap^n)! = a! p^{\frac{ap^n-a}{p-1}} (-1)^{\sum_{i=1}^{n} ap^i+1} \prod_{i=1}^{n} \Gamma_p(ap^i+1). \tag{2.2}$$

For the base case ($n = 0$), we have $(ap^0)! = a! = a!p^0$.

For the inductive step, assume that Equation 2.2 holds when $n = k$. Then

$$\begin{aligned}(ap^{k+1})! &= (ap^k)!\Gamma_p(ap^{k+1}+1)(-1)^{ap^{k+1}+1}p^{ap^k}\\ &= \left[a!p^{\frac{ap^k-a}{p-1}}(-1)^{\sum_{i=1}^{k} ap^i+1}\prod_{i=1}^{k}\Gamma_p(ap^i+1)\right]\Gamma_p(ap^{k+1}+1)(-1)^{ap^{k+1}+1}p^{ap^k}\\ &= a!p^{\frac{ap^{k+1}-a}{p-1}}(-1)^{\sum_{i=1}^{k+1} ap^i+1}\prod_{i=1}^{k+1}\Gamma_p(ap^i+1),\end{aligned}$$

completing the induction and proving that Equation 2.2 holds for all n. It can thus be shown that

$$\binom{2ap^n}{ap^n} = \frac{(2ap^n)!}{(ap^n)!^2} = \frac{(2a)!(-1)^n}{(a!)^2}\prod_{i=1}^{n}\frac{\Gamma_p(2ap^i+1)}{\Gamma_p(ap^i+1)^2} = \binom{2a}{a}\prod_{i=1}^{n}\frac{\Gamma_p(2ap^i)}{\Gamma_p(ap^i)^2},$$

the desired result. □

Lemma 2.2 and Lemma 2.5 imply that

$$C(ap^n) \to \binom{2ap^n}{ap^n} \to \binom{2a}{a}\prod_{i=1}^{\infty}\frac{\Gamma_p(2ap^i)}{\Gamma_p(ap^i)^2}, \tag{2.3}$$

if the latter converges. To show this, one more lemma is needed.

Lemma 2.6. *Let p be prime and let $a \in \mathbb{N}$. In $\mathbb{Z}_p$, $\lim_{n\to\infty}\Gamma_p(ap^n) = 1$.*

Given Lemma 2.6, Equation 2.3, stated here as a theorem, can be proven.

Theorem 2.7 (Limits of Catalan Subsequences)**.** *For all primes p and all $a \in \mathbb{Z}$, the p-adic limit of $C(ap^n)$ exists and is given by*

$$\lim_{n\to\infty} C(ap^n) = \binom{2a}{a}\prod_{i=1}^{\infty}\frac{\Gamma_p(2ap^i)}{\Gamma_p(ap^i)^2}.$$

Note: An elementary proof that $\{C(ap^n)\}$ converges (not that it approaches the stated limit) is given in an Appendix (Section 6).

Proof of Theorem 2.7. By Lemma 2.2 and Lemma 2.5, it suffices to show that

$$\prod_{i=1}^{\infty}\frac{\Gamma_p(2ap^i)}{\Gamma_p(ap^i)^2}$$

converges.

To do so, fix $k \geq 1$, and let $n > k$ be arbitrary. Then

$$\begin{aligned}
\left| \prod_{i=1}^{n} \frac{\Gamma_p(2ap^i)}{\Gamma_p(ap^i)^2} - \prod_{i=1}^{n-1} \frac{\Gamma_p(2ap^i)}{\Gamma_p(ap^i)^2} \right|_p &= \left| \left(\prod_{i=1}^{n-1} \frac{\Gamma_p(2ap^i)}{\Gamma_p(ap^i)^2} \right) \left(\frac{\Gamma_p(2ap^n)}{\Gamma_p(ap^n)^2} - 1 \right) \right|_p \\
&= \left| \prod_{i=1}^{n-1} \frac{\Gamma_p(2ap^i)}{\Gamma_p(ap^i)^2} \right|_p \cdot \left| \frac{\Gamma_p(2ap^n)}{\Gamma_p(ap^n)^2} - 1 \right|_p \\
&= 1 \cdot \left| \frac{\Gamma_p(2ap^n)}{\Gamma_p(ap^n)^2} - 1 \right|_p \to 0,
\end{aligned}$$

where $\lim\limits_{n\to\infty} \left(\frac{\Gamma_p(2ap^n)}{\Gamma_p(ap^n)^2} - 1 \right) = 0$ because by Lemma 2.6, $\Gamma_p(2ap^n) \to 1$ and $\Gamma_p(ap^n) \to 1$. □

We conclude this section by proving Lemma 2.6.

Proof of Lemma 2.6. By Proposition 1.7, to prove Lemma 2.6 it thus suffices to prove that for all $k \geq 1$ and all sufficiently large n,

$$\Gamma_p(ap^n) \equiv 1 \pmod{p^k}. \tag{2.4}$$

To verfiy this, taking $n > k$ will suffice. For such n,[2]

$$\begin{aligned}
\Gamma_p(ap^n) &= (-1)^{ap^n} \left(\begin{array}{ccc} (1) & \cdots & (p^n - 1) \\ (p^n + 1) & \cdots & (2p^n - 1) \\ \vdots & & \\ ((a-1)p^n + 1) & \cdots & (ap^n - 1) \end{array} \right) \\
&\equiv (-1)^{ap^n} \left((1) \cdots (p^n - 1) \right)^a \pmod{p^k} \\
&= (-1)^{ap^n} \left(\begin{array}{ccc} (1) & \cdots & (p^k - 1) \\ (p^k + 1) & \cdots & (2p^k - 1) \\ \vdots & & \\ (p^{k+1} - p^k + 1) & \cdots & (p^{k+1} - 1) \\ (p^{k+1} + 1) & \cdots & (p^{k+1} + p^k - 1) \\ \vdots & & \\ (p^n - p^k + 1) & \cdots & (p^n - 1) \end{array} \right)^a \pmod{p^k}
\end{aligned}$$

[2] The arrays here are not matricies. Each row is a product, and the rows are being multiplied together. They are displayed in this way because it makes it easier to see what the terms of $\Gamma_p(ap^n)$ are equivalent to modulo p^k.

$$
\begin{aligned}
&\equiv (-1)^{ap^n}\big((1)\cdots(p^k-1)\big)^{ap^{n-k}} \pmod{p^k}\\
&\equiv (-1)^{ap^n}(p^k-1)^{ap^{n-k}} \equiv (-1)^{ap^n}(-1)^{ap^{n-k}} \equiv (-1)^{ap^{n-k}(1+p^k)} \equiv 1 \pmod{p^k}.
\end{aligned}
$$

The second to last equivalence is due to the fact that the factors of the product $(1)\cdots(p^k-1)$ are precisely the elements of the multiplication group $(\mathbb{Z}/p^k\mathbb{Z})^\times$. After multiplying inverses, p^k-1, which is its own inverse, remains. The last equivalence follows because either ap^{n-k} or $1+p^k$ is even. This proves Equation 2.4.

As was noted at the beginning of the proof, Equation 2.4 implies that for arbitrary k and all $n > k$,

$$\Gamma_p(ap^n) - 1 \equiv 0 \pmod{p^k},$$

so that

$$\nu_p(\Gamma_p(ap^n) - 1) \geq k,$$

and finally

$$|\Gamma_p(ap^n) - 1|_p \leq p^{-k}. \qquad \square$$

Example 2.8. This example demonstrates Lemma 2.6 for the case where $a = 1$ and $p = 2$. For an arbitrary $k \geq 1$ and $n > k$,

$$\Gamma_p(2^n) = (-1)^{2^n}(1)(3)\cdots(2^n-3)(2^n-1).$$

The power of (-1) clearly evaluates to 1. The remainder of the expression can be further expanded by writing

$$\Gamma_p(2^n) = \overbrace{(1)(3)\cdots(2^k-1)}\overbrace{(2^k+1)(2^k+3)\cdots(2^{k+1}-1)}\cdots\overbrace{(2^{n-1}+1)(2^{n+1}+3)\cdots(2^n-1)}.$$

As the braces indicate, the product can be divided into sections containing $\frac{2^k}{2} = 2^{k-1}$ terms. There are $\frac{2^n}{2^k} = 2^{n-k}$ such sections. The first is $(1)(3)\cdots(2^k-1)$, and the rest are all of the form

$$(2^l+1)(2^l+3)\cdots(2^{l+1}-1),$$

where l runs from k to $n-1$. Thus each section is equivalent to

$$(1)(3)\cdots(2^k-1) \pmod{2^k},$$

and we have that

$$\Gamma_p(2^n) \equiv \big((1)(3)\cdots(2^k-1)\big)^{2^{n-k}} \pmod{p^k}.$$

As noted in the proof of Lemma 2.6, the product $(1)(3)\cdots(2^k-1)$ contains precisely the elements of $(\mathbb{Z}/2^k\mathbb{Z})^\times$. Now

$$\big((1)(3)\cdots(2^k-1)\big)^2 \equiv 1 \pmod{p^k},$$

because when one copy of $(1)(3)\cdots(2^k-1)$ is multiplied by a second copy, every element of the group is multipled by its inverse, yielding 1. Thus, since in the expression for $\Gamma_p(2^n)$ the product $(1)(3)\cdots(2^k-1)$ is raised to a multiple of 2, we get that $\Gamma_p(2^n) \equiv 1 \pmod{p^k}$ for all $k \geq 1$ and all $n > k$. By Proposition 1.7, this implies that $\Gamma_p(2^n) \to 1$.

The next section uses the fact that $\lim\limits_{n\to\infty} C(ap^n)$ is known to find $\lim\limits_{n\to\infty} C(ap^n + r)$ for all $r \in \mathbb{Z}$.

3 Finding the Limit of $C(ap^n + r)$

Given that $\lim\limits_{n\to\infty} C(ap^n)$ is known, it is not hard to find $\lim\limits_{n\to\infty} C(ap^n + r)$ for all $r \in \mathbb{Z}$. The latter limit is thus presented as a corollary to Theorem 2.7.

Corollary 3.1. *Let $r \in \mathbb{Z}$ and let $L = \lim\limits_{n\to\infty} C(ap^n)$. Then*

$$\lim_{n\to\infty} C(ap^n + r) = \begin{cases} C(r)\cdot L & \textit{if } r > 0 \\ -\frac{1}{2}L & \textit{if } r = -1 \textit{ and } p \neq 2 \\ 0 & \textit{if } r < -1. \end{cases}$$

Proof. Each case will be proven using induction and the recurrence

$$C(x+1) = \frac{2(2x+1)}{x+2}C(x),$$

with the base case $C(0) = 1$. Begin with the $r > 0$ case. For the base case ($r = 1$), we have

$$C(ap^n + 1) \;=\; \frac{2(2ap^n+1)}{ap^n+2}C(ap^n) \to \frac{2}{2}\cdot L = C(1)\cdot L,$$

as desired.

For the inductive step, suppose that $C(ap^n + r) \to C(r) \cdot L$. Then

$$C(ap^n + r + 1) = \frac{2(2(ap^n + r) + 1)}{ap^n + r + 2} C(ap^n + r) \to \frac{2(2r + 1)}{r + 2} C(r) \cdot L = C(r + 1) \cdot L,$$

proving the $r > 0$ case.

For the cases for which $r < 0$, rewrite the recurrence as

$$C(x) = \frac{(x + 2)}{2(2x + 1)} C(x + 1).$$

If $r = -1$, then

$$C(ap^n - 1) = \frac{ap^n - 1 + 2}{2(2(ap^n - 1) + 1)} C(ap^n) = \frac{ap^n + 1}{4ap^n - 2} C(ap^n) \to -\frac{1}{2} \cdot L,$$

as desired.

For the base case of the $r < -1$ case, we have

$$C(ap^n - 2) = \frac{ap^n - 2 + 2}{2(2(ap^n - 2) + 1)} C(ap^n - 1) = \frac{ap^n}{4ap^n - 6} C(ap^n - 1) \to \frac{0}{-6} \cdot \frac{-1}{2} \cdot L = 0.$$

Now suppose that $C(ap^n - r) = 0$. Then for the inductive step,

$$C(ap^n - r - 1) = \frac{ap^n - r - 1 + 2}{2(2(ap^n - r - 1) + 1)} C(ap^n - r) = \frac{ap^n - r + 1}{4ap^n - 4r - 3} C(ap^n - r) \to \frac{r - 1}{4r + 3} \cdot 0 = 0,$$

completing the $r < -1$ case and proving the theorem. □

We note two interesting consequences of Corollary 3.1. First, since $\lim_{n\to\infty} \frac{C(ap^n + r)}{C(ap^n)} = C(r)$ even when $r < 0$, it suggests a definition of $C(n)$ for $n < 0$. Such a defintion would, for example, give $C(-1) = -1/2$.

Secondly, Corollary 3.1 implies that $C(n)$ does not converge p-adically. This is because for a fixed a we can choose distinct values of r that yield convergent subsequences with different limits.

Proposition 3.2. *For any prime p, $\{C(n)\}$ does not converge p-adically.*

Proof. Given a prime p, suppose that $\{C(n)\}$ converges p-adically. Then every infinite subsequence of $\{C(n)\}$ converges to the same limit. But consider the two subsequences $\{C(p^n + 1)\}$ and $\{C(p^n + 2)\}$. By Corollary 3.1,

$$\lim_{n\to\infty} \left(\frac{C(p^n + 1)}{C(p^n + 2)} \right) = \frac{C(1)}{C(2)} = \frac{1}{2} \neq 1,$$

contradicting that all subsequences of $\{C(n)\}$ approach the same limit. □

4 An Alternative Way of Stating the Limit of $C(ap^n)$

Theorem 2.7 showed that

$$\lim_{n\to\infty} C(ap^n) = \binom{2a}{a} \prod_{i=1}^{\infty} \frac{\Gamma_p(2ap^i)}{\Gamma_p(ap^i)^2}. \tag{4.1}$$

The goal of this section is to find a more illuminating expression of these limits. Hence, we arrive at the following proposition.

Proposition 4.1. *The limits in* (4.1) *can be written as*

$$\binom{2a}{a} \prod_{\substack{i=1 \\ p\nmid i}}^{\infty} i^{2\left\lfloor \log_p(i/a)\right\rfloor - \lfloor \log(i/2a)\rfloor}.$$

The proof of Proposition 4.1 requires a lemma similar to Lemma 2.6.

Lemma 4.2. *Let p be prime and let $a \in \mathbb{N}$. In $\mathbb{Z}_p$,*

$$\lim_{n\to\infty} (\Gamma_p(ap^n))^n = 1.$$

Proof. The proof of Lemma 2.6 showed that for all $k \geq 1$,

$$\Gamma_p(ap^n) \equiv (-1)^{ap^n}((1)\cdots(p^k-1))^{ap^{n-k}} \equiv 1 \pmod{p^k}.$$

Thus $(\Gamma_p(ap^n))^n \equiv 1^n \equiv 1 \pmod{p^k}$, so $(\Gamma_p(2ap^n)^n \to 1$, proving Lemma 4.2. □

Proposition 4.1 can now be proven.

Proof of Proposition 4.1. The goal is to prove that

$$\prod_{i=1}^{\infty} \frac{\Gamma_p(2ap^i)}{\Gamma_p(ap^i)^2} = \prod_{\substack{i=1 \\ p\nmid i}}^{\infty} i^{2\left\lfloor \log_p(i/a)\right\rfloor - \lfloor \log_p(i/2a)\rfloor}.$$

We have

$$\prod_{i=1}^{n} \frac{\Gamma_p(2ap^i)}{\Gamma_p(2ap^i)^2} = \frac{(1\cdots(2ap-1))^n((2ap+1)\cdots(2ap^2-1))^{n-1}\cdots((2ap^{n-1}+1)\cdots(2ap^n-1))}{[(1\cdots(ap-1))^n((ap+1)\cdots(ap^2-1))^{n-1}\cdots((ap^{n-1}+1)\cdots(ap^n-1))]^2}.$$

Factoring out a copy of each factor raised to n, we thus have

$$\left(\frac{\Gamma_p(2ap^n)}{\Gamma_p(ap^n)^2}\right)^n \frac{(1\cdots(2ap-1))^0((2ap+1)\cdots(2ap^2-1))^{-1}\cdots((2ap^{n-1}+1)\cdots(2ap^n-1))^{n-1}}{[(1\cdots(ap-1))^0((ap+1)\cdots(ap^2-1))^{-1}\cdots((ap^{n-1}+1)\cdots(ap^n-1))^{n-1}]^2}.$$

The factor on the right has a nice form as the product of coprime numbers raised to logarithmically increasing powers. The whole expression is written as follows.

$$
\begin{aligned}
\left(\frac{\Gamma_p(2ap^n)}{\Gamma_p(ap^n)^2}\right)^n \frac{\prod\limits_{\substack{i=1\\ p\nmid i}}^{ap^n-1}\left(i^{2\left\lfloor \log_p(i/a)\right\rfloor}\right)}{\prod\limits_{\substack{i=1\\ p\nmid i}}^{2ap^n-1}\left(i^{\left\lfloor \log_p(i/2a)\right\rfloor}\right)} &= \left(\frac{\Gamma_p(2ap^n)}{\Gamma_p(ap^n)^2}\right)^n \frac{\prod\limits_{\substack{i=1\\ p\nmid i}}^{ap^n-1}\left(i^{2\left\lfloor \log_p(i/a)\right\rfloor-\left\lfloor \log_p(i/2a)\right\rfloor}\right)}{\prod\limits_{\substack{i=ap^n+1\\ p\nmid i}}^{2ap^n-1}\left(i^{\left\lfloor \log_p(i/2a)\right\rfloor}\right)} \\
&= \left(\frac{\Gamma_p(2ap^n)}{\Gamma_p(ap^n)^2}\right)^n \frac{\prod\limits_{\substack{i=ap+1\\ p\nmid i}}^{ap^n-1}\left(i^{2\left\lfloor \log_p(i/a)\right\rfloor-\left\lfloor \log_p(i/2a)\right\rfloor}\right)}{\prod\limits_{\substack{i=ap^n+1\\ p\nmid i}}^{2ap^n-1}\left(i^{n-1}\right)} \\
&= \left(\frac{\Gamma_p(2ap^n)}{\Gamma_p(ap^n)^2}\right)^n \left(\frac{\Gamma_p(ap^n)}{\Gamma_p(2ap^n)}\right)^{n-1} \prod_{\substack{i=ap+1\\ p\nmid i}}^{ap^n-1}\left(i^{2\left\lfloor \log_p(i/a)\right\rfloor-\left\lfloor \log_p(i/2a)\right\rfloor}\right) \\
&= \left(\frac{\Gamma_p(2ap^n)}{\Gamma_p(ap^n)^{n+1}}\right) \prod_{\substack{i=ap+1\\ p\nmid i}}^{ap^n-1}\left(i^{2\left\lfloor \log_p(i/a)\right\rfloor-\left\lfloor \log_p(i/2a)\right\rfloor}\right).
\end{aligned}
$$

The result follows from Lemma 4.2 and Lemma 2.6. □

Using Proposition 4.1, $\lim\limits_{n\to\infty} C(2^n)$ (see Example 2.1) can be expressed nicely as a product numbers coprime to 2 raised to logarithmically increasing powers.

Example 4.3. In $\mathbb{Z}_p$, $\lim\limits_{n\to\infty} C(2^n) = 2\cdot 3\cdot (5\cdot 7)^2\cdot (9\cdot 11\cdot 13\cdot 15)^3\cdots$. This is an infinite product consisting of blocks of 2^n consecutive odd numbers raised to the $n+1^{st}$ power.

5 Conclusion

Combinatorial sequences, while they may not have limits, are integer sequences, and as such they have convergent subsequences by compactness of the p-adic integers. Sometimes the form of these limits can be difficult to characterize explicitly. In the case of the Catalan numbers, the sequence does not converge p-adically. However, we have an infinite class of increasing subsequences which have limits.

The limits of these subsequences appear to resist evaluation by any standard means (such as power series expansions, or continuity). However, we have evaluated the p-adic limit of the subsequence $C(ap^n)$, and even more generally $C(ap^n + r)$, where a is a constant and $r \in \mathbb{Z}$. The limits of these sequences can be written as an infinite product of numbers which don't divide p, raised to powers increasing logarithmically.

5.1 Open Problems

It remains an open problem to characterize all convergent subsequences of Catalan numbers as well as to find the limits of these subsequences. The methods used to answer these questions will no doubt present their utility in a similar analysis of other combinatorial sequences. Furthermore, it is unknown whether or not the limits established here are transcendental over the rational numbers.

6 Appendix: An Elementary Proof that $\{C(ap^n)\}$ Converges

Proposition 1.7 states that to show that a sequence $\{f(n)\}$ converges p-adically, it suffices to show that its elements are eventually constant modulo arbitrarily large powers of p. This equivalent definition of p-adic convergence is useful because there are existing results on factorials, binomial coefficients, and Catalan numbers modulo powers of primes. One such result is used to prove

Theorem 6.1. *For all primes p and all $a \in \mathbb{N}$, $\{C(ap^n)\}_{n\geq 0}$ converges p-adically.*

The proof of Theorem 6.1 relies on a 1997 result due to Granville.

Theorem 6.2 (Granville 1997)**.** *Let n be an integer, and write $n = \gamma_0 + \gamma_1 p + \cdots + \gamma_d p^d$ in base p. For $j \geq 0$ and p^k a power of p, define n_j to be the least positive residue of $\lfloor \frac{n}{p^j} \rfloor$* (mod p^k) *(so that $n_j = \gamma_j + \gamma_{j+1}p + \cdots + \gamma_{j+k-1}p^{k-1}$). Define $(n_j!)_p$ to be the product of numbers $\leq n_j$ that are coprime with p. Then*

$$n! \equiv p^{\nu_p(n!)}(\delta(p,k))^{\nu_{p^k}(n!)} \prod_{j=\geq 0} (n_j!)_p \pmod{p^k},$$

where $\delta(p,k) = \begin{cases} 1 & \textit{if } p=2 \textit{ and } k \geq 3 \\ -1 & \textit{otherwise.} \end{cases}$

Since $C(n) = \frac{(2n)!}{n!(n+1)!}$, applying Theorem 6.2 to $C(n)$ yields

$$C(n) \equiv \delta^{\nu_{p^k}(C(n))} p^{\nu_p(C(n))} \overbrace{\frac{\prod_{j\geq 0}((2n)_j)!_p}{\prod_{j\geq 0}(n_j)!_p \prod_{j\geq 0}((n+1)_j)!_p}}^{\mathcal{P}(n)} \pmod{p^k}. \tag{6.1}$$

Theorem 6.1 uses the case $n = ap^n$. To show that $\{C(ap^n)\}$ is eventually constant modulo p^k, it thus suffices to show that all three components of the right-hand side of (Equation 6.1) (the power of δ, the power of p, and $\mathcal{P}(n)$) are eventually constant modulo p^k.

Proof of Theorem 6.1. Fix $k \geq 1$. Write $a = \alpha_0 + \alpha_1 p + \cdots + \alpha_m p^m$ in base p ($\alpha_i \neq 0$ for all i), so that $ap^n = \alpha_0 p^n + \cdots + \alpha_m p^{n+m}$ in base p. To show that $\delta^{\nu_{p^k}(C(ap^n))}$ and $p^{\nu_p(C(ap^n))}$ are eventually constant modulo p^k, it is clearly sufficient to show that $\nu_{p^k}(C(ap^n))$ is constant for all n. This is an easy application of Legendre's 1808 result that $\nu_p(n!) = \frac{n-s(n)}{p-1}$, where $s(n)$ is the sum of the base-p coefficients of n. We have

$$\begin{aligned} \nu_{p^k}(C(ap^n)) = \nu_{p^k}\left(\frac{(2ap^n)!}{((ap^n)!)^2}\right) &= \nu_{p^k}((2ap^n)!) - 2\nu_{p^k}(n!) \\ &= \frac{2ap^n - s(2ap^n)}{p-1} - 2\frac{ap^n - s(ap^n)}{p-1} \\ &= \frac{2ap^n - s(2ap^n}{p-1} - \frac{2ap^n - 2s(ap^n)}{p-1} \\ &= \frac{2s(ap^n) - s(2ap^n)}{p-1}, \end{aligned}$$

which does not vary with n.

Thus, all that remains to show is that $\mathcal{P}(ap^n)$ is eventually constant. This expression can be simplified considerably by showing that

$$(ap^n+1)_j = \begin{cases} ap^n_0 + 1 & \text{if } j = 0 \\ ap^n_j & \text{if } j \neq 0 \end{cases} \tag{6.2}$$

and that

$$(2ap^n)_j = 2(ap^n_j) \text{ for all } j. \tag{6.3}$$

To verify Equation 6.2, note that the base-p expansion of ap^n+1 differs from that of ap^n only in that its p^0 coefficient is 1, whereas the p^0 coefficient of the base-p expansion ap^n is 0. The p^0 coefficient is included in $ap^n_j = a_jp^j + a_{j+1}p^{j+1} + \cdots + a_{j+k-1}p^{j+k-1}$ only when $j=0$; thus, $(ap^n+1)_0 = ap^n_0 + 1$ for $j=0$ and $(ap^n+1)_j = ap^n_j$ otherwise.

To verify Equation 6.3, simply note that for all j

$$(2ap^n)_j = \lfloor \frac{2ap^n}{p^j} \rfloor \pmod{p^k} = 2ap^{n-j} \pmod{p^k} = 2\lfloor \frac{ap^n}{p^j} \rfloor \pmod{p^k} = 2ap^n_j.$$

Applying Equation 6.2 and Equation 6.3 to $\mathcal{P}(ap^n)$ gives

$$\mathcal{P}(ap^n) = \frac{\prod_{j\geq 0}((2ap^n)_j)!_p}{\prod_{j\geq 0}(ap^n_j)!_p \prod_{j\geq 0}((ap^n+1)_j)!_p} = \frac{2}{ap^n_0+1} \cdot \overbrace{\prod_{j\geq 1} \frac{(2ap^n_j)!_p}{((ap^n_j)!_p)^2}}^{\mathcal{P}'(ap^n)}.$$

Clearly, this is eventually constant modulo p^k if ap^n_0 and $\mathcal{P}'(ap^n)$ are. It is easy to check that the former is constant for all $n > k$. $\mathcal{P}'(ap^n)$ varies with n only if the set $\{ap^n_j\}_{j\geq 1}$ does. Define

$$ap^n_J = \{ap^n_j\}_{j\geq 1}.$$

Then $\mathcal{P}'(ap^n)$ is eventually constant modulo p^k if ap^n_J is constant for all sufficiently large n.

To prove this, it suffices to take $n > k$. Given such an n, write $ap^n = a_np^n + a_{n+1}p^{n+1} + \cdots + a_{n+m}p^{n+m}$, where $a_{n+i} = \alpha_i$ for $i \in \{0, \ldots, m\}$. For $j \in \mathbb{N} \setminus \{n-k+1, \ldots, n+m\}$, $ap^n_j = 0$, since none of a_n through a_{n+m} (the non-zero coefficients of the base-p expansion of ap^n) appears as a coefficient of ap^n_j for any such j. Thus there are $n+m-(n-k) = m+k$ values of j for which ap^n_j is non-zero (crucially, this number does not depend on n). Running j from $n-k+1$ to $n+m$, we get that $ap^n_J = \{\alpha_0p^{k-1}, \alpha_0p^{k-2}+\alpha_1p^{k-1}, \ldots, \alpha_{m-1}+\alpha_mp, \alpha_m\}$. None of the elements of this set depends on n, as desired. □

Retracing the steps of the proof, showing that ap^n_J is eventually constant modulo an arbitrary power of p (say p^k) was sufficient to show that $\mathcal{P}'(ap^n)$, and thus $\mathcal{P}(ap^n)$, is eventually constant modulo p^k. This was was needed to prove our original objective, that Equation 6.1 is eventually constant modulo p^k. Furthermore, recall that this is sufficient to show convergence because for all k and sufficiently large m and n,

$$|f(n) - f(m)|_p \leq p^{-k} \text{ if and only if } f(n) \equiv f(m) \pmod{p^k}.$$

Showing that ap^n_J is eventually constant modulo p^k is thus crucial step of the proof. It is also its most difficult step. The following example is meant to give the reader a better sense of ap^n_J, and of why it is eventually constant, by way of the sequence $\{C(p^n)\}$.

Example 6.3. Suppose that $a = 1$, so that $ap^n = p^n$. Fix $k = 3$. For a given $n > 3$, the base-p expansion of $p^n = a_n p^n = 1 \cdot p^n$ has only one non-zero coefficient, so for all $j \geq 1$, $p^n_j = a_j + a_{j+1}p + a_{j+2}p^2$ will have at most one non-zero term. If none of j, $j+1$, or $j+2$ is n, then p^n_j=0; thus, $p^n_j = 0$ for all $j \in \mathbb{N} \setminus \{n-2, n-1, n\}$. For the remaining values of j, we have tht $p^n_{n-2} = p^2$, $p^n_{n-1} = p$, and $p^n_n = 1$, so that $p^n_J = \{1, p, p^2\}$. The cardinality of this set, $3 = 0 + 3 = m + k$, does not depend on n, and neither do its elements.

Notice that taking $n > k = 3$ is necessary because if $n = 2$, for instance, $p^2_1 = p$, $p^2_2 = 1$, and $p^2_j = 0$ for all $j > 2$. Thus $p^2_J = \{1, p\}$; p^2 is excluded from p^2_J because there are no j for which a_{j+2} is non-zero.

7 Acknowledgments

This work was carried out during the 2014 Mathematical Sciences Research Institute Undergraduate Program (MSRI-UP) which is funded by the National Science Foundation (grant No. DMS-1156499) and the National Security Agency (grant No. H-98230-13-1-0262). We would like to thank Dr. Victor Moll, Dr. Herbert Medina, Dr. Eric Rowland, Asia Wyatt and our peers in MSRI-UP 2014 for their support throughout this process.

The first author would like to thank Dr. Zvezdelina Stankova and Dr. Maia Averett for recommending her to MSRI-UP, and supporting her pursuit of education in mathematics.

The second author would like to thank Dr. Robert Benedetto, an exceptional teacher who recommended him to MSRI-UP and who, more importantly, played a crucial role in piquing his interest in mathematics. The second author would surely not have had the opportunity to conduct mathematics research if it were not for Dr. Benedetto's guidance.

The third author would like to thank Dr. Irena Swanson and Dr. James Fix for their support and inspiration, mathematical and otherwise.

References

[FG] Gouvea, Fernando Q. *p-adic Numbers: An Introduction.* Second Edition. Springer, 2003.

[AG] Granville, Andrew. “Binomial coefficients modulo prime powers”. textitCanadian Mathematical Society Conference Proceedings, vol. 20, pp. 253-275. 1997.

[NK] Koblitz, Neal. *p-adic Numbers, p-adic Analysis, and Zeta-Functions.* Second Edition. Springer. 1984.

[SK] Katok, Svetlana. *p-adic Analysis Compared with Real.* American Mathematical Society. 2007.

[ER] Rowland, Eric. “Regularity Versus Complexity in the Binary Representation of 3^n”. *Complex Systems* 18, pp. 367-73. 2009.

[RS] Stanley, Richard. *Enumerative Combinatorics.* Vol 1. Second Edition. Cambridge University Press. 2011.

On the divisibility and valuations of the Franel numbers

Abraham Schulte Northwestern University

Samantha VanSchalkwyk Mount Holyoke College

Adela Yang Bowdoin College

August 2014

Abstract

The Franel numbers are the sums of the cubes of binomial coefficients. This sequence is of great interest. They are the first power for which the sums are not defined by a closed form formula. Primes may be partitioned with respect to the p-adic valuations of Franel numbers: those whose valuation is always 0, those whose valuation is equal to the number of occurrences of a particular digit in base-p, and those which fall into neither category. Furthermore, the 2-adic valuations of the Franel numbers have interesting properties. The goal of this paper is to investigate the properties of these numbers.

Contents

1 Introduction

The sums of the first and second powers of the binomial coefficients are

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n \quad \text{and} \quad \sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n},$$

respectively. The Franel numbers are the sums of the third powers.

Definition 1.1. Let $n \in \mathbb{N}$.[1] The ***n*th Franel number**, denoted Fra_n, is

$$\sum_{k=0}^{n} \binom{n}{k}^3.$$

The Franel numbers are the first sum of powers of binomial coefficients that do not have a closed form expression. In [PWZ], Petkovsek, Wilf and Zeilberger show that the Franel numbers do not have a closed form as a finite sum of hypergeometric functions. However,

[1] Throughout, $\mathbb{N}$ denotes the set of natural numbers, $\{0, 1, \ldots\}$, while $\mathbb{Z}^+$ denotes the set of positive integers, $\{1, 2, \ldots\}$.

Franel, after whom the numbers are named, derives a second order recurrence formula and proof for the Franel numbers in [Fr].

Theorem 1.2. *Let $n \geq 2$ be a natural number. Then*

$$n^2 \operatorname{Fra}_n = \left(7n^2 - 7n + 2\right) \operatorname{Fra}_{n-1} + 8(n-1)^2 \operatorname{Fra}_{n-2}$$

with $\operatorname{Fra}_0 = 1$ *and* $\operatorname{Fra}_1 = 2$.

Example 1.3 illustrates the second order recurrence of the Franel numbers.

Example 1.3. A few of the first Franel numbers are

$$\operatorname{Fra}_5 = \sum_{k=0}^{5} \binom{5}{k}^3 = 2252,$$

$$\operatorname{Fra}_4 = \sum_{k=0}^{4} \binom{4}{k}^3 = 346,$$

$$\operatorname{Fra}_3 = \sum_{k=0}^{3} \binom{3}{k}^3 = 56.$$

Then, the values are replaced in the recurrence equation and the following is the result:

$$5^2(2252) = 56300 = (142)(346) + 128(56) = \left(7 * 5^2 - 7 * 5 + 2\right)(346) + 8(5-1)^2(56).$$

It is not clear that the Franel recurrence yields an integer sequence. Section 4 investigates which initial conditions of the Franel recurrence yield integer sequences. Additionally, the divisibility of the Franel numbers will be discussed.

Definition 1.4. Let p be a prime. Let $n \in \mathbb{N}$. The ***p*-adic valuation of *n***, denoted $\nu_p(n)$, is the highest power of p that divides n.

Example 1.5.

1. The 3-adic valuation of 24, $\nu_3(24) = 1$, since $3^1 \mid 24$ but $3^2 \nmid 24$.

2. The 2-adic valuation of any odd number is 0, since no odd number is divisible by 2.

If $\nu_p(\operatorname{Fra}_n) = 0$ for some prime p for all $n \in \mathbb{N}$, then no Franel number is divisible by p. These primes, which will be referred to as type I, will be discussed in Section 2.

Using the Mathematica code below, the p-adic valuations for $\operatorname{Fra}_0, \operatorname{Fra}_1, \ldots, \operatorname{Fra}_{nmax}$ were evaluated.

```
Table[IntegerExponent[Franel[n],5],{n,0,nmax}]
```

where

```
Franel[n_]:=Sum[Binomial[n,k]^3,{k,0,n}]
```

After much experimentation, it was found that for some primes, which will be referred to as type II, the p-adic valuation of the n^{th} Franel number is given by the number of occurrences of a particular digit in the base-p representation of n. This is discussed in Section 2.

During experimentation with the above code, it was seen that 2-adic valuations of the Franel numbers seem to have a different structure than valuations with other primes. A thorough treatment of the topic is given in Section 3.

A few results tangential to the main study are presented in Section 4 and potential directions for future research are given in Section 5.

2 Prime types

Based on the valuations of the Franel numbers, a natural partition of the primes into types arises. Prior to this paper, this partition does not seem to exist within the literature. The goal of this section is to classify the primes are of each type.

Definition 2.1.

(a) A prime p is **type I** if p does not divide any Franel number.

(b) A prime p is **type II** if $\nu_p(\mathrm{Fra}_n) = C_p\big(n, \frac{p-1}{2}\big)$ for all $n \in \mathbb{N}$, where $C_p(n,k)$ is the number of k's in the base-p representation of n.

(c) A prime p is **type III** if p is neither type I nor type II.

2.1 The prime 3

Fermat's little Theorem will be applied in Proposition 2.2. As this is a well known result, the proof is omitted.

Fermat's Little Theorem (FLT). *Let p be a prime. Let $a \in \mathbb{Z}$. Then*

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

Using this, the modular residues of the Franel numbers are determined.

Proposition 2.2. *Let $n \in \mathbb{N}$. Then*

$$\mathrm{Fra}_n \equiv \begin{cases} 1 \pmod{3} & \text{if } n \text{ is even} \\ 2 \pmod{3} & \text{if } n \text{ is odd.} \end{cases}$$

Proof. Observe

$$\begin{aligned} \mathrm{Fra}_n &= \sum_{k=0}^{n} \binom{n}{k}^3 \overset{\text{FLT}}{\equiv} \sum_{k=0}^{n} \binom{n}{k} \pmod{3} \\ &= 2^n \equiv (-1)^n \pmod{3} \\ &= \begin{cases} 1 & \text{if } n \text{ is even} \\ -1 & \text{if } n \text{ is odd} \end{cases} \equiv \begin{cases} 1 \pmod{3} & \text{if } n \text{ is even} \\ 2 \pmod{3} & \text{if } n \text{ is odd.} \end{cases} \end{aligned}$$

□

The type of the prime 3 is now determined.

Theorem 2.3. *The prime 3 is type I.*

Proof. This follows immediately from Proposition 2.2. □

2.2 Divisibility using modular arithmetic and valuations

One may recover several results regarding the divisibility of Franel numbers using modular arithmetic and p-adic valuations. The goal of this subsection is to explore these applications.

2.2.1 Preliminaries

Functions for the sum of the digits of a number are introduced, as they will appear in the discussion.

Definition 2.4. For any prime p and any $n \in \mathbb{N}$, define $S_p(n)$ to be the sum of base-p digits of n.

Example 2.5. Consider the prime 2 and the number 346. The base-2 representation of 346 is 101011010_2. Thus,

$$S_2(346) = 1 + 0 + 1 + 0 + 1 + 1 + 0 + 1 + 0 = 5.$$

Lemma 2.6 and its proof were given by Legendre in [Le].

Lemma 2.6. *Let p be a prime. Let $n \in \mathbb{N}$. Then*

$$\nu_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor = \frac{n - S_p(n)}{p-1}.$$

From this, the p-adic valuations of the binomial coefficients are obtained.

Corollary 2.7. *Let p be a prime. Let $n, k \in \mathbb{N}$. Then*

$$\nu_p\left(\binom{n}{k}\right) = \frac{S_p(n-k) + S_p(k) - S_p(n)}{p-1}.$$

Proof. The proof follows directly from Lemma 2.6. □

Additionally, note the following relation regarding the sums of digits of base-p representations of a number, given in [JLF].

Lemma 2.8. *Let p be a prime number. Let $n_1, n_2, \ldots, n_k \in \mathbb{N}$. Then*

$$S_p(n_1) + S_p(n_2) + \cdots + S_p(n_k) \geq S_p(n_1 + n_2 + \cdots + n_k)$$

with equality if and only if there are no carries in the base-p sum of $n_1, n_2, \ldots,$ and n_k.[2]

Proof. The lemma is proven for k=2 and the general result follows by induction. Each carry in the base-p sum of 2 numbers subtracts p from the two digits being added, and adds 1 to the sum of the next two digits. That is, each carry reduces the digit sum by $p - 1$. Since p is prime, $p \geq 2$. That is, $p - 1 \geq 1$. The result follows due to the fact that the number of carries is nonnegative. □

Theorem 2.9 is given by Strehl in [S]. The proof is reproduced here as well.

[2] For example, there are 2 carries in the base-10 sum 279 + 541 = 820.

Theorem 2.9. *Let $n \in \mathbb{N}$. Then*

$$\mathrm{Fra}_n = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{2k}{n}.$$

Proof. The n^{th} Franel number can be rewritten as:

$$\begin{aligned}
\mathrm{Fra}_n &= \sum_{k} \binom{n}{k}^3 \\
&= \sum_{i+j=n} \binom{n}{i}\binom{n}{j}\binom{i+j}{i} \\
&= \sum_{i+j=n} \binom{n}{i}\binom{n}{j} \sum_{k} \binom{i}{k}\binom{j}{k} \\
&= \sum_{k} \binom{n}{k}^2 \sum_{i+j=n} \binom{n-k}{n-i}\binom{n-k}{n-j} \\
&= \sum_{k} \binom{n}{k}^2 \sum_{i+j=n} \binom{k}{i}\binom{k}{j} \\
&= \sum_{k} \binom{n}{k}^2 \binom{2k}{n}.
\end{aligned}$$

□

Motivated by Theorem 2.9, the function g is defined as follows.

Definition 2.10. For any $n, k \in \mathbb{N}$, define

$$g(n,k) = \binom{n}{k}^2 \binom{2k}{n}.$$

Note. For any $n \in \mathbb{N}$,

$$\mathrm{Fra}_n = \sum_{k=0}^{n} g(n,k)$$

by Theorem 2.9.

The divisibility of $g(n,k)$ by p can be determined as in the lemma below. As the sums in the lemma will be often used, they are labeled for future referencing.

Lemma 2.11. *Let p be a prime. Let $n, k \in \mathbb{N}$. Then $g(n,k)$ is not divisible by p if and only if the sums*

$$k + k = 2k \quad \text{and} \quad (n-k) + (n-k) + (2k-n) = n \tag{2.1}$$

have no carries in the base-p representations.

Proof. Observe

$$\begin{aligned}
\nu_p(g(n,k)) &= 2\nu_p\left(\binom{n}{k}\right) + \nu_p\left(\binom{2k}{n}\right) \\
&= 2\left(\frac{S_p(n-k)+S_p(k)-S_p(n)}{p-1}\right) + \frac{S_p(2k-n)+S_p(n)-S_p(2k)}{p-1} \\
& \qquad \text{(Corollary 2.7)} \\
&= \frac{2S_p(k)-S_p(2k)+2S_p(n-k)+S_p(2k-n)-S_p(n)}{p-1} \\
&= \frac{\gamma(n,k)+\delta(n,k)}{p-1},
\end{aligned}$$

where

$$\gamma(n,k) = S_p(k) + S_p(k) - S_p(2k)$$

and

$$\delta(n,k) = S_p(n-k) + S_p(n-k) + S_p(2k-n) - S_p(n).$$

By Lemma 2.8 (where $n_1 = k, n_2 = k$ for γ and $n_1 = n-k$, $n_2 = n-k$, and $n_3 = 2k-n$ for δ), γ and δ are nonnegative. Thus, $\nu_p(g(n,k)) = 0$ if and only if $\gamma(n,k) = 0$ and $\delta(n,k) = 0$. Therefore, by Lemma 2.8, $\nu_p(g(n,k)) = 0$ if and only if (2.1) has no carries in the base-p sums. □

Theorem 2.12 and its proof were given by Lucas in [Lu].

Theorem 2.12. *Let p be a prime. Let $n = n_d n_{d-1} \cdots n_0$ and $k = k_d k_{d-1} \cdots k_0$ be natural numbers with their associated base-p representations, allowing for leading zeroes in the latter. Then*

$$\binom{n}{k} \equiv \prod_{j=0}^{d} \binom{n_j}{k_j} \pmod{p}.$$

With an additional condition, a similar congruence holds for the function g.

Corollary 2.13. *Notation as in Theorem 2.12. If n and k are such that* (2.1) *has no carries in the base-p sums, then*

$$g(n,k) \equiv \prod_{j=0}^{d} g(n_j,k_j) \pmod{p}.$$

Proof. Suppose n, k are such that (2.1) has no carries in the base-p sums. Then $k_j < \frac{p}{2}$ for each digit k_j of k. Thus, $(2k)_j = 2k_j$ for each digit $(2k)_j$ of $2k$. Therefore,

$$\begin{aligned} g(n,k) &= \binom{n}{k}^2 \binom{2k}{n} \\ &\equiv \left(\prod_{j=0}^{d} \binom{n_j}{k_j}\right)^2 \prod_{j=0}^{d} \binom{(2k)_j}{n_j} \pmod{p} \qquad \text{(Theorem 2.12)} \\ &= \prod_{j=0}^{d} \binom{n_j}{k_j}^2 \binom{2k_j}{n_j} = \prod_{j=0}^{d} g(n_j, k_j). \end{aligned}$$

□

2.2.2 The prime 3 (revisited)

An alternate proof that 3 is type I is presented. This proof, based on the proof of Theorem 2 in [JLF], starts with a lemma.

Lemma 2.14. *Let $n, k \in \mathbb{N}$. Then (2.1) has no carries in the base-3 sums if and only if for each digit n^* in the base-3 representation of n, the following correspondence holds:*

$$n^* = 0 \leftrightarrow k^* = 0$$

$$n^* = 1 \leftrightarrow k^* = 1$$

$$n^* = 2 \leftrightarrow k^* = 1.$$

where k^* is the digit of the base-3 representation of k corresponding to n^*.

Proof.

(⇒) Suppose the sums have no carries. Let n^* be a digit in the base-p representation of n. Note that by the first sum, $k^* \leq \frac{3-1}{2} = 1$, else there is a carry. Suppose $n^* = 0$. Then by the second sum, $k^* = 0$, else $(n-k)^* = 2$, and there is a carry. The cases of $n^* = 1$, $n^* = 2$, $n^* = 3$, and $n^* = 4$ are similar.

(⇐) Suppose the correspondence holds. Then clearly there are no carries in the sums. □

Example 2.15. Let $n = 142 = 12021_3$ (12021_3, for example, denotes 142 in base-3). Then $k = 130 = 11111_3$ is such that (2.1) has carries in the base-3 sums. In particular, the second sum has a carry in the third least significant digit.

Example 2.16. Let $n = 142 = 12021_3$. Then $k = 112 = 11011_3$ is the unique k such that (2.1) has no carries in the base-3 sums. This k is obtained by replacing each 2 in the base-3 representation of n by 1, each 1 by 1, and each 0 by 0. Uniqueness is given by Lemma 2.14.

Corollary 2.17. *Let $n, k \in \mathbb{N}$. Then $g(n, k)$ is not divisible by 3 if and only if the correspondence from Lemma 2.14 holds.*

Proof. The proof follows directly from Lemma 2.11. □

Example 2.18. Let $n = 15 = 120_3$ and $k = 14 = 112_3$. Then $g(15, 11)$ is divisible by 3, since n and k do not follow the correspondence of Lemma 2.14. This may be checked numerically by observing that $g(15, 14) = 8424486000 \equiv 0 \pmod 3$.

Example 2.19. Let $n = 15 = 120_3$ and $k = 12 = 110_3$. Then $g(15, 12)$ is not divisible by 3, since each digit of n and k follows the correspondence of Lemma 2.14. This may be checked numerically by observing that $g(15, 12) = 270686015600 \equiv 2 \pmod 3$. Additional numerical checks verify that $k = 12$ is the unique k such that $g(15, k)$ is not divisible by 3.

A new proof of Theorem 2.3, restated here, is presented.

Theorem 2.3. *The prime 3 is type I.*

Proof. Let $n, k \in \mathbb{N}$. By Corollary 2.17, $g(n, k)$ is not divisible by 3 if and only if the correspondence of digits from Lemma 2.14 holds. Thus, there exists a unique k_0, given by the correspondence of digits with n, such that $g(n, k_0)$ is not divisible by 3. Thus,

$$\mathrm{Fra}_n = \sum_{k=0}^{n} g(n, k) \equiv g(n, k_0) \not\equiv 0 \pmod 3.$$ □

2.2.3 The prime 5

Next, the prime 5 is discussed, beginning with a lemma.

Lemma 2.20. *Let $n, k \in \mathbb{N}$. Then (2.1) has no carries in the base-5 sums if and only if for each digit n^* in the base-5 representation of n, the following correspondence holds:*

$$\begin{aligned}
n^* = 0 &\leftrightarrow k^* = 0 \\
n^* = 1 &\leftrightarrow k^* = 1 \\
n^* = 2 &\leftrightarrow k^* = 1 \text{ or } 2 \\
n^* = 3 &\leftrightarrow k^* = 2 \\
n^* = 4 &\leftrightarrow k^* = 2,
\end{aligned}$$

where k^* is the digit of the base-5 representation of k corresponding to n^*.

Proof. The proof is similar to the proof of Lemma 2.14, and so is omitted. □

Example 2.21. Let $n = 606836 = 123404321_5$, then

$$\begin{aligned}
k_1 &= 112202211_5 = 506556 \\
k_2 &= 112202221_5 = 506561 \\
k_3 &= 122202211_5 = 584681 \\
k_4 &= 122202221_5 = 584686
\end{aligned}$$

are the unique k's such that (2.1) has no carries in the base-5 sums. These k's are found by replacing each 4 in the base-5 representation of n by 2, each 3 by 2, each 1 by 1, and each 0 by 0. Then, for each 2 in the base-5 representation of n, there are two corresponding values of that digit of k such that (2.1) has no carries in the base-5 sums, producing $2^2 = 4$ k's with no carries. By Lemma 2.20, these k's are the only such k.

Corollary 2.22. *Let $n, k \in \mathbb{N}$. Then $g(n, k)$ is not divisible by 5 if and only if the correspondence from Lemma 2.20 holds.*

Proof. The proof follows directly from Lemma 2.11. □

Corollary 2.23. *Let $n = n_d n_{d-1} \cdots n_0$ and $k = k_d k_{d-1} \cdots k_0$ be natural numbers with their associated base-5 representations, allowing for leading zeroes in the latter. If n and k are such that the correspondence of digits from Lemma 2.20 holds, then*

$$g(n, k) \equiv \prod_{j=0}^{d} g(n_j, k_j) \pmod{5}.$$

Proof. The proof follows directly from Corollary 2.13 (with $p = 5$). □

Hellof

Theorem 2.24. *Let $n \in \mathbb{N}$. Then Fra_n is divisible by 5 if and only if n contains at least one 2 in its base-5 representation.*

Proof.

(⇒) Suppose n does not contain a 2 in its base-5 representation. By Corollary 2.22, $g(n,k)$ is not divisible by 5 if and only if the correspondence of digits from Lemma 2.20 holds. Since there is no 2 in the base-5 representation of n, there exists a unique k_0, given by the correspondence of digits with n, such that $g(n,k_0)$ is not divisible by 5. Therefore,

$$\mathrm{Fra}_n = \sum_{k=0}^{n} g(n,k) \equiv g(n,k_0) \not\equiv 0 \pmod{5}.$$

(⇐) Suppose n contains a 2 in its base-5 representation. Let $n = n_d n_{d-1} \cdots n_0$ be the base-5 representation of n. Proceed by induction on the number of digits of n that are 2 in the base-5 representation.

Case I. Suppose n has $q = 1$ digit that is 2 in its base-5 representation. Let α be the index of the digit of n that is 2. Define

$$k_1 = k_d^{(1)} k_{d-1}^{(1)} \cdots k_0^{(1)} \quad \text{and} \quad k_2 = k_d^{(2)} k_{d-1}^{(2)} \cdots k_0^{(2)}$$

by using the correspondence of Lemma 2.20 for all digits of k_1, k_2, so $k_j^{(1)} = k_j^{(2)}$ for $j \neq \alpha$ with $k_\alpha^{(1)} = 1$ and $k_\alpha^{(2)} = 2$. Since there is exactly one digit of n that is 2 in the base-5 representation, by Corollary 2.22, k_1, k_2 are the only values of k such that $g(n,k)$ is not divisible by 5. By Corollary 2.23 (with $p = 5$, $n = n$, and $k = k_1, k_2$),

$$g(n,k_1) \equiv \prod_{j=0}^{d} g\left(n_j, k_j^{(1)}\right) \pmod{5}$$

and

$$g(n,k_2) \equiv \prod_{j=0}^{d} g\left(n_j, k_j^{(2)}\right) \pmod{5}.$$

Then

$$\begin{aligned}
\mathrm{Fra}_n &= \sum_{k=0}^{n} g(n,k) \equiv g(n,k_1) + g(n,k_2) \pmod 5 \\
&\equiv \prod_{j=0}^{d} g\Big(n_j, k_j^{(1)}\Big) + \prod_{j=0}^{d} g\Big(n_j, k_j^{(2)}\Big) \pmod 5 \\
&= \left(\prod_{j \in S \setminus \{\,\alpha\,\}} g\Big(n_j, k_j^{(1)}\Big) \right) \Big(g\big(n_\alpha, k_\alpha^{(1)}\big) + g\big(n_\alpha, k_\alpha^{(2)}\big)\Big) \qquad (S = \{\,0, 1, \ldots, d\,\}) \\
&\equiv 0 \pmod 5,
\end{aligned}$$

since

$$g\big(n_\alpha, k_\alpha^{(1)}\big) + g\big(n_\alpha, k_\alpha^{(2)}\big) = g(2,1) + g(2,2) = 10 \equiv 0 \pmod 5.$$

Case II. Suppose n has $q > 1$ digits that are equal to 2 in its base-5 representation. Note that there are 2^q values of k corresponding to n such that $g(n,k) \not\equiv 0 \pmod 5$. Observe that these k may be paired so that the elements of each pair differ in only one digit. The base step demonstrates that for each of these 2^{q-1} pairs, the factor $g(2,1) + g(2,2) = 10$ appears. Therefore, $\mathrm{Fra}_n \equiv 0 \pmod 5$. □

2.2.4 Lucas' theorem for the Franel numbers

A general formulation of the congruence (mod p) of the n^{th} Franel number follows. This is analogous to Theorem 2.12.

Theorem 2.25. *Let p be a prime. Let $n = n_d n_{d-1} \cdots n_0$ be a natural number with its associated base-p representation. Then,*

$$\mathrm{Fra}_n \equiv \prod_{j=0}^{d} F_{n_j} \pmod p.$$

Proof. For each natural number $k < p^{d+1}$, let $k = k_d k_{d-1} k_0$ be the base-p representation of k, allowing for leading zeroes. Notice that for all natural numbers k_j, if $k_j > n_j$, then $g(n_j, k_j) = 0$. Thus,

$$\prod_{j=0}^{d} F_{n_j} = \prod_{j=0}^{d} \sum_{k_j=0}^{n_k} g(n_j, k_j) = \prod_{j=0}^{d} \sum_{k_j=0}^{p-1} g(n_j, k_j).$$

By Lemma 2.11, $g(n,k) \not\equiv 0 \pmod{p}$ if and only if the sums of (2.1) have no carries in the base-p representations. Thus, by Corollary 2.13,

$$\sum_{k=0}^{p^{d+1}-1} g(n,k) \equiv \sum_{k=0}^{p^{d+1}-1} \prod_{j=0}^{d} g(n_j,k_j) \pmod{p}.$$

Observe that $n = n_0p^0 + n_1p^1 + \cdots + n_dp^d \leq (p-1)p^0 + (p-1)p^1 + \cdots + (p-1)p^d = p^{d+1} - 1$. Additionally, $p^{d+1} - 1 \geq p^d - 1$ with equality if and only if $d = 0$. Therefore,

$$\begin{aligned}
F_n &= \sum_{k=0}^{n} g(n,k) = \sum_{k=0}^{p^{d+1}-1} g(n,k) \equiv \sum_{k=0}^{p^{d+1}-1} \prod_{j=0}^{d} g(n_j,k_j) \pmod{p} \\
&= \sum_{k_0=0}^{p-1} \sum_{k_1=0}^{p-1} \cdots \sum_{k_d=0}^{p-1} \prod_{j=0}^{d} g(n_j,k_j) = \sum_{k_0=0}^{p-1} \sum_{k_1=0}^{p-1} \cdots \sum_{k_d=0}^{p-1} (g(n_0,k_0)g(n_1,k_1)\cdots g(n_d,k_d)) \\
&= \sum_{k_0=0}^{p-1} \cdots \sum_{k_{d-1}=0}^{p-1} \\
&\quad [g(n_0,k_0)\cdots g(n_{d-1},k_{d-1})g(n_d,0) + g(n_0,k_0)\cdots g(n_{d-1},k_{d-1})g(n_d,1) + \cdots + \\
&\quad g(n_0,k_0)\cdots g(n_{d-1},k_{d-1})g(n_d,p-1)] \\
&= \sum_{k_0=0}^{p-1} \cdots \sum_{k_{d-1}=0}^{p-1} \prod_{i=0}^{d-1} g(n_i,k_i) \prod_{j=d}^{d} \sum_{k_j=0}^{p-1} g(n_j,k_j) \\
&= \sum_{k_0=0}^{p-1} \cdots \sum_{k_{d-2}=0}^{p-1} \\
&\quad [[g(n_0,k_0)\cdots g(n_{d-1},0)g(n_d,0) + \cdots + g(n_0,k_0)\cdots g(n_{d-1},0)g(n_d,p-1)] + \\
&\quad [g(n_0,k_0)\cdots g(n_{d-1},1)g(n_d,0) + \cdots + g(n_0,k_0)\cdots g(n_{d-1},1)g(n_d,p-1)] + \cdots + \\
&\quad [g(n_0,k_0)\cdots g(n_{d-1},p-1)g(n_d,0) + \cdots + g(n_0,k_0)\cdots g(n_{d-1},p-1)g(n_d,p-1)]] \\
&= \sum_{k_0=0}^{p-1} \cdots \sum_{k_{d-2}=0}^{p-1} \prod_{i=0}^{d-2} g(n_i,k_i) \prod_{j=d-1}^{d} \sum_{k_j=0}^{p-1} g(n_j,k_j) \\
&\quad \vdots \\
&= \sum_{k_0=0}^{p-1} \prod_{i=0}^{0} g(n_i,k_i) \prod_{j=1}^{d} \sum_{k_j=0}^{p-1} g(n_j,k_j) = \prod_{j=0}^{d} \sum_{k_j=0}^{p-1} g(n_j,k_j) = \prod_{j=0}^{d} F_{n_j} \pmod{p}. \qquad \square
\end{aligned}$$

By applying Theorem 2.25 it is possible to verify if a prime is type I.

Corollary 2.26. *A prime number p is type I if and only if p does not divide any of $\{\,\mathrm{Fra}_0, \mathrm{Fra}_1, \ldots, \mathrm{Fra}_{p-1}\,\}$.*

Proof. By Theorem 2.25, for all $n \in \mathbb{N}$, $\mathrm{Fra}_n \not\equiv 0 \pmod{p}$ if and only if $\mathrm{Fra}_{n_d} \mathrm{Fra}_{n_{d-1}} \cdots \mathrm{Fra}_{n_0} \not\equiv 0 \pmod{p}$, where $n = n_d n_{d-1} \cdots n_0$ is the base-p representation of n. Since p is prime, for all $n \in \mathbb{N}$, $p \nmid \mathrm{Fra}_n$ if and only if $p \nmid \mathrm{Fra}_{n_d}, \mathrm{Fra}_{n_{d-1}}, \ldots \mathrm{Fra}_{n_0}$. The result follows by observing $\{\, n^* : n^* \text{ is a digit of } n \text{ for some } n \in \mathbb{N} \,\} = \{\, 0, 1, \ldots, p-1 \,\}$. □

Corollary 2.26 easily recovers Theorems 2.3, 2.24, and 2.41 and provides a list of type I primes.

Proposition 2.27. *The primes 3, 11, 17, 19, 43, 83, 89, 97, 113, 137, 139, 163, 193, 211, 233, 241, 283, 307, 313, 331, 347, 353, 379, 401, 409, 419, 433, 443, 491, 499, 523, 547, 569, 587, 601, 617, 619, 641, 643, 673, 811, 827, 859, 881, 929, 947, 953, and 977 are the only primes less than 1000 that are type I.*

Proof. For each prime $p \leq 1000$, numerically check if p divides any of $\{\, \mathrm{Fra}_0, \mathrm{Fra}_1, \ldots, \mathrm{Fra}_{p-1} \,\}$, and the result follows by Corollary 2.26. □

Additionally, Theorem 2.25 may be used to extend Theorem 2.24.

Theorem 2.28. *Let $n \in \mathbb{N}$. For the primes p = 5, 7, 13, 23, 31, 37, 47, 53, 71, 101, 103, 167, 181, 191, 197, 199, 223, 229, 263, 271, 293, 317, 349, 383, 397, 431, 439, 461, 479, 503, 509, 541, 557, 599, 607, 613, 647, 653, 677, 709, 719, 727, 733, 743, 751, 757, 797, 821, 823, 839, 877, 887, 911, 919, 991, and 997,* Fra_n *is divisible by p if and only if n contains at least one $\frac{p-1}{2}$ in its base-p representation.*

Proof. For each prime p listed, numerical checks verify that of $\{\, \mathrm{Fra}_0, \mathrm{Fra}_1, \ldots, \mathrm{Fra}_{p-1} \,\}$, only $\mathrm{Fra}_{\frac{p-1}{2}}$ is divisible by p and the result follows by Theorem 2.25. □

Example 2.29. By Theorem 2.28, for each $n \in \mathbb{N}$, Fra_n is divisible by the prime 13 if and only if n contains at least one 6 in its base-13 representation. For example, $13 \mid \mathrm{Fra}_{19}$ since $19 = 16_{13}$ has a 6 in its base-13 representation, while $13 \nmid \mathrm{Fra}_{20}$ since $20 = 17_{13}$ has no 6 in its base-13 representation.

2.2.5 A congruence for prime multiples of indices

The goal of this subsection is to find a congruence relation between Fra_{np^r} and $\mathrm{Fra}_{np^{r-1}}$. The proof begins by reformulating Lemma 2.8 to give an exact relation between the sum of the sum of digits of numbers and the sum of the digits of the sum of numbers.

Lemma 2.30. *Let p be a prime. Let $n_1, n_2, \ldots, n_k \in \mathbb{N}$. Then*

$$S_p(n_1) + S_p(n_2) + \cdots + S_p(n_k) - S_p(n_1 + n_2 + \cdots + n_k) = (p-1)c(n_1, n_2, \ldots, n_k),$$

where $c(n_1, n_2, \ldots, n_k)$ denotes the number of carries in the base-p sum $n_1 + n_2 + \cdots n_k$.

Proof. When $k = 2$ the lemma follows from the proof of Lemma 2.8. The general result follows by induction on k. □

With Lemma 2.30, an inequality between the valuations of $g(n,k)$ and n is found.[3]

Lemma 2.31. *Let p be a prime. Let $n, k \in \mathbb{N}$. If $p \nmid k$, then*

$$\nu_p(g(n,k)) \geq \nu_p(n).$$

Proof. From the proof of Lemma 2.11,

$$\nu_p(g(n,k)) = \frac{S_p(k) + S_p(k) - S_p(2k) + S_p(n-k) + S_p(n-k) + S_p(2k-n) - S_p(n)}{p-1}.$$

By Lemma 2.30,

$$\nu_p(g(n,k)) = c(k,k) + c(n-k, n-k, 2k-n),$$

where $c(k,k)$ and $c(n-k, n-k, 2k-n)$ denote the number of carries in the base-p sums

$$k + k = 2k \quad \text{and} \quad (n-k) + (n-k) + (2k-n) = n,$$

respectively.

Define $r = \nu_p(n)$.

Case I. Suppose $r = 0$. Then the result holds trivially.

[3] Recall that $g(n,k) = \binom{n}{k}^2 \binom{2k}{n}$.

Case II. Suppose $r > 0$. It is clear that the r least significant base-p digits of n are 0. Since $p \nmid k$, the least significant base-p digit of k is non-zero. Thus, the least significant base-p digit of $n - k$ is non-zero. Thus, the base-p sum $(n-k)+(n-k)+(2k-n) = n$ has carries in the r least significant base-p digits. That is, $c(n-k, n-k, 2k-n) \geq r$. Therefore,

$$\nu_p(g(n,k)) \geq \nu_p(n). \qquad \square$$

A similar method of proof shows the following.

Lemma 2.32. *Let p be a prime. Let $n, k, r, s \in \mathbb{N}$ such that $r \geq s$. If $p \nmid k$, then*

$$p^{r-s} \mid g(np^r, kp^s).$$

Proof. As seen in the proof of Lemma 2.31,

$$\nu_p(g(np^r, kp^s)) = c(kp^s, kp^s) + c(np^r - kp^s, np^r - kp^s, 2kp^s - np^r),$$

where $c(kp^s, kp^s)$ and $c(np^r - kp^s, np^r - kp^s, 2kp^s - np^r)$ denote the number of carries in the base-p sums

$$kp^s + kp^s = 2kp^s \quad \text{and} \quad (np^r - kp^s) + (np^r - kp^s) + (2kp^s - np^r) = np^r,$$

respectively.

Case I. Suppose $r = s$. Then the result holds trivially.

Case II. Suppose $r > s$. It is clear that the r least significant base-p digits of np^r are 0. Since $p \nmid k$, the s least significant base-p digits of kp^s are 0, and the $(s+1)^{\text{th}}$ least significant base-p digit of kp^s is nonzero. Thus, since $r > s$, the s least significant base-p digits of $np^r - kp^s$ are 0, and the $(s+1)^{\text{th}}$ least significant base-p digit of $np^r - kp^s$ is nonzero. Thus, the base-p sum $(np^r - kp^s) + (np^r - kp^s) + (2kp^s - np^r) = np^r$ has carries in the $(s+1)^{\text{th}}, (s+2)^{\text{th}}, \ldots, r^{\text{th}}$ least significant base-p digits. That is, $c(np^r - kp^s, np^r - kp^s, 2kp^s - np^r) \geq r - s$. Therefore,

$$\nu_p(g(np^r, kp^s)) \geq r - s. \qquad \square$$

Letting $s = 0$, the following result ensues.

Corollary 2.33. *Let p be a prime. Let $n, k, r \in \mathbb{N}$. If $p \nmid k$, then*

$$p^r \mid g(np^r, k),$$

that is,

$$g(np^r, k) \equiv 0 \pmod{p^r}.$$

Proof. The proof follows directly from Lemma 2.32 (with $s = 0$). $\square$

To proceed, Corollaries 2.34 and 2.35 are necessary. Corollary 2.34 and its proof were given by Jarvis and Verrill in [JV] as Corollary 5.2.

Corollary 2.34. *Let p be an odd prime. Let $r \in \mathbb{Z}^+$. Let $n = n_d n_{d-1} \cdots n_0$ be a natural number with its associated base-p representation. Let N_j be the residue of $\left\lfloor \frac{n}{p_j} \right\rfloor$ modulo p^r (that is, $N_j = n_j + n_{j+1}p^1 + \cdots + n_{j+r-1}p^{r-1}$) for each $j = 0, 1, \ldots, d$. Let $k = k_d k_{d-1} \cdots k_0$ and $l = l_d l_{d-1} \cdots l_0$ be natural numbers with their associated base-p representations such that $n = k + l$. Make corresponding definitions for K_j, L_j based on N_j. Let e_0 be the number of indices i such that $k_i + l_i \geq p$, that is, the number of carries in the base-p sum of k and l. Then*

$$\frac{1}{p^{e_0}}\binom{pn}{pk} \equiv \left(\frac{((pN_0)!)_p}{((pK_0)!)_p((pL_0)!)_p}\right) \cdot \frac{1}{p^{e_0}}\binom{n}{k} \pmod{p^r}.$$

Additionally, Corollary 2.35 and its proof were given in [JV] as Corollary 5.3. Note that a slightly different set of hypotheses are given here: rather than the stricter condition $r \geq s \geq q$, only $r \geq q$ and $s \geq q$ are imposed here. That is to say, no specific ordering between r and s is required. An analysis of the proof shows that this is valid.

Corollary 2.35. *Let p be an odd prime. Let $n, k, q, r, s \in \mathbb{Z}^+$. Let $e_0 \leq \nu_p\left(\binom{np^r}{kp^s}\right)$. If $r \geq q$ and $s \geq q$, then*

$$\frac{1}{p^{e_0}}\binom{np^r}{kp^s} \equiv \frac{1}{p^{e_0}}\binom{np^{r-1}}{kp^{s-1}} \pmod{p^q}.$$

That is,

$$\binom{np^r}{kp^s} \equiv \binom{np^{r-1}}{kp^{s-1}} \pmod{p^{q+e_0}}.$$

The key to the proof of Theorem 2.37 is now shown.

Lemma 2.36. *Let p be an odd prime. Let $r \in \mathbb{Z}^+$. Let $n, k \in \mathbb{N}$. Then*

$$g(np^r, kp) \equiv g\big(np^{r-1}, k\big) \pmod{p^r}$$

Proof. Write $k = jp^s$, where $p \nmid j$.

Case I. Suppose $s + 1 > r$. By Corollary 2.35, (with $p = p$, $n = n$, $k = j$, $q = r$, $r = r$, $s = s + 1$, and $e_0 = 0$),

$$\begin{aligned}\binom{np^r}{kp} &= \binom{np^r}{jp^{s+1}} \\ &\equiv \binom{np^{r-1}}{jp^s} \pmod{p^r} \\ &= \binom{np^{r-1}}{k}.\end{aligned}$$

Similarly,

$$\binom{2kp}{np^r} \equiv \binom{2k}{np^r} \pmod{p^r}.$$

Therefore,

$$\begin{aligned}g(np^r, kp) &= \binom{np^r}{kp}^2 \binom{2kp}{np^r} \\ &\equiv \binom{np^{r-1}}{k}^2 \binom{2k}{np^r} \pmod{p^r} \\ &= g\big(np^{r-1}, k\big).\end{aligned}$$

Case II. Suppose $s + 1 \leq r$. By Lemma 2.32 (with $p = p$, $n = n$, $k = j$, $r = r, r - 1$, and $s = s + 1, s$), $p^{r-s-1} \mid g(np^r, jp^{s+1})$ and $p^{r-s-1} \mid g(np^{r-1}, jp^s)$. By Corollary 2.35 (with $p = p$, $n = np^{r-s-1}$, $k = j$, $q = s + 1$, $r = r$, $s = s + 1$, and $e_0 = r - s - 1$),

$$\begin{aligned}\frac{1}{p^{r-s-1}}\binom{np^r}{kp} = \frac{1}{p^{r-s-1}}\binom{np^r}{jp^{s+1}} &= \frac{1}{p^{r-s-1}}\binom{p^{s+1}(np^{r-s-1})}{jp^{s+1}} \\ &\equiv \frac{1}{p^{r-s-1}}\binom{p^s(np^{r-s-1})}{jp^s} \pmod{p^{s+1}} \\ &= \frac{1}{p^{r-s-1}}\binom{np^{r-1}}{jp^s} = \frac{1}{p^{r-s-1}}\binom{np^{r-1}}{k}.\end{aligned}$$

Similarly,

$$\frac{1}{p^{r-s-1}}\binom{2kp}{np^r} \equiv \frac{1}{p^{r-s-1}}\binom{2k}{np^{r-1}} \pmod{p^{s+1}}.$$

Thus,

$$\begin{aligned}\left(\frac{1}{p^{r-s-1}}\right)^3 g\big(np^r, jp^{s+1}\big) &= \left(\frac{1}{p^{r-s-1}}\right)^3 \binom{np^r}{kp}^2 \binom{2kp}{np^r} \\ &\equiv \left(\frac{1}{p^{r-s-1}}\right)^3 \binom{np^{r-1}}{k}^2 \binom{2k}{np^{r-1}} \pmod{p^{s+1}} \\ &= \left(\frac{1}{p^{r-s-1}}\right)^3 g\big(np^{r-1}, jp^s\big).\end{aligned}$$

Thus,

$$\frac{1}{p^{r-s-1}} \cdot g\big(np^r, jp^{s+1}\big) \equiv \frac{1}{p^{r-s-1}} \cdot g\big(np^{r-1}, jp^s\big) \pmod{p^{s+1}}$$

Therefore,

$$g\big(np^r, jp^{s+1}\big) \equiv g\big(np^{r-1}, jp^s\big) \pmod{p^r}. \qquad \square$$

Theorem 2.37. *Let p be an odd prime. Let $r \in \mathbb{Z}^+$. Let $n \in \mathbb{N}$. Then*

$$\mathrm{Fra}_{np^r} \equiv \mathrm{Fra}_{np^{r-1}} \pmod{p^r}.$$

Proof. Notice

$$\begin{aligned}\mathrm{Fra}_{np^r} &= \sum_{k=0}^{np^r} g(np^r, k) \\ &\equiv \sum_{\substack{k=0 \\ p\mid k}}^{np^r} g(np^r, k) \pmod{p^r} && \text{(Corollary 2.33)} \\ &= \sum_{j=0}^{np^{r-1}} g(np^r, jp) \\ &\equiv \sum_{j=0}^{np^{r-1}} g\big(np^{r-1}, j\big) \pmod{p^r} && \text{(Lemma 2.36)} \\ &= \mathrm{Fra}_{np^{r-1}}. && \square\end{aligned}$$

Note. It is believed that Theorem 2.37 is the key to proving that particular primes are type II. However, no such proof has yet been found. While an inductive proof was previously attempted, that attempt was made before Theorem 2.37 was available.

2.3 Divisibility using finite automata

In addition to previously discussed methods, primes may be categorized using finite automata, which, in this context, are directed graphs used for finding specific values of a sequence. This subsection is dedicated to the use of this method.

2.3.1 Preliminaries

The following definition and theorem give the basis of this subsection.

Definition 2.38. A directed graph is a **finite automaton** if there exists $k \in \mathbb{Z}^+$ such that each vertex is labeled with an output value and has k edges labeled $0, 1, \ldots, k-1$ and there exists a unique vertex that is the initial state.

Theorem 2.39. *Let p^r be a prime power. The residues of the Franel numbers, mod p^r, are given by a finite automaton.*

Proof. In [E], it is shown that the Franel numbers are the diagonal terms of a generating function for a rational function. By a result from [RY], this proves that a finite automaton generates the residues. □

Note. The finite automata referenced in Theorem 2.39 may be found by the Integer Sequences package of Mathematica provided by Dr. E. Rowland.

2.3.2 Type I primes

By Proposition 2.27, 11 is the next prime after 3 that is type I. A new proof of this fact is presented using the finite automaton of the mod 11 residues of the Franel numbers.

Lemma 2.40. *The following is the finite automaton for determining the residues mod 11 of the Franel numbers.*

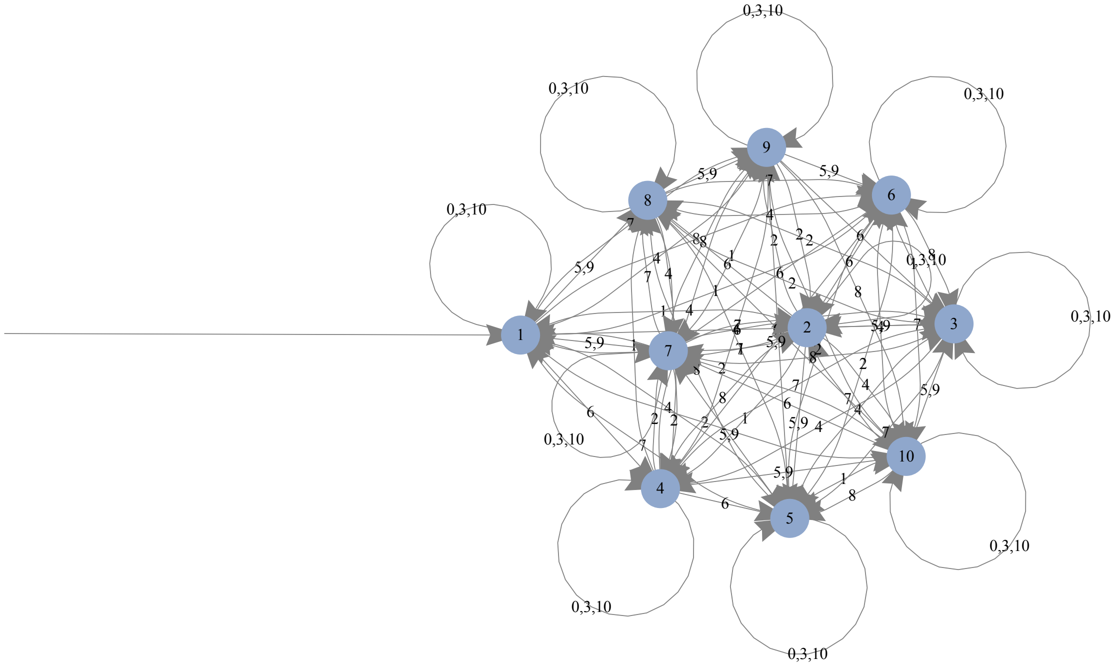


Figure 1: The mod 11 automaton

Proof. Apply Theorem 2.39. □

Lemma 2.40 recovers Proposition 2.27 for the prime 11.

Theorem 2.41. *The prime 11 is type I.*

Proof. In Figure 1 0 does not appear as a state. Therefore, by Lemma 2.40, $\mathrm{Fra}_n \not\equiv 0 \pmod{11}$ for all $n \in \mathbb{N}$. □

Using Theorem 2.39, any prime may be checked for the type I property in the same manner as Theorem 2.41. However, it is seen that generating the finite automata for residues is significantly more computationally difficult than using Corollary 2.26. However, additional applications of finite automata are explored in Subsubsection 2.3.3.

2.3.3 Type II and type III primes

Through computer experimentation, it was found that for some primes, which will be referred to as type II, the p-adic valuation of the n^{th} Franel number is related to the base-p

representation of n. This conjecture was confirmed in some cases using finite automata. This discussion starts with the prime 5.

Lemma 2.42. *The following is the finite automaton for determining the residues mod 5 of the Franel numbers.*

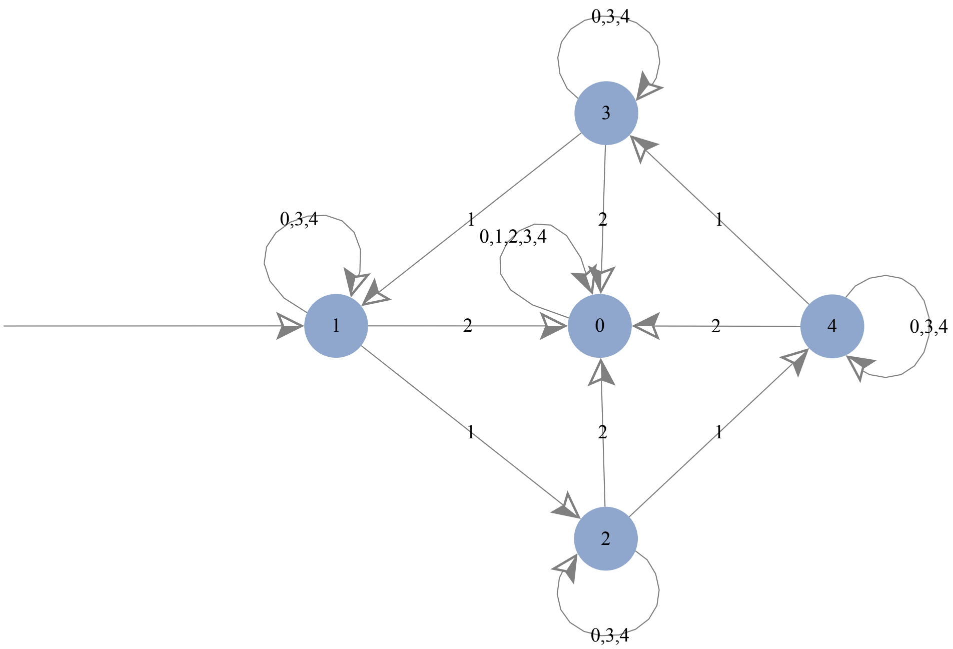


Figure 2: The mod 5 automaton

Proof. The proof follows directly from Theorem 2.39. □

Example 2.43. Consider the number $113 = 423_5$. To determine $\mathrm{Fra}_{113} \pmod 5$, begin at the initial state, indicated by the unlabeled edge in Figure 2. Then, read the digits of 113 in base-5 starting with the least significant digit. In this case, begin with 3 and remain at the initial vertex. Then, move to the vertex labeled 0 since the next most significant digit is 2. Finally, remain at the vertex labeled 0 since the most significant digit is 4. By this process, it is seen that $\mathrm{Fra}_{113} \equiv 0 \pmod 5$. Numerical checks confirm this congruence.

Lemma 2.42 recovers Theorem 2.24.

Theorem 2.24. *Let $n \in \mathbb{N}$. Then Fra_n is divisible by 5 if and only if n contains at least one 2 in its base-5 representation.*

Proof. Let $n_d n_{d-1} \cdots n_0$ be the base-5 representation of n.

($\Rightarrow$) Suppose n does not contain a 2 in its base-5 representation. Then by Lemma 2.42, as the digits $n_0, n_1, \ldots, n_d$ are read into the mod 5 automaton, the residue 0 never appears. Therefore, Fra_n is not divisible by 5.

($\Leftarrow$) Suppose n contains a 2 in its base-5 representation. Let α be an index of a digit of n that is 2 in base-5. By Lemma 2.42, regardless of which state has been reached prior to reading n_α, the state of 0 will be reached after reading n_α. Then, since any future digits return to 0, it is seen that $\mathrm{Fra}_n \equiv 0 \pmod 5$. Therefore, Fra_n is divisible by 5. □

A similar analysis yields the following.

Theorem 2.44. *Let $n \in \mathbb{N}$. Then Fra_n is divisible by 25 if and only if n contains at least two 2's in its base-5 representation.*

Proof. Theorem 2.39 yields the finite automaton for the residues (mod 25) of the Franel numbers. just as in the proof of Theorem 2.24, by analyzing the automaton, it is seen that 0 (mod 25) is reached if and only if there are two 2's in the base-5 representation of n. Then, once two 2's have been read in the base-5 representation of n, any future digits return to 0. That is, $\mathrm{Fra}_n \equiv 0 \pmod{25}$ if and only if n contains two 2's in its base-5 representation. □

Theorems 2.24 and 2.44 motivate the following definition.

Definition 2.45. For any prime p and any $n, k \in \mathbb{N}$, define $C_p(n,k)$ to be the number of $k's$ in the base-p representation of p.

Continuing in the spirit of Theorem 2.44, Theorems 2.46, 2.48, 2.50 arise. The proofs are similar to those of Theorems 2.24 and 2.44, and thus are omitted.

Theorem 2.46. *Let $n \in \mathbb{N}$. Then Fra_n is divisible by 125 if and only if n contains at least three 2's in its base-5 representation.*

Using Theorems 2.24, 2.44, and 2.46, Corollary 2.47 arises. The proofs of Corollaries 2.49 and 2.51 are similar, and so are omitted.

Corollary 2.47. *Let $n \in \mathbb{N}$. Then*

$$\nu_5(\mathrm{Fra}_n) \quad \begin{cases} = C_5(n,2) & \text{if } C_5(n,2) \leq 2 \\ > 2 & \text{if } C_5(n,2) > 2 \end{cases}$$

Proof.

Case I. Suppose $C_5(n,2) = 0$. By Theorem 2.24, $5 \nmid \mathrm{Fra}_n$. Therefore, $\nu_5(\mathrm{Fra}_n) = 0$.

Case II. Suppose $C_5(n,2) = 1$. By Theorem 2.24, $5 \mid \mathrm{Fra}_n$. By Theorem 2.44, $25 \nmid \mathrm{Fra}_n$. Therefore, $\nu_5(\mathrm{Fra}_n) = 1$.

Case III. Suppose $C_5(n,2) = 2$. By Theorem 2.44, $25 \mid \mathrm{Fra}_n$. By Theorem 2.46, $125 \nmid \mathrm{Fra}_n$. Therefore, $\nu_5(\mathrm{Fra}_n) = 2$.

Case IV. Suppose $C_5(n,3) > 2$. By Theorem 2.46, $125 \mid \mathrm{Fra}_n$. Therefore, $\nu_5(\mathrm{Fra}_n) \geq 3$. □

Theorem 2.48. *Let $n \in \mathbb{N}$. Then Fra_n is divisible by 7 if and only if n contains at least one 3 in its base-7 representation. Additionally, Fra_n is divisible by 49 if and only if n contains at least two 3's in its base-7 representation.*

Corollary 2.49. *Let $n \in \mathbb{N}$. If $C_7(n,3) \leq 2$, then $\nu_7(\mathrm{Fra}_n) \geq C_7(n,3)$. In particular, if $C_7(n,3) = 1$, then $\nu_7(\mathrm{Fra}_n) = C_7(n,3)$.*

Theorem 2.50. *Let $n \in \mathbb{N}$. Then Fra_n is divisible by 13 if and only if n contains at least one 6 in its base-13 representation. Additionally, Fra_n is divisible by 169 if and only if n contains at least two 6's in its base-13 representation.*

Corollary 2.51. *Let $n \in \mathbb{N}$. If $C_{13}(n,6) \leq 2$, then $\nu_{13}(\mathrm{Fra}_n) \geq C_{13}(n,6)$. In particular, if $C_{13}(n,6) = 1$, then $\nu_{13}(\mathrm{Fra}_n) = C_{13}(n,6)$.*

Recall the definition for type II primes, again stated here. Corollaries 2.47, 2.49, and 2.51 motivated Definition 2.52. Due to this definition, Corollaries 2.47, 2.49, and 2.51 will be collectively referred to as the small prime type II corollaries.

Definition 2.52. A prime p is **type II** if $\nu_p(\mathrm{Fra}_n) = C_p\big(n, \frac{p-1}{2}\big)$ for all $n \in \mathbb{N}$.

Example 2.53. Observe the following.

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
n (base-5)	0	1	2	3	4	10	11	12	13	14	20	21	22	23	24	30	31	32	33	34	40	41	42	43	44
$\nu_5(\mathrm{Fra}_n)$	0	0	1	0	0	0	0	1	0	0	1	1	2	1	1	0	0	1	0	0	0	0	1	0	0

It is apparent that $\nu_5(\mathrm{Fra}_n) = C_5(n, 2)$ for the first 25 natural numbers n. This observation has been verified computationally for the first million natural numbers. This, with Corollary 2.47 show that it is reasonable to believe that the prime 5 is type II. Similarly, it is reasonable to believe that the primes 7 and 13 are type II. However, these statements are still conjectures and have not been proven.

An additional condition to be a type II prime is given.

Theorem 2.54. *If a prime is type II, then it is congruent to 5 or 7* $\pmod 8$.

Proof. Let p be a type II prime. Then $p \mid \mathrm{Fra}_{\frac{p-1}{2}}$, since $\nu_p\Big(\mathrm{Fra}_{\frac{p-1}{2}}\Big) = C_p\big(\frac{p-1}{2}, \frac{p-1}{2}\big) = 1$. By Corollary 2.5 of [JV], $p \equiv 5 \pmod 8$ or $p \equiv 7 \pmod 8$. □

From the small prime type II corollaries, Theorems 2.25 and 2.54, the following conjecture arises.

Conjecture 2.55. The primes 5, 7, 13, 23, 31, 37, 47, 53, 71, 101, 103, 167, 181, 191, 197, 199, 223, 229, 263, 271, 293, 317, 349, 383, 397, 431, 439, 461, 479, 503, 509, 541, 557, 599, 607, 613, 647, 653, 677, 709, 719, 727, 733, 743, 751, 757, 797, 821, 823, 839, 877, 887, 911, 919, 991, 997 are type II.

Note. The small prime type II corollaries only apply to the primes 5, 7, and 13. That is, analogous statements have *not* been proven for the other primes. This means that the evidence is stronger that the primes 5, 7, and 13 are type II. However, Theorem 2.28 applies to all of the primes and of course, each prime given is congruent to 5 or 7 mod 5.

The final type of prime is again defined.

Definition 2.56. A prime p is **type III** if p is neither type I nor type II.

Example 2.57. Consider the prime 29. It is seen that $\nu_{29}(\mathrm{Fra}_{12}) = \nu_{29}(2046924400) = 1$ and there are zero 14's ($\frac{29-1}{2} = 14$) in the base-29 representation of 12. That is, $C_{29}(12, 14) = 0 \neq 1$. Thus, 29 is not type II.

Since $\nu_{29}(\mathrm{Fra}_{12}) = 1$, Fra_{12} is divisible by 29. Thus, 29 is not type I. Therefore, 29 is type III.

While currently only conjectures may be made regarding type II primes, proving that a prime p is type III may be achieved by finding a counterexample, that is, a natural number n such that $\nu_p(\mathrm{Fra}_n) \neq C_p\big(n, \frac{p-1}{2}\big)$, as shown in Example 2.57.

Proposition 2.58. *The primes 2, 29, 41, 59, 61, 67, 73, 79, 107, 109, 127, 131, 149, 151, 157, 173, 179, 227, 239, 251, 257, 269, 277, 281, 311, 337, 359, 367, 373, 389, 421, 449, 457, 463, 467, 487, 521, 563, 571, 577, 593, 631, 659, 661, 683, 691, 701, 739, 761, 769, 773, 787, 809, 829, 853, 857, 863, 883, 907, 937, 941, 967, 971, 983 are type III.*

Proof. Numerical examples show that these primes are neither type I nor type II. □

Note. The primes listed in Conjectures 2.55 and 2.58 do not appear in [OEIS].

3 Exploring 2-adic valuations

The 2-adic valuations of the Franel numbers produce interesting patterns. The outcomes may be used to produce the following tree which describes the 2-adic valuations of various Franel numbers of the index n up to 10000. The nodes of the tree below indicate the index of the Franel number whose 2-adic valuation is being considered. The nodes of the tree that have circles around them indicate the existence of a recurrence relation with other nodes. Let $m \in \mathbb{N}$, then the tree is created as follows.

It should be noted that this tree is created for n up to 10,000. When n is increased to 350000, at the 3rd level, where the level refers to the number of parent nodes a node has, there no longer exists a consistent recurrence for any node. However, very few n do not satisfy the recurrence relation, while the rest of the values of n do. It is seen that the 2-adic valuations of the Franel numbers provide certain recursions with a few exceptions, which appear to be categorizable.

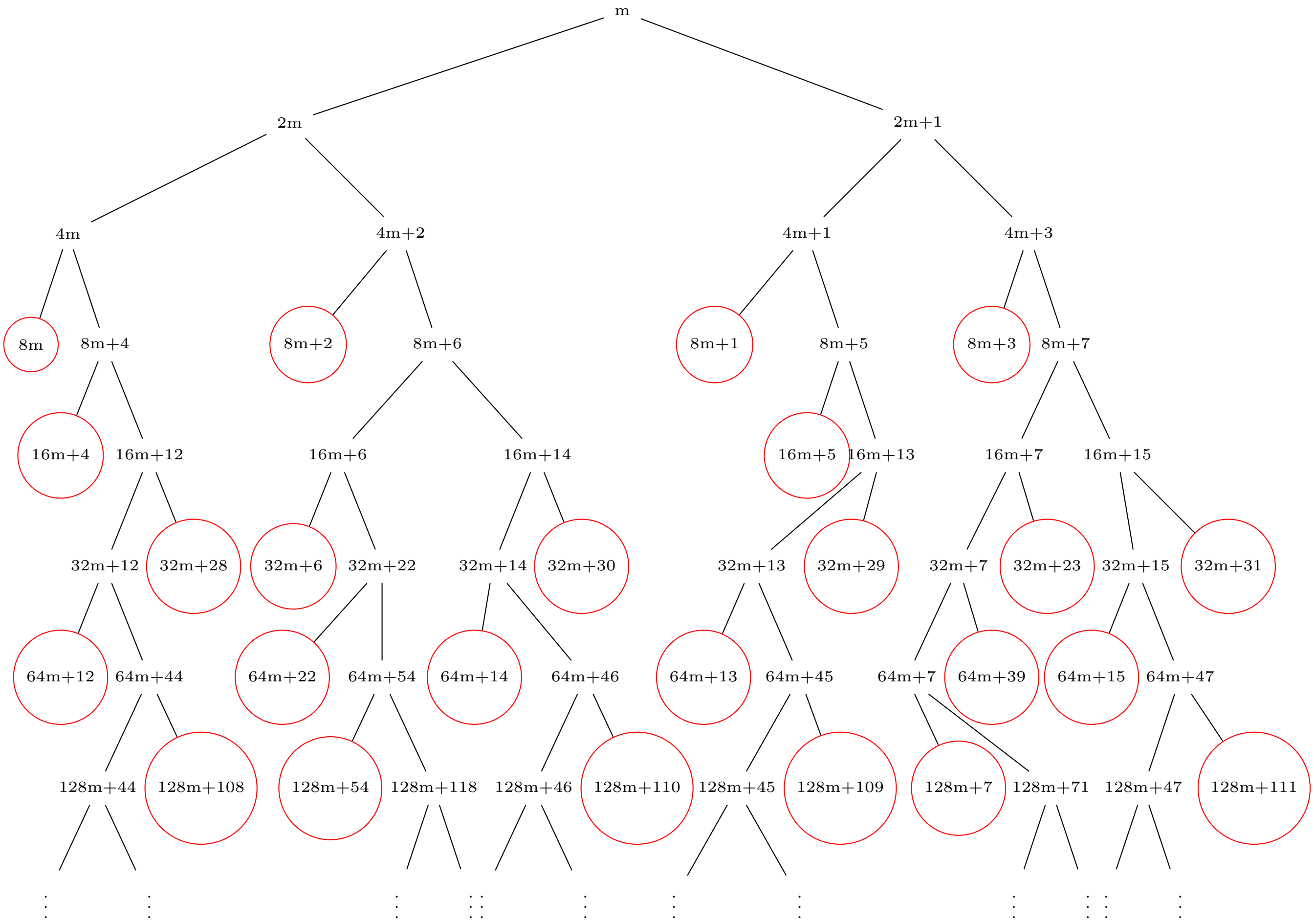


Figure 3: The 2-adic tree

3.1 Observations of the 3rd level of the tree

The following statements apply for n up to 7.7 million.

The relationship between the index n and the nodes of the form $am + b$ is that the node only applies to the n values that satisfy the form of a particular node, where $a = 2^c, b < a$ and $a, b, c \in \mathbb{N}$. For the node of $8m$, the exceptions to the previously supposed recurrence occur at $n = 349528$, 1398104, 2446680, 3495256, and 4543832.

Example 3.1. The Franel number with index 349528 is of the form $8m$, where $a = 8$, $b = 0$, and $m = 43691$. The Franel number with index $n = 87385$ is of the form $8m + 1$, where $a = 8, b = 1$ and $m = 10923$.

The following table is the list of indices that have exceptions to the recurrence found for $n = 8m$, the corresponding base-2 representation, and its index in the table, denoted by i.

n	base-2 of n	i
349528	$000\vert 01010101010101011000_2$	0
1398104	$001\vert 01010101010101011000_2$	1
2446680	$010\vert 01010101010101011000_2$	2
3495256	$011\vert 01010101010101011000_2$	3
4543832	$100\vert 01010101010101011000_2$	4
5592408	$101\vert 01010101010101011000_2$	5
6640984	$110\vert 01010101010101011000_2$	6
7689560	$111\vert 01010101010101011000_2$	7

Table 1: $8m$ exceptions

Note that the exceptions of n can be categorized. The last 20 digits on the right of the base-2 representation are the same for all, but the digits on the left ascend in increasing order from 0 to 7 in binary corresponding to the index.

Conjecture 3.2. The n terms of the form $8m$ can be expressed as:

$$349528 + i \times 2^{20},$$

where i is the corresponding index in the table. This has been verified for n up to 7.7 million.

This result is remarkable because it repeats for other nodes. In particular, the same pattern is observed for the $8m + 1$, $8m + 2$ and $8m + 3$ nodes.

By observing the exceptions for the $8m + 1$ recurrence, it is observed that the last 18 digits on the right of the base-2 representation are the same for all, but the digits on the left ascend in increasing order starting from 0 in binary corresponding to the index.

Conjecture 3.3. The n terms of the form $8m + 1$ can be expressed as:

$$87385 + i \times 2^{18},$$

where i is the corresponding index to the exception. This has been verified for n up to 7.7 million.

The last 19 digits on the right of the base-2 representation are the same for all, but the digits on the left ascend in increasing order starting from 0 in binary corresponding to the index.

Conjecture 3.4. The n terms in the form $8m + 2$ can be expressed as:

$$349530 + i \times 2^{19},$$

where i is the corresponding index to the exception. This has been verified for n up to 7.7 million.

The last 19 digits on the right of the base-2 representation are the same for all, but the digits on the left ascend in increasing order from starting from 0 in binary corresponding to the index.

Conjecture 3.5. The n terms in the form $8m + 3$ can be expressed as:

$$349531 + i \times 2^{19},$$

where i is the corresponding index to the exception. This has been verified for n up to 7.7 million.

It seems that the exceptions can be categorized by formulas given a node. Therefore $8m, 8m + 1, 8m + 2$, and $8m + 3$ are almost recurrences with certain exceptions of n. Some areas of concern are that there may be exceptions for other recurrences for greater values of n. That is, for levels beyond 3 it is believed that there may be certain exceptions to the supposed recurrences. However, due to computational limitations, this claim has not been verified.

3.2 Observations of other levels

The following conjectures have been formulated to describe some of the behavior in the tree.

Conjecture 3.6. For a fixed m, the following relations hold:

(i) $\nu_2(\mathrm{Fra}_{16m+4}) + 1 = \nu_2(\mathrm{Fra}_{16m+5})$.

(ii) $\nu_2(\mathrm{Fra}_{32m+28}) + 2 = \nu_2(\mathrm{Fra}_{32m+29}) + 1 = \nu_2(\mathrm{Fra}_{32m+30})$.

(iii) $\nu_2(\mathrm{Fra}_{64m+12})+6 = \nu_2(\mathrm{Fra}_{64m+13})+5 = \nu_2(\mathrm{Fra}_{64m+14}) = \nu_2(\mathrm{Fra}_{64m+22})+4 = \nu_2(\mathrm{Fra}_{64m+15})$.

(iv) $\nu_2(\mathrm{Fra}_{128m+108}) + 6 = \nu_2(\mathrm{Fra}_{128m+109}) + 5 = \nu_2(\mathrm{Fra}_{128m+110}) + 4 = \nu_2(\mathrm{Fra}_{128m+111})$.

These conjectures have been verified for n up to 100000.

Upon further investigation of the recurrences listed above, almost every one of these recurrences is related by the existence of shifts with recurrences in earlier levels, with the one exception of the node $32m + 31$. Though it is unclear if such a recurrence exists for this particular node among other nodes, this portion of the tree is under investigation so it can be compared to other recurrences within the tree. It has been proved that there exists an exception to the known recurrence of the node $32m + 31$ at $n = 5592415$. By observing the base-2 representation of this number, it can be observed that it is 7 digits away from a shift by a power of 2 of the earlier exceptions for the nodes of level 3. It is unclear why the first exception occurs at this position, but in order to investigate more, a much greater amount of data is required.

4 Other results

A few results unrelated to the main topics of discussion are presented here. For example, almost every Franel number is even.

Proposition 4.1. *Every Franel number except* Fra_0 *is even.*

Proof. $\mathrm{Fra}_0 = 1$ is not even. Let $n \geq 1 \in \mathbb{N}$. Then

$$\sum_{k=0}^{n} \binom{n}{k}^3 \equiv \sum_{k=0}^{n} \binom{n}{k} = 2^n \equiv 0 \pmod 2$$

Therefore, Fra_n is even. □

4.1 Initial conditions of the Franel occurrence

While the Franel numbers are given explicitly by a finite sum, a recurrence also gives their values. The recurrence for the Franel numbers is given again here.

Theorem 1.2. *Let $n \geq 2$ be a natural number. Then*

$$n^2 \operatorname{Fra}_n = \left(7n^2 - 7n + 2\right) \operatorname{Fra}_{n-1} + 8(n-1)^2 \operatorname{Fra}_{n-2}$$

with $\operatorname{Fra}_0 = 1$ *and* $\operatorname{Fra}_1 = 2$.

When the initial conditions of the Franel recurrence are of the form i and $2i$, integer sequences result.

Proposition 4.2. *Let* $(\operatorname{Fra}_{n,i_0,i_1})_{n=0}^{\infty}$ *denote the sequence generated by the Franel recurrence with initial conditions* $\operatorname{Fra}_0 = i_0$ *and* $\operatorname{Fra}_1 = i_1$. *Let* $i \in \mathbb{Z}^+$. *Let* $n \in \mathbb{N}$. *Then* $\operatorname{Fra}_{n,i,2i} = i \operatorname{Fra}_{n,1,2}$. *That is, the sequence generated by the Franel recurrence with initial conditions i and $2i$ is simply the sequence of Franel numbers multiplied by i.*

Proof. Proceed by induction on n. Let $i \in \mathbb{Z}^+$.

Base step. Clearly

$$\operatorname{Fra}_{0,i,2i} = i = i \operatorname{Fra}_{0,1,2} \quad \text{and} \quad \operatorname{Fra}_{1,i,2i} = 2i = i \operatorname{Fra}_{0,1,2} .$$

Inductive step. Suppose $\operatorname{Fra}_{n-1,i,2i} = i \operatorname{Fra}_{n-1,1,2}$ and $\operatorname{Fra}_{n-2,i,2i} = i \operatorname{Fra}_{n-2,1,2}$. Then

$$\begin{aligned} n^2 \operatorname{Fra}_{n,i,2i} &= \left(7n^2 - 7n + 2\right) \operatorname{Fra}_{n-1,i,2i} + 8(n-1)^2 \operatorname{Fra}_{n-2,i,2i} \\ &= \left(7n^2 - 7n + 2\right) i \operatorname{Fra}_{n-1,1,2} + 8(n-1)^2 i \operatorname{Fra}_{n-2,1,2} \quad \text{(inductive hypothesis)} \\ &= i\left(\left(7n^2 - 7n + 2\right) \operatorname{Fra}_{n-1,1,2} + 8(n-1)^2 \operatorname{Fra}_{n-2,1,2}\right) \\ &= i n^2 \operatorname{Fra}_{n,1,2} . \end{aligned}$$

Therefore, $\operatorname{Fra}_{n,i,2i} = i \operatorname{Fra}_{n,1,2}$ for all $n \in \mathbb{N}$. □

Corollary 4.3. *Notation as in Proposition 4.2. For all positive integers i, the sequence* $(\operatorname{Fra}_{n,i,2i})$ *is an integer sequence.*

Proof. Apply Proposition 4.2 and the fact that the Franel numbers are integers. □

Example 4.4. The Franel numbers have the initial conditions of $\mathrm{Fra}_0 = 1$ and $\mathrm{Fra}_1 = 2$. The first 10 elements of the Franel numbers are 1, 2, 10, 56, 346, 2252, 15184, 104960, 739162, and 5280932.

Let $\mathrm{Fra}_{0,3,6} = 3$ and $\mathrm{Fra}_{1,3,6} = 6$. Then the first 10 elements of the sequence are 3, 6, 30, 168, 1038, 6756, 45552, 314880, 2217486, and 15842796, as expected, since the initial conditions of $\mathrm{Fra}_{0,3,6} = 3$ are 3 times that of the Franel numbers and the elements of $\mathrm{Fra}_{n,3,6} = 3$ are also 3 times the corresponding Franel numbers.

If the initial conditions of the Franel recurrence are not of the form i and $2i$, then it is conjectured that non-integer sequences are produced. For example, consider the sequence $(\mathrm{Fra}_{n,3,4})$. The first 10 elements of the sequence are 3, 4, 22, 121.78, 753.56, 4903.70, 33063.75, 228553.78, 1.61×10^6, and 1.15×10^7 (rounded to two decimal places). It is apparent that not all of these elements are integers.

The following conjectures arise from Proposition 4.2. Currently, proofs are not available for these statements, however, Conjecture 4.5 has been verified computationally for i_0 up to 500, for i_1 up to 1000, among n up to 5000.

Conjecture 4.5. Notation as in Proposition 4.2. The sequence Fra_{n,i_0,i_1} is an integer sequence if and only if $i_0 = i$ and $i_1 = 2i$ for some $i \in \mathbb{Z}^+$.

5 Further work

It is clear that more questions can be explored regarding the Franel numbers and similar sequences. Specifically, a deeper understanding of which primes are which types as well as of the 2-adic valuations are desired. It also seems that for some type III primes, the p-adic valuations are bounded below by the amount of occurrences of particular digits (putting emphasis on the fact that there are more than one) in the base-p representations. Additionally, as the Franel numbers are the sums of the cubes of the binomial coefficients, it is natural to look at the sums of powers of binomial coefficients for higher powers.

Definition 5.1. Let $a \in \mathbb{Z}^+$. Let $n \in \mathbb{N}$. The $\boldsymbol{n^{\text{th}}}$ ***a*-SPB number**,[4] denoted $\mathrm{SPB}_{n,a}$ is

$$\sum_{k=0}^{n} \binom{n}{k}^a.$$

Example 5.2. The 3-SPB numbers are the Franel numbers.

Example 5.3. The 5-SPB numbers are given by $\sum\limits_{k=0}^{n} \binom{n}{k}^5$.

1. The 0th 5-SPB number is $\mathrm{SPB}_{0,5} = \sum\limits_{k=0}^{0} \binom{0}{k}^5$=1.
2. The 1st 5-SPB number is $\mathrm{SPB}_{1,5} = \sum\limits_{k=0}^{1} \binom{1}{k}^5$=2.
3. The 10th 5-SPB number is $\mathrm{SPB}_{10,5} = \sum\limits_{k=0}^{10} \binom{10}{k}^5 = 1883210876284$.

The following conjecture has been verified computationally for a up to 100 checking the first 250 primes for divisibility among n up to 2500.

Conjecture 5.4. For each $a \in \mathbb{Z}^+$, there exists a prime which does not divide any element of the sequence $(\mathrm{SPB}_{n,a})_{n=0}^{\infty}$ if and only if a is odd. That is to say, there exists a type I prime with regards to the sequence $(\mathrm{SPB}_{n,a})$ if and only if a is odd.

Note that Proposition 4.1 may be generalized.

Proposition 5.5. *Let $a \in \mathbb{Z}^+$. Every a-SPB number except* $\mathrm{SPB}_{0,a}$ *is even.*

Proof. The proof is similar to that of Proposition 4.1. □

The following conjecture arises from Proposition 5.5. It has been verified computationally for a up to 250 and for n up to 2500.

Conjecture 5.6. For each positive integer $a \geq 2$ and each $n \in \mathbb{Z}^+$, $\frac{1}{2}\,\mathrm{SPB}_{n,a}$ is odd if and only if n is a power of 2.[5]

[4] Note that SPB is used since the numbers are the Sums of Powers of Binomial coefficients. The "C" is omitted for brevity.

[5] By Proposition 5.5, $\frac{1}{2}\,\mathrm{SPB}_{n,a}$ is even for all $a \geq 2$ and all $n \in \mathbb{Z}^+$.

6 Acknowledgments

This work was carried out during the 2014 Mathematical Sciences Research Institute Undergraduate Program (MSRI-UP) which is funded by the National Science Foundation (grant No. DMS-1156499) and the National Security Agency (grant No. H-98230-13-1-0262). The authors would like to thank program director Dr. Herbert Medina, academic mentors Drs. Victor Moll and Eric Rowland, group leader Asia Wyatt, and our fellow MSRI-UP peers.

Additionally, the first author would like to thank Drs. John Alongi and Vadim Ponomarenko, whose support made his research possible.

The second author would like to thank Dr. Margaret Robinson for helping to make this project possible.

The third author would like to thank Drs. William Silver, Michael King, and Laura Toma for their inspiration and advice.

References

[E] Ekhad, S. B., "A linear recurrence equation for the diagonal coefficients of the power series of $\frac{1}{1-x-y-z+4xyz}$", Preprint (2012), 1 p.; available from `http://www.math.rutgers.edu/~zeilberg/tokhniot/oMultiAlmkvistZeilberger3`.

[Fr] Franel, J., *Comments on question 42 by Laisant. L'Intermediaire des Mathematiciens* 1:45–47, 1894.

[G] Granville, A., "Binomial coefficients modulo prime powers," *Organic Mathematics* (1997), 253-276

[JLF] Jarvis, A.F., Larcombe, P., and French, D., "On small prime divisibility of the Catalan-Larcombe-French sequence," *Indian J. Math.* **47** (2005), 159–181.

[JV] Jarvis, A.F., and Verrill, H. A., "Supercongruences for the Catalan-Larcombe-French numbers," *Ramanujan J.* **22** no. 2 (2010), 171–186.

[Le] Legendre, A. M., *Theorie des Nombres*, Firmin Didot Freres, Paris, 1830.

[Lu] Lucas, E., “Théorie des Fonctions Numériques Simplement Périodiques” *Amer. J. Math.* **1** no.2 (1878), 184–196.

“Théorie des Fonctions Numériques Simplement Périodiques” *Amer. J. Math.* **1** no.3 (1878), 197–240.

“Théorie des Fonctions Numériques Simplement Périodiques” *Amer. J. Math.* **1** no.4 (1878), 289–321.

[OEIS] “The online encyclopedia of integer sequences” `http://oeis.org/`.

[PWZ] Petkovsek, M., Wilf, H., and Zeilberger, D., *A=B*, 1st Ed., A.K. Peters, Massachusetts, 1996.

[RY] Rowland, E., and Yassawi, R., “Automatic congruences for diagonals of rational functions,” *J. Théor. Nombres Bordeaux*, to appear, 2014, `http://arxiv.org/abs/1310.8635`.

[S] Strehl, V., “Binomial identities-combinatorial and algorithmic aspects,” *Discrete Math.* **136** (1994), 309–346.