Congruences for diagonals of rational power series

Eric Rowland   Reem Yassawi

University of Liège, Belgium

2014 October 16

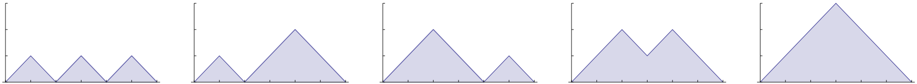
Outline

1. Algebraic sequences
2. Automatic sequences
3. Diagonals of rational power series
4. Congruence gallery

Algebraic sequences

A sequence $(a_n)_{n\geq 0}$ of integers is algebraic if its generating function $\sum_{n\geq 0} a_n x^n$ is algebraic over $\mathbb{Q}(x)$.

Catalan numbers $C(n)_{n\geq 0} = 1, 1, 2, 5, 14, 42, 132, 429, \ldots$ [A000108]

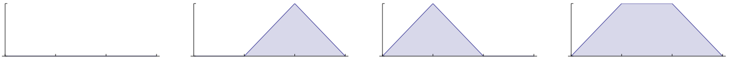


$C(3) = 5$
$C(n) = \frac{1}{n+1}\binom{2n}{n}$

$$y = \sum_{n\geq 0} C(n)x^n = \frac{1-\sqrt{1-4x}}{2x} \text{ satisfies } xy^2 - y + 1 = 0.$$

Motzkin numbers

Motzkin numbers $M(n)_{n\geq 0} = 1, 1, 2, 4, 9, 21, 51, 127, \ldots$ [A001006]



$M(3) = 4$

$y = \sum_{n\geq 0} M(n)x^n$ satisfies $x^2y^2 + (x-1)y + 1 = 0$.

Other algebraic sequences:

- sequence of Fibonacci numbers, etc.
- number of binary trees avoiding a pattern
- number of planar maps with n vertices

Arithmetic properties

Let p^α be a prime power.

Question

If $(a_n)_{n\geq 0}$ is algebraic, what does $(a_n \bmod p^\alpha)_{n\geq 0}$ look like?

Deutsch and Sagan (2006) studied Catalan and Motzkin numbers, Riordan numbers, central binomial and trinomial coefficients, etc.

$$C(n)_{n\geq 0} = 1, 1, 2, 5, 14, 42, 132, 429, \dots$$
$$(C(n) \bmod 2)_{n\geq 0} = 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, \dots$$

Theorem

For all $n \geq 0$, $C(n)$ is odd if and only if $n+1$ is a power of 2.

Deutsch and Sagan gave a combinatorial proof.

Motzkin numbers modulo 8

$M(n)_{n\geq 0} = 1, 1, 2, 4, 9, 21, 51, 127, \ldots$ [A001006]

Deutsch, Sagan, and Amdeberhan conjectured necessary and sufficient conditions for $M(n)$ to be divisible by 4.

…and that no Motzkin number is divisible by 8.

Theorem (Eu–Liu–Yeh 2008)

For all $n \geq 0$, $M(n) \not\equiv 0 \mod 8$.

Catalan numbers modulo 4

To prove this, Eu, Liu, and Yeh determined $C(n) \bmod 4 \ldots$

Theorem (Eu–Liu–Yeh)

For all $n \geq 0$,

$$C(n) \bmod 4 = \begin{cases} 1 & \text{if } n = 2^a - 1 \text{ for some } a \geq 0 \\ 2 & \text{if } n = 2^b + 2^a - 1 \text{ for some } b > a \geq 0 \\ 0 & \text{otherwise.} \end{cases}$$

In particular, $C(n) \not\equiv 3 \mod 4$ for all $n \geq 0$.

Catalan numbers modulo 8

…and $C(n)$ mod 8:

Theorem 4.2. *Let C_n be the nth Catalan number. First of all, $C_n \not\equiv_8 3$ and $C_n \not\equiv_8 7$ for any n. As for other congruences, we have*

$$C_n \equiv_8 \begin{cases} 1 & \text{if } n = 0 \text{ or } 1; \\ 2 & \text{if } n = 2^a + 2^{a+1} - 1 \text{ for some } a \geq 0; \\ 4 & \text{if } n = 2^a + 2^b + 2^c - 1 \text{ for some } c > b > a \geq 0; \\ 5 & \text{if } n = 2^a - 1 \text{ for some } a \geq 2; \\ 6 & \text{if } n = 2^a + 2^b - 1 \text{ for some } b - 2 \geq a \geq 0; \\ 0 & \text{otherwise}. \end{cases}$$

Catalan numbers modulo 16

Liu and Yeh (2010) determined $C(n)$ mod 16:

Theorem 5.5. *Let c_n be the n-th Catalan number. First of all, $c_n \not\equiv_{16} 3, 7, 9, 11, 15$ for any n. As for the other congruences, we have*

$$c_n \equiv_{16} \begin{cases} \left.\begin{array}{c} 1 \\ 5 \\ 13 \end{array}\right\} & \textit{if} \quad d(\alpha) = 0 \ \textit{and} \quad \begin{cases} \beta \le 1, \\ \beta = 2, \\ \beta \ge 3, \end{cases} \\ \left.\begin{array}{c} 2 \\ 10 \end{array}\right\} & \textit{if} \quad d(\alpha) = 1,\ \alpha = 1 \ \textit{and} \quad \begin{cases} \beta = 0 \ \textit{or} \ \beta \ge 2, \\ \beta = 1, \end{cases} \\ \left.\begin{array}{c} 6 \\ 14 \end{array}\right\} & \textit{if} \quad d(\alpha) = 1,\ \alpha \ge 2 \ \textit{and} \quad \begin{cases} (\alpha = 2, \beta \ge 2) \ \textit{or} \ (\alpha \ge 3, \beta \le 1), \\ (\alpha = 2, \beta \le 1) \ \textit{or} \ (\alpha \ge 3, \beta \ge 2), \end{cases} \\ \left.\begin{array}{c} 4 \\ 12 \end{array}\right\} & \textit{if} \quad d(\alpha) = 2 \ \textit{and} \quad \begin{cases} zr(\alpha) \equiv_2 0, \\ zr(\alpha) = 1, \end{cases} \\ \quad 8 & \textit{if} \quad d(\alpha) = 3, \\ \quad 0 & \textit{if} \quad d(\alpha) \ge 4. \end{cases}$$

where $\alpha = (CF_2(n+1) - 1)/2$ and $\beta = \omega_2(n+1)$ (or $\beta = \min\{i \mid n_i = 0\}$).

They also determined $C(n)$ mod 64.

Questions

$C(n)$ mod 2^α seems to reflect the base-2 digits of n.

Does this hold for other combinatorial sequences modulo p^α?

Are piecewise functions the best notation?

Power series congruences

Kauers, Krattenthaler, and Müller developed a systematic method for producing congruences modulo 2^α (2012) and modulo 3^α (2013).

Let $\Phi(z) = \sum_{n \geq 0} z^{2^n}$.

$$\begin{aligned}\sum_{n=0}^{\infty} \mathrm{Cat}_n\, z^n &= 32z^5 + 16z^4 + 6z^2 + 13z + 1 + \left(32z^4 + 32z^3 + 20z^2 + 44z + 40\right)\Phi(z)\\ &+ \left(16z^3 + 56z^2 + 30z + 52 + \frac{12}{z}\right)\Phi^2(z) + \left(32z^3 + 60z + 60 + \frac{28}{z}\right)\Phi^3(z)\\ &+ \left(32z^3 + 16z^2 + 48z + 18 + \frac{35}{z}\right)\Phi^4(z) + \left(32z^2 + 44\right)\Phi^5(z)\\ &+ \left(48z + 8 + \frac{50}{z}\right)\Phi^6(z) + \left(32z + 32 + \frac{4}{z}\right)\Phi^7(z) \qquad \text{modulo } 64\end{aligned}$$

Outline

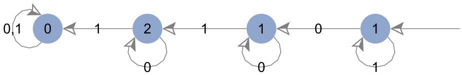
Catalan numbers modulo 4

Theorem (Eu–Liu–Yeh)

For all $n \geq 0$,

$$C(n) \bmod 4 = \begin{cases} 1 & \text{if } n = 2^a - 1 \text{ for some } a \geq 0 \\ 2 & \text{if } n = 2^b + 2^a - 1 \text{ for some } b > a \geq 0 \\ 0 & \text{otherwise.} \end{cases}$$

Process the binary digits of n, starting with the least significant digit.



This machine is a deterministic finite automaton with output (DFAO).

Automatic sequences

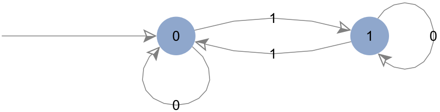
A sequence $(a_n)_{n\geq 0}$ is k-automatic if there is DFAO whose output is a_n when fed the base-k digits of n.

$(C(n) \bmod 4)_{n\geq 0} = 1, 1, 2, 1, 2, 2, 0, 1, \ldots$ is 2-automatic.

Let $T(n) = $ (number of 1s in the binary representation of n) mod 2.
The Thue–Morse sequence

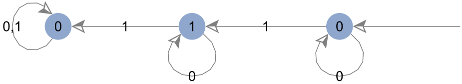
$$T(n)_{n\geq 0} = 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, \ldots$$

is 2-automatic. It is also cube-free.

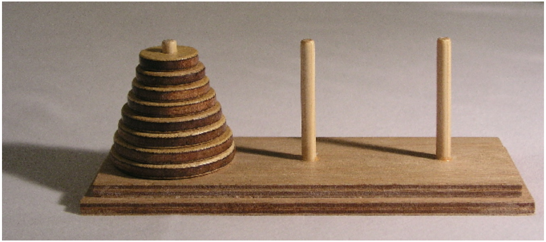


Examples of 2-automatic sequences

- Characteristic sequence of powers of 2:



- Minimal solution to the “infinite” tower of Hanoi puzzle

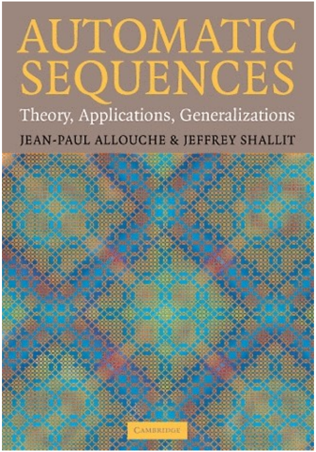


Automatic sequences

Automatic sequences have been studied extensively.

Büchi 1960:
Every eventually periodic sequence is k-automatic for every $k \geq 2$.

Several natural characterizations of automatic sequences are known.



Algebraic characterization

Theorem (Christol–Kamae–Mendès France–Rauzy 1980)

Let $(a_n)_{n\geq 0}$ be a sequence of elements in $\mathbb{F}_p$. Then $(a_n)_{n\geq 0}$ is p-automatic if and only if $\sum_{n\geq 0} a_n x^n$ is algebraic over $\mathbb{F}_p(x)$.

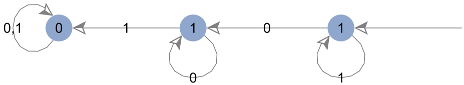
Algebraic sequences of integers modulo p are p-automatic.

$y = 1 + 1x + 0x^2 + 1x^3 + 0x^4 + 0x^5 + 0x^6 + \cdots$ satisfies

$$xy^2 + y + 1 = 0$$

in $\mathbb{F}_2[\![x]\!]$.

The proof is constructive.



Prime powers?

Outline

Converting algebraic to rational

The diagonal of a formal power series is

$$\mathcal{D}\left(\sum_{n,m\geq 0} a_{n,m}x^n y^m\right) := \sum_{n\geq 0} a_{n,n}x^n.$$

Algebraic sequences can be realized as diagonals of rational functions.

Proposition (Furstenberg 1967)

Let $P(x,y) \in \mathbb{Q}[x,y]$ such that $\frac{\partial P}{\partial y}(0,0) \neq 0$.
If $f(x) \in \mathbb{Q}[\![x]\!]$ is a power series with $f(0) = 0$ and $P(x, f(x)) = 0$, then

$$f(x) = \mathcal{D}\left(\frac{y\frac{\partial P}{\partial y}(xy,y)}{P(xy,y)/y}\right).$$

Catalan numbers

$$y = \sum_{n \geq 0} C(n) x^n = \frac{1 - \sqrt{1 - 4x}}{2x} \text{ satisfies } xy^2 - y + 1 = 0.$$

Since $C(0) = 1 \neq 0$, consider $y = 0 + \sum_{n \geq 1} C(n) x^n$, which satisfies

$$P(x, y) := x(y+1)^2 - (y+1) + 1 = 0.$$

Then $\frac{\partial P}{\partial y}(0,0) = -1 \not\equiv 0 \mod 2$, so $\sum_{n \geq 1} C(n) x^n$ is the diagonal of

$$\begin{aligned}
\frac{y(2xy^2 + 2xy - 1)}{xy^2 + 2xy + x - 1} = \quad & 0x^0y^0 + 1x^0y + 0x^0y^2 + 0x^0y^3 + 0x^0y^4 + 0x^0y^5 + \cdots \\
& + 0x^1y^0 + 1x^1y + 0x^1y^2 - 1x^1y^3 + 0x^1y^4 + 0x^1y^5 + \cdots \\
& + 0x^2y^0 + 1x^2y + 2x^2y^2 + 0x^2y^3 - 2x^2y^4 - 1x^2y^5 + \cdots \\
& + 0x^3y^0 + 1x^3y + 4x^3y^2 + 5x^3y^3 + 0x^3y^4 - 5x^3y^5 + \cdots \\
& + 0x^4y^0 + 1x^4y + 6x^4y^2 + 14x^4y^3 + 14x^4y^4 + 0x^4y^5 + \cdots \\
& + 0x^5y^0 + 1x^5y + 8x^5y^2 + 27x^5y^3 + 48x^5y^4 + 42x^5y^5 + \cdots \\
& + \cdots .
\end{aligned}$$

Automata for diagonals of rational power series

Theorem (Denef–Lipshitz 1987)

Let $R(x, y)$ and $Q(x, y)$ be polynomials in $\mathbb{Z}_p[x, y]$ such that $Q(0, 0) \not\equiv 0 \mod p$, and let $\alpha \geq 1$.
Then the coefficient sequence of

$$\mathcal{D}\left(\frac{R(x, y)}{Q(x, y)}\right) \bmod p^\alpha$$

is p-automatic.

Here $\mathbb{Z}_p$ denotes the set of p-adic integers.

Algorithm

Let $0 \leq d \leq p-1$.
The Cartier operator is the map on $\mathbb{Z}_p[\![x,y]\!]$ defined by

$$\Lambda_{d,d}\left(\sum_{n,m\geq 0} a_{n,m} x^n y^m\right) := \sum_{n,m\geq 0} a_{pn+d,pm+d} x^n y^m.$$

To compute an automaton for the coefficients of $\mathcal{D}\left(\frac{R(x,y)}{Q(x,y)}\right)$ mod p^α:

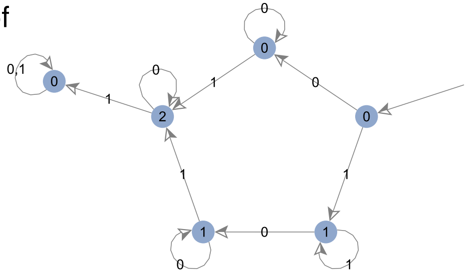
1. Compute the image of $\frac{R(x,y)}{Q(x,y)} = \frac{R(x,y)\cdot Q(x,y)^{p^{\alpha-1}-1}}{Q(x,y)^{p^{\alpha-1}}}$ under each $\Lambda_{d,d}$.
2. Draw an edge labeled d from $\frac{s(x,y)}{Q(x,y)^{p^{\alpha-1}}}$ to $\frac{t(x,y)}{Q(x,y)^{p^{\alpha-1}}}$ if

$$\Lambda_{d,d}\left(\frac{s(x,y)}{Q(x,y)^{p^{\alpha-1}}}\right) = \frac{t(x,y)}{Q(x,y)^{p^{\alpha-1}}}.$$

3. Iterate, and stop when all images have been computed.

Catalan numbers modulo 4

$\sum_{n \geq 1} C(n)x^n$ is the diagonal of
$$\frac{y(2xy^2 + 2xy - 1)}{xy^2 + 2xy + x - 1}.$$



By computing an automaton for a sequence $\bmod p^\alpha$, we can answer...

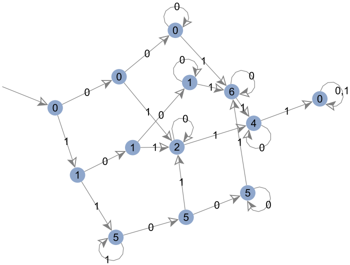
- Are there forbidden residues?
- What is the limiting distribution of residues (if it exists)?
- Is the sequence eventually periodic?

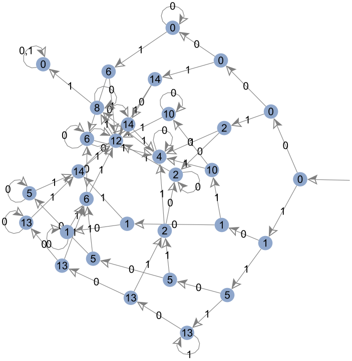
Outline

Catalan numbers modulo 8 and 16

Theorem (Liu–Yeh)

For all $n \geq 0$, $C(n) \not\equiv 9 \mod 16$.





Catalan numbers modulo 2^α

Theorem

For all $n \geq 0$*,*

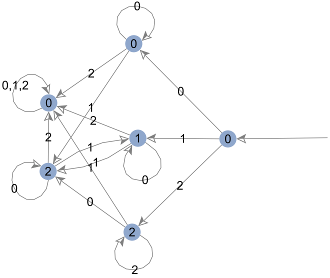
- $C(n) \not\equiv 17, 21, 26 \mod 32$*,*
- $C(n) \not\equiv 10, 13, 33, 37 \mod 64$*,*
- $C(n) \not\equiv 18, 54, 61, 65, 66, 69, 98, 106, 109 \mod 128$*,*
- $C(n) \not\equiv 22, 34, 45, 62, 82, 86, 118, 129, 130, 133, 157, 170, 178, 253 \mod 256$*.*

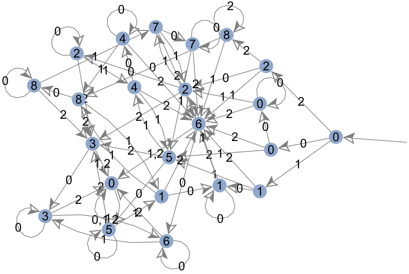
Only $\approx 35\%$ of the residues modulo 512 are attained by some $C(n)$.

Open question

Does the fraction of residues modulo 2^α *that are attained by some Catalan number tend to* 0 *as* α *gets large?*

Catalan numbers modulo 3^α





There are no known forbidden residues modulo 3^α.

Open question

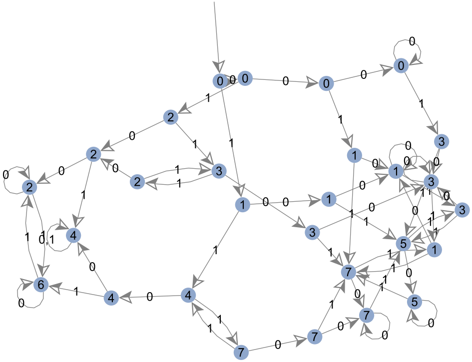
Do there exist α and r such that $C(n) \not\equiv r \mod 3^\alpha$ for all $n \geq 0$?

Motzkin numbers modulo 8

Theorem (Eu–Liu–Yeh)

For all $n \geq 0$, $M(n) \not\equiv 0 \mod 8$.

Proof:



Motzkin numbers modulo p^2

Theorem

For all $n \geq 0$, $M(n) \not\equiv 0 \mod 5^2$.

(2 seconds; 144 states)

Theorem

For all $n \geq 0$, $M(n) \not\equiv 0 \mod 13^2$.

(10 minutes; 2125 states)

Conjecture

Let $p \in \{31, 37, 61\}$. For all $n \geq 0$, $M(n) \not\equiv 0 \mod p^2$.

Open question

Are there infinitely many p such that $M(n) \not\equiv 0 \mod p^2$ for all $n \geq 0$?

A few more well-known sequences

Riordan numbers: $R(n)_{n \geq 0} = 1, 0, 1, 1, 3, 6, 15, 36, \ldots$ [A005043]

Theorem

For all $n \geq 0$, $R(n) \not\equiv 16 \mod 32$.

Number of directed animals:
$P(n)_{n \geq 0} = 1, 1, 2, 5, 13, 35, 96, 267, \ldots$ [A005773]

Theorem

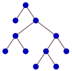
For all $n \geq 0$, $P(n) \not\equiv 16 \mod 32$.

Number of restricted hexagonal polyominoes:
$H(n)_{n \geq 0} = 1, 1, 3, 10, 36, 137, 543, 2219, \ldots$ [A002212]

Theorem

For all $n \geq 0$, $H(n) \not\equiv 0 \mod 8$.

Binary trees avoiding a pattern

Let a_n be the number of $(n+1)$-leaf binary trees avoiding  .

$(a_n)_{n\geq 0} = 1, 1, 2, 5, 14, 41, 124, 385, \ldots$ [A159771]

The generating function satisfies

$$2x^2y^2 - (3x^2 - 2x + 1)y + x^2 - x + 1 = 0.$$

Theorem

For all $n \geq 0$,

$$\begin{aligned} a_n &\not\equiv 3 \mod 4, \\ a_n &\not\equiv 13 \mod 16, \\ a_n &\not\equiv 21 \mod 32, \\ a_n &\not\equiv 37 \mod 64. \end{aligned}$$

Permutations avoiding a pair of patterns

Let a_n be the number of permutations of length n avoiding 3412 and 2143.

$(a_n)_{n\geq 0} = 1, 1, 2, 6, 22, 86, 340, 1340, \ldots$ [A029759]

Atkinson (1998) showed that $\sum_{n\geq 0} a_n x^n$ is algebraic.

Theorem

For all $n \geq 0$,

$$\begin{aligned}
a_n &\not\equiv 10, 14 && \mod 16,\\
a_n &\not\equiv 18 && \mod 32,\\
a_n &\not\equiv 34, 54 && \mod 64,\\
a_n &\not\equiv 44, 66, 102 && \mod 128,\\
a_n &\not\equiv 20, 130, 150, 166, 188, 204, 212, 214, 220, 236, 252 && \mod 256.
\end{aligned}$$

Apéry numbers

$A(n) = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2$ arose in Apéry's proof that $\zeta(3)$ is irrational.

$A(n)_{n \geq 0} = 1, 5, 73, 1445, 33001, 819005, 21460825, \ldots$ [A005259]

Straub (2014): $\sum_{n \geq 0} A(n) x^n$ is the diagonal of

$$\frac{1}{(1 - x_1 - x_2)(1 - x_3 - x_4) - x_1 x_2 x_3 x_4}.$$

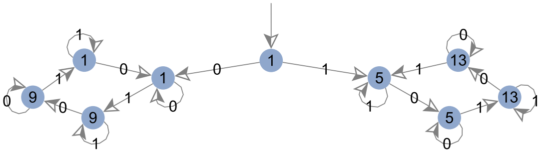
Computing automata allows us to resolve some conjectures.

Apéry numbers modulo 16

Chowla, Cowles, and Cowles conjectured, and Gessel (1982) proved,

$$A(n) \bmod 8 = \begin{cases} 1 & \text{if } n \text{ is even} \\ 5 & \text{if } n \text{ is odd.} \end{cases}$$

Gessel asked whether $A(n)$ is periodic modulo 16.



Theorem

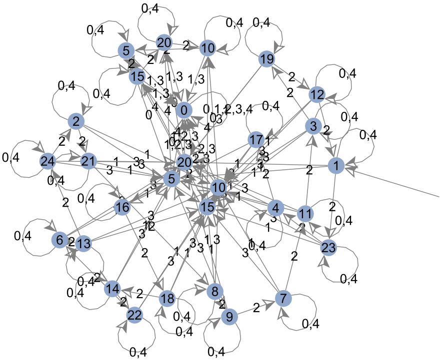
The sequence $(A(n) \bmod 16)_{n \geq 0}$ *is not eventually periodic.*

Apéry numbers modulo 25

Beukers (1995) conjectured that if there are α 1s and 3s in the standard base-5 representation of n then $A(n) \equiv 0 \mod 5^\alpha$. (Proved recently by Delaygue.)

Theorem

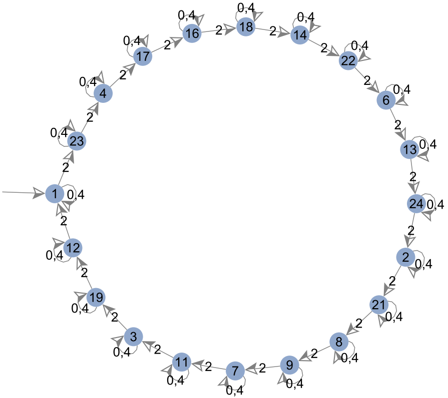
Beukers' conjecture is true for $\alpha = 2$.



Apéry numbers modulo 25

Theorem

Let $e_2(n)$ be the number of 2s in the standard base-5 representation of n. If n contains no 1 or 3 in base 5, then $A(n) \equiv (-2)^{e_2(n)} \mod 25$.



Scope

Christol (1990) conjectured that if $(a_n)_{n \geq 0}$ is an integer sequence which

- is holonomic (satisfies a linear recurrence with polynomial coefficients) and
- grows at most exponentially,

then $(a_n)_{n \geq 0}$ is the diagonal of a rational function.

$(n!)_{n \geq 0}$ grows too quickly to be the diagonal of a rational function.

If the conjecture is true, then essentially every sequence that occurs in combinatorics is p-automatic when reduced modulo p^α.

Symbolic p^α

Write $n = n_\ell \cdots n_1 n_0$ and $m = m_\ell \cdots m_1 m_0$ in base p.
Lucas' theorem:

$$\binom{n}{m} \equiv \prod_{i=0}^{\ell} \binom{n_i}{m_i} \mod p.$$

For the Apéry numbers, Gessel (1982) proved

$$A(n) \equiv \prod_{i=0}^{\ell} A(n_i) \mod p.$$

Our method doesn't allow α to vary (for fixed p).