Computing congruences for combinatorial sequences

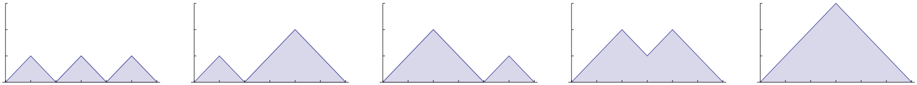
Eric Rowland Reem Yassawi

Université de Liège

2015 August 6

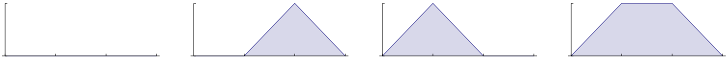
Catalan and Motzkin numbers

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



$C(3) = 5$

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



$M(3) = 4$

Arithmetic properties

Question

What does a combinatorial sequence look like modulo p^α?

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

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

Theorem

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

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 $C(n) \bmod 4$ ...

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*

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

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

Is there a systematic way to obtain this information?

$C(n) \bmod 2^\alpha$ reflects 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 (2012) developed a systematic method for producing congruences of power series.

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

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

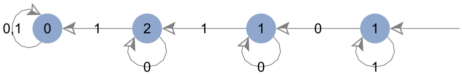
Automatic sequences

Theorem (Eu–Liu–Yeh)

For all $n \geq 0$,

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

This automaton outputs $C(n) \bmod 4$ when fed the base-2 digits of n, starting with the least significant digit:



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

Automata for diagonals of rational power series

The diagonal of a formal power series is

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

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.

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

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

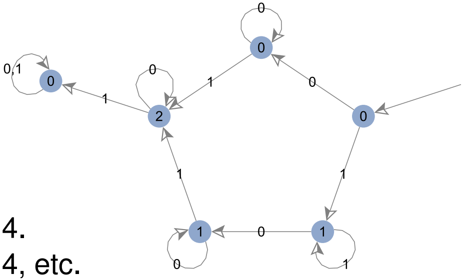
$$\Lambda_{d,d}\left(\frac{s(x,y)}{Q(x,y)^{p^{\alpha-1}}}\right) \equiv \frac{t(x,y)}{Q(x,y)^{p^{\alpha-1}}} \mod p^\alpha.$$

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

$$\frac{y(2xy^2 + 2xy - 1)}{xy^2 + 2xy + x - 1}.$$



Apply $\Lambda_{0,0}$ and reduce modulo 4.
Apply $\Lambda_{1,1}$ and reduce modulo 4, etc.

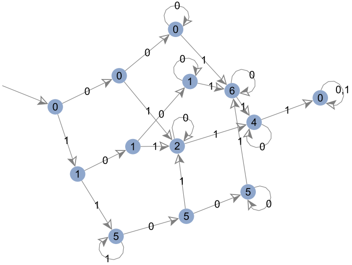
By computing an automaton for a sequence $\bmod p^\alpha$, we can answer...

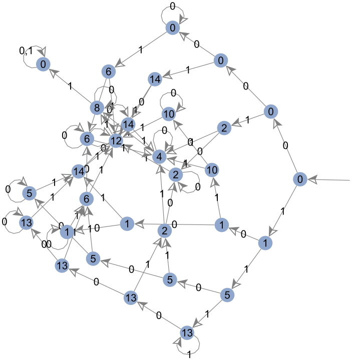
- Are there forbidden residues?
- What is the limiting distribution of residues (if it exists)?
- Is the sequence eventually periodic?
- Many other decidable properties.

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

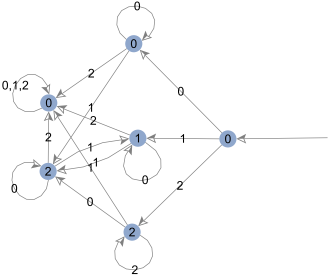
For all $n \geq 0$,

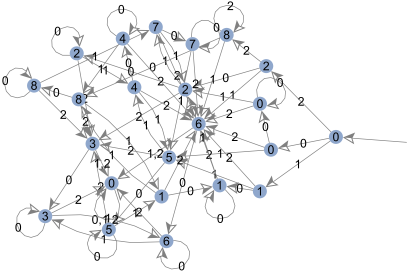
- $C(n) \not\equiv 17, 21, 26 \mod 32$,
- $C(n) \not\equiv 10, 13, 33, 37 \mod 64$,
- $C(n) \not\equiv 18, 54, 61, 65, 66, 69, 98, 106, 109 \mod 128$,
- $C(n) \not\equiv 22, 34, 45, 62, 82, 86, 118, 129, 130, 133, 157, 170, 178, 253 \mod 256$.

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?





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* $n \geq 0$*?*

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

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

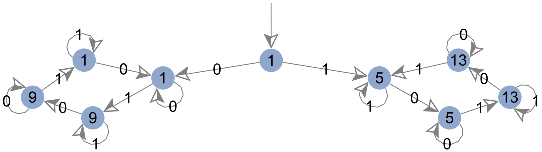
Computing automata allows us to resolve some conjectures.

Apéry numbers modulo 16

Gessel (1982) proved a conjecture of Chowla–Cowles–Cowles that

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

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



Theorem

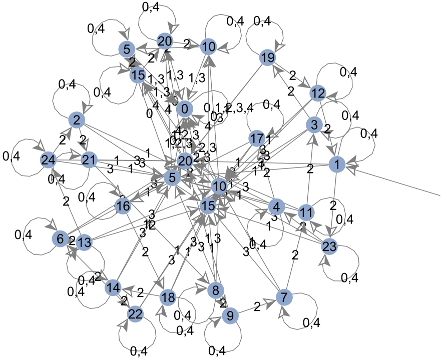
The sequence $(A(n) \bmod 16)_{n \geq 0}$ *is not eventually periodic.*

Apéry numbers modulo 25

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

Theorem

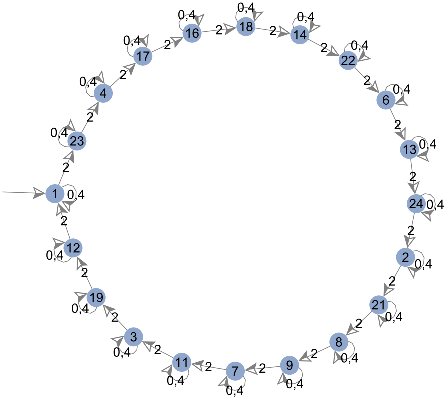
Beukers' conjecture is true for $\alpha = 2$.



Apéry numbers modulo 25

Theorem

Let $e_2(n)$ be the number of 2s in the 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 an integer sequence

- is holonomic and
- grows at most exponentially,

then it 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 many sequences that occur in combinatorics are p-automatic when reduced modulo p^{α}.

Constant terms of Laurent polynomials

$C(n)$ is the coefficient of x^0 in $(1-x)(\frac{1}{x}+2+x)^n$.

With Zeilberger, we showed how to compute automata for constant terms modulo p^α.

What is the relationship between diagonals of rational power series and constant terms of $P(x)Q(x)^n$?