Automatic Lucas-type congruences

Applications of Computer Algebra — ACA 2023

Session on D-Finite Functions and Beyond: Algorithms, Combinatorics, and Arithmetic

Warsaw, Poland — July 17–21, 2023

Armin Straub

July 19, 2023

University of South Alabama

THM Lucas 1878

$$\binom{n}{k} \equiv \binom{n_0}{k_0}\binom{n_1}{k_1}\binom{n_2}{k_2}\cdots \pmod{p}$$

where n_i and k_i are the base p digits of n and k.

includes joint work with:

Joel Henningsen
(Baylor University)

Slides available at:
`http://arminstraub.com/talks`

Diagonals

$$\sum_{n_1,\ldots,n_d \geqslant 0} a(n_1,\ldots,n_d)\, x_1^{n_1} \cdots x_d^{n_d}$$

multivariate series

$$\sum_{n \geqslant 0} a(n,\ldots,n)\, t^n$$

diagonal

EG

$$\frac{1}{1-x-y}$$

Diagonals

$$\sum_{n_1,\ldots,n_d \geqslant 0} a(n_1,\ldots,n_d)\, x_1^{n_1} \cdots x_d^{n_d}$$

multivariate series

$$\sum_{n \geqslant 0} a(n,\ldots,n)\, t^n$$

diagonal

EG

$$\frac{1}{1-x-y} = \sum_{k=0}^{\infty} (x+y)^k$$

Diagonals

$$\sum_{n_1,\ldots,n_d \geqslant 0} a(n_1,\ldots,n_d)\, x_1^{n_1} \cdots x_d^{n_d}$$

multivariate series

$$\sum_{n \geqslant 0} a(n,\ldots,n)\, t^n$$

diagonal

EG

$$\frac{1}{1-x-y} = \sum_{k=0}^{\infty} (x+y)^k$$

diagonal: $$\sum_{n=0}^{\infty} \binom{2n}{n} t^n = \frac{1}{\sqrt{1-4t}}$$

Diagonals

$$\sum_{n_1,\ldots,n_d \geqslant 0} a(n_1,\ldots,n_d)\, x_1^{n_1} \cdots x_d^{n_d}$$

multivariate series

$$\sum_{n \geqslant 0} a(n,\ldots,n)\, t^n$$

diagonal

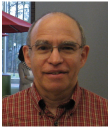
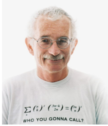
EG $$\frac{1}{1-x-y} = \sum_{k=0}^{\infty} (x+y)^k$$ diagonal: $$\sum_{n=0}^{\infty} \binom{2n}{n} t^n = \frac{1}{\sqrt{1-4t}}$$

THM Gessel, Zeilberger, Lipshitz 1981–88

The diagonal of a rational function is D-finite.

More generally, the diagonal of a D-finite function is D-finite.

$F \in K[[x_1,\ldots,x_d]]$ is D-finite if its partial derivatives span a finite-dimensional vector space over $K(x_1,\ldots,x_d)$.

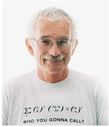



Diagonals: an example from positivity

CONJ Kauers-Zeilberger 2008

All Taylor coefficients of the following function are positive:

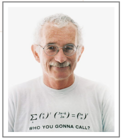
$$\frac{1}{1-(x+y+z+w)+2(yzw+xzw+xyw+xyz)+4xyzw}.$$



Diagonals: an example from positivity

CONJ Kauers-Zeilberger 2008 All Taylor coefficients of the following function are positive:

$$\frac{1}{1-(x+y+z+w)+2(yzw+xzw+xyw+xyz)+4xyzw}.$$



- Would imply conjectured positivity of Lewy–Askey function

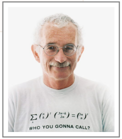
$$\frac{1}{(1-x)(1-y)+(1-x)(1-z)+\ldots+(1-z)(1-w)}.$$

Non-negativity proved by a very general result of Scott–Sokal ('14)

Diagonals: an example from positivity

CONJ Kauers-Zeilberger 2008: All Taylor coefficients of the following function are positive:

$$\frac{1}{1-(x+y+z+w)+2(yzw+xzw+xyw+xyz)+4xyzw}.$$



- Would imply conjectured positivity of Lewy–Askey function

$$\frac{1}{(1-x)(1-y)+(1-x)(1-z)+\ldots+(1-z)(1-w)}.$$

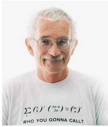
Non-negativity proved by a very general result of Scott–Sokal ('14)

PROP S-Zudilin 2015: The **diagonal coefficients** of the Kauers–Zeilberger function are

$$D(n)=\sum_{k=0}^{n}\binom{n}{k}^2\binom{2k}{n}^2.$$

- $D(n)$ is an example of an **Apéry-like sequence**.

Diagonals: an example from positivity



CONJ Kauers-Zeilberger 2008

All Taylor coefficients of the following function are positive:

$$\frac{1}{1-(x+y+z+w)+2(yzw+xzw+xyw+xyz)+4xyzw}.$$

- Would imply conjectured positivity of Lewy–Askey function

$$\frac{1}{(1-x)(1-y)+(1-x)(1-z)+\ldots+(1-z)(1-w)}.$$

Non-negativity proved by a very general result of Scott–Sokal ('14)

PROP S-Zudilin 2015

The **diagonal coefficients** of the Kauers–Zeilberger function are

$$D(n)=\sum_{k=0}^{n}\binom{n}{k}^2\binom{2k}{n}^2.$$

- $D(n)$ is an example of an **Apéry-like sequence**.

Q S-Zudilin 2015

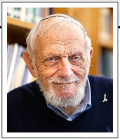
Can we conclude the conjectured positivity from the positivity of $D(n)$ together with the (easy) positivity of $\frac{1}{1-(x+y+z)+2xyz}$?

Characterizations of diagonals

EG Diagonals of rational functions

- $F(x) \quad = \quad C$-finite sequences

Characterizations of diagonals

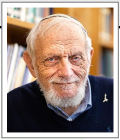


EG Diagonals of rational functions

- $F(x)$ = C-finite sequences
- $F(x,y)$ = sequences with algebraic GF (Furstenberg '67)

To see the latter, express the diagonal as $\frac{1}{2\pi i}\int_{|x|=\varepsilon} F\left(x, \frac{z}{x}\right)\frac{\mathrm{d}x}{x}$.

Characterizations of diagonals



EG Diagonals of rational functions

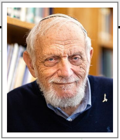
- $F(x)$ $=$ C-finite sequences
- $F(x,y)$ $=$ sequences with algebraic GF (Furstenberg '67)

To see the latter, express the diagonal as $\frac{1}{2\pi i}\int_{|x|=\varepsilon} F\left(x, \frac{z}{x}\right)\frac{\mathrm{d}x}{x}$.

THM Bostan, Lairez, Salvy '17: Diagonals of rational functions $=$ (multiple) binomial sums



Characterizations of diagonals



EG Diagonals of rational functions

- $F(x)$ = C-finite sequences
- $F(x,y)$ = sequences with algebraic GF (Furstenberg '67)

To see the latter, express the diagonal as $\frac{1}{2\pi i}\int_{|x|=\varepsilon} F\left(x, \frac{z}{x}\right)\frac{\mathrm{d}x}{x}$.

THM Bostan, Lairez, Salvy '17

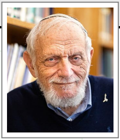
Diagonals of rational functions = (multiple) binomial sums

CONJ Christol '90

Diagonals of rational functions over $\mathbb{Q}$ ($\subseteq$ known)
= globally bounded, D-finite sequences

(i.e. $cd^n a_n \in \mathbb{Z}$ for $c, d \in \mathbb{Z}$ and at most exponential growth)

Characterizations of diagonals



EG Diagonals of rational functions

- $F(x)$ = C-finite sequences
- $F(x, y)$ = sequences with algebraic GF (Furstenberg '67)

To see the latter, express the diagonal as $\frac{1}{2\pi i}\int_{|x|=\varepsilon} F\left(x, \frac{z}{x}\right)\frac{\mathrm{d}x}{x}$.

THM Bostan, Lairez, Salvy '17

Diagonals of rational functions = (multiple) binomial sums

CONJ Christol '90

Diagonals of rational functions over $\mathbb{Q}$ ($\subseteq$ known)
= globally bounded, D-finite sequences

(i.e. $cd^n a_n \in \mathbb{Z}$ for $c, d \in \mathbb{Z}$ and at most exponential growth)

- Open: example of a diagonal that requires more than 3 variables

Though we have numerous candidates.

Automatic automata

THM Rowland, Yassawi '15: If an integer sequence $A(n)$ is the diagonal of $F(\boldsymbol{x}) \in \mathbb{Z}(\boldsymbol{x})$, then the reductions $A(n) \pmod{p^r}$ are p-**automatic**.

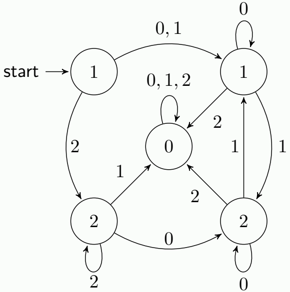
Constructive proof of results by Denef and Lipshitz '87.

Automatic automata

THM Rowland, Yassawi '15: If an integer sequence $A(n)$ is the diagonal of $F(\boldsymbol{x}) \in \mathbb{Z}(\boldsymbol{x})$, then the reductions $A(n) \pmod{p^r}$ are p-**automatic**.

Constructive proof of results by Denef and Lipshitz '87.

EG Catalan numbers $C(n)$ modulo 3:



$$C(35) = 3{,}116{,}285{,}494{,}907{,}301{,}262 \equiv 1 \pmod 3$$

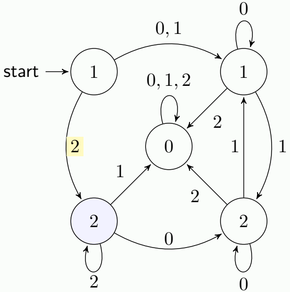
Instead via automaton:

$35 = 1\ 0\ 2\ 2$ in base 3

THM Rowland, Yassawi '15: If an integer sequence $A(n)$ is the diagonal of $F(\boldsymbol{x}) \in \mathbb{Z}(\boldsymbol{x})$, then the reductions $A(n) \pmod{p^r}$ are p-**automatic**.

Constructive proof of results by Denef and Lipshitz '87.

EG Catalan numbers $C(n)$ modulo 3:



$$C(35) = 3{,}116{,}285{,}494{,}907{,}301{,}262$$
$$\equiv 1 \pmod 3$$

Instead via automaton:

$35 = 1\ 0\ 2\ 2$ in base 3

$C(2)$

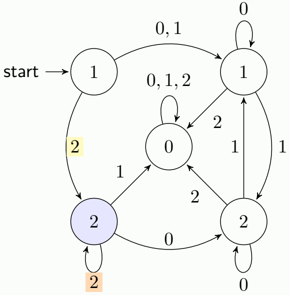
$C(2) \equiv 2$

Automatic automata

THM Rowland, Yassawi '15: If an integer sequence $A(n)$ is the diagonal of $F(\boldsymbol{x}) \in \mathbb{Z}(\boldsymbol{x})$, then the reductions $A(n) \pmod{p^r}$ are p-**automatic**.

Constructive proof of results by Denef and Lipshitz '87.

EG Catalan numbers $C(n)$ modulo 3:



$$C(35) = 3{,}116{,}285{,}494{,}907{,}301{,}262$$
$$\equiv 1 \pmod 3$$

Instead via automaton:

$35 = 1\ 0\ 2\ 2$ in base 3

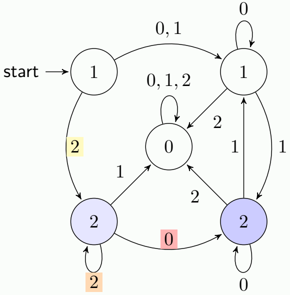
$C(2)$ $\qquad C(2) \equiv 2$

$C(8)$ $\qquad C(2\ 2) \equiv 2$

THM Rowland, Yassawi '15: If an integer sequence $A(n)$ is the diagonal of $F(\boldsymbol{x}) \in \mathbb{Z}(\boldsymbol{x})$, then the reductions $A(n) \pmod{p^r}$ are p-**automatic**.

Constructive proof of results by Denef and Lipshitz '87.

EG Catalan numbers $C(n)$ modulo 3:



$$C(35) = 3{,}116{,}285{,}494{,}907{,}301{,}262$$
$$\equiv 1 \pmod{3}$$

Instead via automaton:

$35 = 1\ 0\ 2\ 2$ in base 3

$C(2)$ $\qquad C(2) \equiv 2$

$C(8)$ $\qquad C(22) \equiv 2$

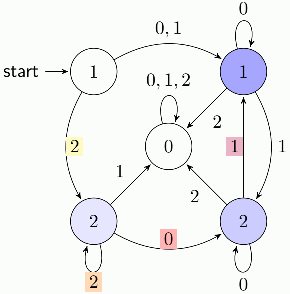
$C(022) \equiv 2$

Automatic automata

THM Rowland, Yassawi '15: If an integer sequence $A(n)$ is the diagonal of $F(\boldsymbol{x}) \in \mathbb{Z}(\boldsymbol{x})$, then the reductions $A(n) \pmod{p^r}$ are p-**automatic**.

Constructive proof of results by Denef and Lipshitz '87.

EG Catalan numbers $C(n)$ modulo 3:



$$C(35) = 3{,}116{,}285{,}494{,}907{,}301{,}262 \equiv 1 \pmod 3$$

Instead via automaton:

$35 = 1\,0\,2\,2$ in base 3

$C(2)$ $\quad C(2) \equiv 2$

$C(8)$ $\quad C(2\,2) \equiv 2$

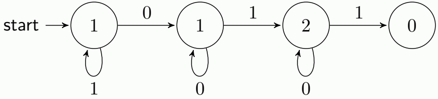
$\quad C(0\,2\,2) \equiv 2$

$C(35)$ $\quad C(1\,0\,2\,2) \equiv 1$

THM Rowland, Yassawi '15 — If an integer sequence $A(n)$ is the diagonal of $F(\boldsymbol{x}) \in \mathbb{Z}(\boldsymbol{x})$, then the reductions $A(n) \pmod{p^r}$ are p-**automatic**.

Constructive proof of results by Denef and Lipshitz '87.

EG Rowland, Yassawi '15 — Catalan numbers $C(n)$ modulo 4:

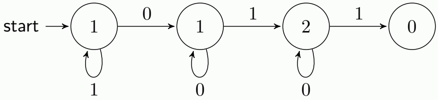


Automatic automata

THM Rowland, Yassawi '15 — If an integer sequence $A(n)$ is the diagonal of $F(\boldsymbol{x}) \in \mathbb{Z}(\boldsymbol{x})$, then the reductions $A(n) \pmod{p^r}$ are p-**automatic**.

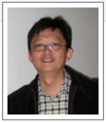
Constructive proof of results by Denef and Lipshitz '87.

EG Rowland, Yassawi '15 — Catalan numbers $C(n)$ modulo 4:



THM Eu, Liu, Yeh '08

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

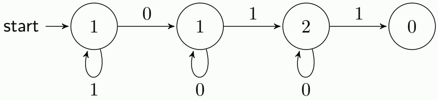


Automatic automata

THM Rowland, Yassawi '15 If an integer sequence $A(n)$ is the diagonal of $F(\boldsymbol{x}) \in \mathbb{Z}(\boldsymbol{x})$, then the reductions $A(n) \pmod{p^r}$ are p-**automatic**.

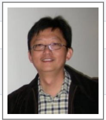
Constructive proof of results by Denef and Lipshitz '87.

EG Rowland, Yassawi '15 Catalan numbers $C(n)$ modulo 4:



THM Eu, Liu, Yeh '08

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



COR $C(n) \not\equiv 3 \pmod{4}$

Things quickly get more complicated

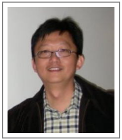
- Liu–Yeh (2010) also determine the Catalan numbers modulo 16 and 64.

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*

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

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

$$\begin{aligned} \omega_p(n) &= p\text{-adic valuation of } n \\ CF_p(n) &= n \,/\, p^{\omega_p(n)} \\ d(n) &= \text{sum of 2-adic digits of } n \end{aligned}$$



- For comparison: the corresponding minimal automaton has 26 states.

A different approach to congruences

THM Kauers, Krattenthaler, Müller '12

The Catalan numbers modulo 64 are determined by

$$\begin{aligned}\sum_{n=0}^{\infty} C(n)x^n \equiv\ & 1 + 13x + 6x^2 + 16x^4 + 32x^5 \\ & +(40 + 44x + 20x^2 + 32x^3 + 32x^4)\Phi(x) \\ & +(12x^{-1} + 52 + 30x + 56x^2 + 16x^3)\Phi(x)^2 \\ & +(28x^{-1} + 60 + 60x + 32x^3)\Phi(x)^3 \\ & +(35x^{-1} + 18 + 48x + 16x^2 + 32x^3)\Phi(x)^4 \\ & +(44 + 32x^2)\Phi(x)^5 + (50x^{-1} + 8 + 48x)\Phi(x)^6 \\ & +(4x^{-1} + 32 + 32x)\Phi(x)^7 \pmod{64}\end{aligned}$$

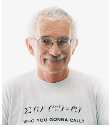
where

$$\Phi(x) = \sum_{n=0}^{\infty} x^{2^n}.$$



- Such expressions can be automatically obtained modulo any power of 2.
- For comparison: the corresponding minimal automaton has 134 states.

Constant terms and p-schemes



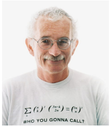
- Rowland and Zeilberger '14 construct congruence automata for **constant terms** $A(n) = \operatorname{ct}[P(\boldsymbol{x})^n Q(\boldsymbol{x})]$.

EG

$$C(n) = \operatorname{ct}[(x^{-1} + 2 + x)^n (1 - x)]$$ Catalan numbers

$$\sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k} = \operatorname{ct}\left[\frac{(x+1)(x+y)(x+y+1)}{xy}\right]^n$$ Apéry numbers

Constant terms and p-schemes



- Rowland and Zeilberger '14 construct congruence automata for **constant terms** $A(n) = \mathrm{ct}[P(\boldsymbol{x})^n Q(\boldsymbol{x})]$.

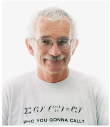
EG

$$C(n) = \mathrm{ct}[(x^{-1} + 2 + x)^n (1 - x)]$$ Catalan numbers

$$\sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k} = \mathrm{ct}\left[\frac{(x+1)(x+y)(x+y+1)}{xy}\right]^n$$ Apéry numbers

- Start with the state $A_0(n) = \mathrm{ct}[P(\boldsymbol{x})^n Q(\boldsymbol{x})]$.

All states mod p^r.



- Rowland and Zeilberger '14 construct congruence automata for **constant terms** $A(n) = \operatorname{ct}[P(\boldsymbol{x})^n Q(\boldsymbol{x})]$.

EG

$$C(n) = \operatorname{ct}[(x^{-1} + 2 + x)^n (1 - x)]$$ Catalan numbers

$$\sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k} = \operatorname{ct}\left[\frac{(x+1)(x+y)(x+y+1)}{xy}\right]^n$$ Apéry numbers

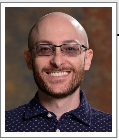
- Start with the state $A_0(n) = \operatorname{ct}[P(\boldsymbol{x})^n Q(\boldsymbol{x})]$.

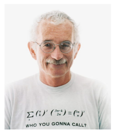
All states mod p^r.

- For each state $A_i(n) = \operatorname{ct}[P_i(\boldsymbol{x})^n Q_i(\boldsymbol{x})]$ and each $k \in \{0, 1, \ldots, p-1\}$,

$$A_i(pn + k) = \operatorname{ct}[P_i(\boldsymbol{x})^{pn} \; Q_i(\boldsymbol{x}) P_i(\boldsymbol{x})^k]$$

Constant terms and p-schemes





- Rowland and Zeilberger '14 construct congruence automata for **constant terms** $A(n) = \mathrm{ct}[P(\boldsymbol{x})^n Q(\boldsymbol{x})]$.

EG

$$C(n) = \mathrm{ct}[(x^{-1} + 2 + x)^n (1 - x)]$$ Catalan numbers

$$\sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k} = \mathrm{ct}\left[\frac{(x+1)(x+y)(x+y+1)}{xy}\right]^n$$ Apéry numbers

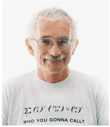
- Start with the state $A_0(n) = \mathrm{ct}[P(\boldsymbol{x})^n Q(\boldsymbol{x})]$.
- For each state $A_i(n) = \mathrm{ct}[P_i(\boldsymbol{x})^n Q_i(\boldsymbol{x})]$ and each $k \in \{0, 1, \ldots, p-1\}$,

All states mod p^r.

$$A_i(pn + k) = \mathrm{ct}[P_i(\boldsymbol{x})^{pn} \; Q_i(\boldsymbol{x}) P_i(\boldsymbol{x})^k]$$
$$\equiv \mathrm{ct}[P_j(\boldsymbol{x})^n \; Q_j(\boldsymbol{x})]$$

where the RHS is either a previous state or a new one.

Repeat until done!



- Rowland and Zeilberger '14 construct congruence automata for **constant terms** $A(n) = \text{ct}[P(\boldsymbol{x})^n Q(\boldsymbol{x})]$.

EG

$$C(n) = \text{ct}[(x^{-1} + 2 + x)^n (1 - x)]$$ Catalan numbers

$$\sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k} = \text{ct}\left[\frac{(x+1)(x+y)(x+y+1)}{xy}\right]^n$$ Apéry numbers

- Start with the state $A_0(n) = \text{ct}[P(\boldsymbol{x})^n Q(\boldsymbol{x})]$.

All states mod p^r.

- For each state $A_i(n) = \text{ct}[P_i(\boldsymbol{x})^n Q_i(\boldsymbol{x})]$ and each $k \in \{0, 1, \ldots, p-1\}$,

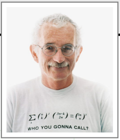
$$\begin{aligned} A_i(pn+k) &= \text{ct}[P_i(\boldsymbol{x})^{pn} Q_i(\boldsymbol{x}) P_i(\boldsymbol{x})^k] \\ &\equiv \text{ct}[P_j(\boldsymbol{x})^n Q_j(\boldsymbol{x})] \end{aligned}$$

where the RHS is either a previous state or a new one.

Repeat until done!

LEM $P(\boldsymbol{x})^{p^r} \equiv P(\boldsymbol{x}^p)^{p^{r-1}} \pmod{p^r}$ for any $P \in \mathbb{Z}[\boldsymbol{x}^{\pm 1}]$.

Constant terms and p-schemes



- Rowland and Zeilberger '14 construct congruence automata for **constant terms** $A(n) = \operatorname{ct}[P(\boldsymbol{x})^n Q(\boldsymbol{x})]$.

EG

$$C(n) = \operatorname{ct}[(x^{-1} + 2 + x)^n (1 - x)]$$ Catalan numbers

$$\sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k} = \operatorname{ct}\left[\frac{(x+1)(x+y)(x+y+1)}{xy}\right]^n$$ Apéry numbers

- Start with the state $A_0(n) = \operatorname{ct}[P(\boldsymbol{x})^n Q(\boldsymbol{x})]$.

All states mod p^r.

- For each state $A_i(n) = \operatorname{ct}[P_i(\boldsymbol{x})^n Q_i(\boldsymbol{x})]$ and each $k \in \{0, 1, \ldots, p-1\}$,

$$A_i(pn + k) = \operatorname{ct}[P_i(\boldsymbol{x})^{pn} \; Q_i(\boldsymbol{x}) P_i(\boldsymbol{x})^k]$$
$$\equiv \operatorname{ct}[P_j(\boldsymbol{x})^n \; Q_j(\boldsymbol{x})]$$

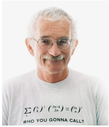
where the RHS is either a previous state or a new one.

Repeat until done!

LEM $P(\boldsymbol{x})^{p^r} \equiv P(\boldsymbol{x}^p)^{p^{r-1}} \pmod{p^r}$ for any $P \in \mathbb{Z}[\boldsymbol{x}^{\pm 1}]$.

- Simplifying using this lemma, the P_i are $P(\boldsymbol{x})^{p^s}$ with $0 \leqslant s < r$.

Constant terms and p-schemes



- Rowland and Zeilberger '14 construct congruence automata for **constant terms** $A(n) = \mathrm{ct}[P(\boldsymbol{x})^n Q(\boldsymbol{x})]$.

EG

$C(n) = \mathrm{ct}[(x^{-1} + 2 + x)^n (1 - x)]$ — Catalan numbers

$$\sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k} = \mathrm{ct}\left[\frac{(x+1)(x+y)(x+y+1)}{xy}\right]^n$$

Apéry numbers

- Start with the state $A_0(n) = \mathrm{ct}[P(\boldsymbol{x})^n Q(\boldsymbol{x})]$.

All states mod p^r.

- For each state $A_i(n) = \mathrm{ct}[P_i(\boldsymbol{x})^n Q_i(\boldsymbol{x})]$ and each $k \in \{0, 1, \ldots, p-1\}$,

$$\begin{aligned} A_i(pn+k) &= \mathrm{ct}[P_i(\boldsymbol{x})^{pn} \; Q_i(\boldsymbol{x}) P_i(\boldsymbol{x})^k] \\ &\equiv \mathrm{ct}[P_j(\boldsymbol{x})^n \; Q_j(\boldsymbol{x})] \end{aligned}$$

where the RHS is either a previous state or a new one.

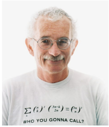
Repeat until done!

LEM $P(\boldsymbol{x})^{p^r} \equiv P(\boldsymbol{x}^p)^{p^{r-1}} \pmod{p^r}$ for any $P \in \mathbb{Z}[\boldsymbol{x}^{\pm 1}]$.

- Simplifying using this lemma, the P_i are $P(\boldsymbol{x})^{p^s}$ with $0 \leqslant s < r$.
- The degree of the Q_i can be bounded.

Hence, this process terminates.

Constant terms and p-schemes



- Rowland and Zeilberger '14 construct congruence automata for **constant terms** $A(n) = \mathrm{ct}[P(\boldsymbol{x})^n Q(\boldsymbol{x})]$.

EG

$C(n) = \mathrm{ct}[(x^{-1} + 2 + x)^n (1 - x)]$ — Catalan numbers

$$\sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k} = \mathrm{ct}\left[\frac{(x+1)(x+y)(x+y+1)}{xy}\right]^n$$ — Apéry numbers

- Start with the state $A_0(n) = \mathrm{ct}[P(\boldsymbol{x})^n Q(\boldsymbol{x})]$.
- For each state $A_i(n) = \mathrm{ct}[P_i(\boldsymbol{x})^n Q_i(\boldsymbol{x})]$ and each $k \in \{0, 1, \ldots, p-1\}$,

All states mod p^r.

$$A_i(pn + k) = \mathrm{ct}[P_i(\boldsymbol{x})^{pn} \; Q_i(\boldsymbol{x}) P_i(\boldsymbol{x})^k]$$
$$\equiv \mathrm{ct}[P_j(\boldsymbol{x})^n \; Q_j(\boldsymbol{x})]$$

linear p-scheme: $\equiv \sum_j \alpha_j \, \mathrm{ct}[P_j(\boldsymbol{x})^n Q_j(\boldsymbol{x})]$

where the RHS is either a previous state or a new one.

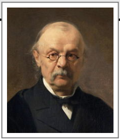
Repeat until done!

LEM $P(\boldsymbol{x})^{p^r} \equiv P(\boldsymbol{x}^p)^{p^{r-1}} \pmod{p^r}$ for any $P \in \mathbb{Z}[\boldsymbol{x}^{\pm 1}]$.

- Simplifying using this lemma, the P_i are $P(\boldsymbol{x})^{p^s}$ with $0 \leqslant s < r$.
- The degree of the Q_i can be bounded.

Hence, this process terminates.

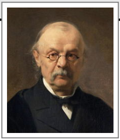
Linear vs. automatic schemes



- The Catalan numbers $C(n)$ have the constant term expression:

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

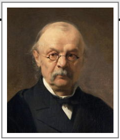
Linear vs. automatic schemes



- The Catalan numbers $C(n)$ have the constant term expression:

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

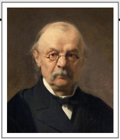
Linear vs. automatic schemes



- The Catalan numbers $C(n)$ have the constant term expression:

$$C(n) = \frac{1}{n+1}\binom{2n}{n} = \binom{2n}{n} - \binom{2n}{n-1} = \operatorname{ct}\left[\frac{(1+x)^{2n}}{x^n}(1-x)\right]$$

Linear vs. automatic schemes

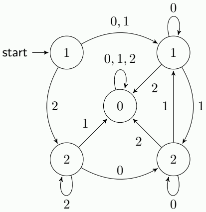


- The Catalan numbers $C(n)$ have the constant term expression:

$$C(n) = \frac{1}{n+1}\binom{2n}{n} = \binom{2n}{n} - \binom{2n}{n-1} = \operatorname{ct}\left[\frac{(1+x)^{2n}}{x^n}(1-x)\right]$$

EG
mod 3

automatic 3-scheme



$$\begin{aligned} A_0(3n) &= A_1(n) & A_2(3n) &= A_3(n)\\ A_0(3n+1) &= A_1(n) & A_2(3n+1) &= 0\\ A_0(3n+2) &= A_2(n) & A_2(3n+2) &= A_2(n)\\ A_1(3n) &= A_1(n) & A_3(3n) &= A_3(n)\\ A_1(3n+1) &= A_3(n) & A_3(3n+1) &= A_1(n)\\ A_1(3n+2) &= 0 & A_3(3n+2) &= 0 \end{aligned}$$

Initial conditions:
$A_0(0) = A_1(0) = 1, \quad A_2(0) = A_3(0) = 2$

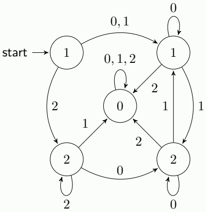
Linear vs. automatic schemes

- The Catalan numbers $C(n)$ have the constant term expression:

$$C(n) = \frac{1}{n+1}\binom{2n}{n} = \binom{2n}{n} - \binom{2n}{n-1} = \operatorname{ct}\left[\frac{(1+x)^{2n}}{x^n}(1-x)\right]$$

EG mod 3

automatic 3-scheme



$$\begin{aligned} A_0(3n) &= A_1(n) & A_2(3n) &= A_3(n) \\ A_0(3n+1) &= A_1(n) & A_2(3n+1) &= 0 \\ A_0(3n+2) &= A_2(n) & A_2(3n+2) &= A_2(n) \\ A_1(3n) &= A_1(n) & A_3(3n) &= A_3(n) \\ A_1(3n+1) &= A_3(n) & A_3(3n+1) &= A_1(n) \\ A_1(3n+2) &= 0 & A_3(3n+2) &= 0 \end{aligned}$$

Initial conditions:
$A_0(0) = A_1(0) = 1, \quad A_2(0) = A_3(0) = 2$

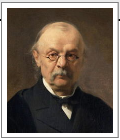
EG mod 3

linear 3-scheme

$$\begin{aligned} A_0(3n) &= A_1(n) & A_1(3n) &= A_1(n) \\ A_0(3n+1) &= A_1(n) & A_1(3n+1) &= 2A_1(n) \\ A_0(3n+2) &= A_0(n) + A_1(n) & A_1(3n+2) &= 0 \end{aligned}$$

Initial conditions: $A_0(0) = A_1(0) = 1$

Linear vs. automatic schemes

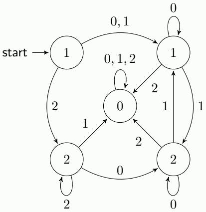


- The Catalan numbers $C(n)$ have the constant term expression:

$$C(n) = \frac{1}{n+1}\binom{2n}{n} = \binom{2n}{n} - \binom{2n}{n-1} = \operatorname{ct}\left[\frac{(1+x)^{2n}}{x^n}(1-x)\right]$$

EG
mod 3

automatic 3-scheme



$$\begin{aligned} A_0(3n) &= A_1(n) & A_2(3n) &= A_3(n)\\ A_0(3n+1) &= A_1(n) & A_2(3n+1) &= 0\\ A_0(3n+2) &= A_2(n) & A_2(3n+2) &= A_2(n)\\ A_1(3n) &= A_1(n) & A_3(3n) &= A_3(n)\\ A_1(3n+1) &= A_3(n) & A_3(3n+1) &= A_1(n)\\ A_1(3n+2) &= 0 & A_3(3n+2) &= 0 \end{aligned}$$

Initial conditions:
$A_0(0) = A_1(0) = 1, \quad A_2(0) = A_3(0) = 2$

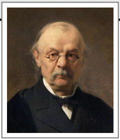
EG
mod 3

linear 3-scheme

$$\begin{aligned} A_0(3n) &= A_1(n) & A_1(3n) &= A_1(n)\\ A_0(3n+1) &= A_1(n) & A_1(3n+1) &= 2A_1(n)\\ A_0(3n+2) &= A_0(n) + A_1(n) & A_1(3n+2) &= 0 \end{aligned}$$

Initial conditions: $A_0(0) = A_1(0) = 1$

Linear vs. automatic schemes

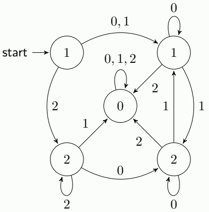


- The Catalan numbers $C(n)$ have the constant term expression:

$$C(n) = \frac{1}{n+1}\binom{2n}{n} = \binom{2n}{n} - \binom{2n}{n-1} = \operatorname{ct}\left[\frac{(1+x)^{2n}}{x^n}(1-x)\right]$$

EG mod 3

automatic 3-scheme



$$\begin{aligned} A_0(3n) &= A_1(n) & A_2(3n) &= A_3(n) \\ A_0(3n+1) &= A_1(n) & A_2(3n+1) &= 0 \\ A_0(3n+2) &= A_2(n) & A_2(3n+2) &= A_2(n) \\ A_1(3n) &= A_1(n) & A_3(3n) &= A_3(n) \\ A_1(3n+1) &= A_3(n) & A_3(3n+1) &= A_1(n) \\ A_1(3n+2) &= 0 & A_3(3n+2) &= 0 \end{aligned}$$

Initial conditions:
$A_0(0) = A_1(0) = 1, \quad A_2(0) = A_3(0) = 2$

EG mod 3

linear 3-scheme

$$\begin{aligned} A_0(3n) &= A_1(n) & A_1(3n) &= A_1(n) \\ A_0(3n+1) &= A_1(n) & A_1(3n+1) &= 2A_1(n) \\ A_0(3n+2) &= A_0(n) + A_1(n) & A_1(3n+2) &= 0 \end{aligned}$$

Initial conditions: $A_0(0) = A_1(0) = 1$

EG
mod 3

linear 3-scheme

$$
\begin{aligned}
A_0(3n) &= A_1(n) & A_1(3n) &= A_1(n)\\
A_0(3n+1) &= A_1(n) & A_1(3n+1) &= 2A_1(n)\\
A_0(3n+2) &= A_0(n)+A_1(n) & A_1(3n+2) &= 0
\end{aligned}
$$

Initial conditions: $A_0(0) = A_1(0) = 1$

Scaling schemes

EG mod 3

linear 3-scheme

$$\begin{aligned} A_0(3n) &= A_1(n) & A_1(3n) &= A_1(n) \\ A_0(3n+1) &= A_1(n) & A_1(3n+1) &= 2A_1(n) \\ A_0(3n+2) &= A_0(n) + A_1(n) & A_1(3n+2) &= 0 \end{aligned}$$

Initial conditions: $A_0(0) = A_1(0) = 1$

EG mod 3

scaling 3-scheme

$$\begin{aligned} A_0(3n) &= A_1(n) & A_1(3n) &= A_1(n) & A_2(3n) &= A_1(n) \\ A_0(3n+1) &= A_1(n) & A_1(3n+1) &= 2A_1(n) & A_2(3n+1) &= 0 \\ A_0(3n+2) &= 2A_2(n) & A_1(3n+2) &= 0 & A_2(3n+2) &= A_2(n) \end{aligned}$$

Initial conditions: $A_0(0) = A_1(0) = A_2(0) = 1$

- 3-schemes for Catalan numbers modulo 3:
  - automatic: 4 states (most informative)
  - scaling: 3 states
  - linear: 2 states (least informative)

Scaling schemes

EG
mod 3

linear 3-scheme

$$\begin{aligned} A_0(3n) &= A_1(n) & A_1(3n) &= A_1(n) \\ A_0(3n+1) &= A_1(n) & A_1(3n+1) &= 2A_1(n) \\ A_0(3n+2) &= A_0(n) + A_1(n) & A_1(3n+2) &= 0 \end{aligned}$$

Initial conditions: $A_0(0) = A_1(0) = 1$

EG
mod 3

scaling 3-scheme

$$\begin{aligned} A_0(3n) &= A_1(n) & A_1(3n) &= A_1(n) & A_2(3n) &= A_1(n) \\ A_0(3n+1) &= A_1(n) & A_1(3n+1) &= 2A_1(n) & A_2(3n+1) &= 0 \\ A_0(3n+2) &= 2A_2(n) & A_1(3n+2) &= 0 & A_2(3n+2) &= A_2(n) \end{aligned}$$

Initial conditions: $A_0(0) = A_1(0) = A_2(0) = 1$

- 3-schemes for Catalan numbers modulo 3:
  - automatic: 4 states (most informative)
  - scaling: 3 states
  - linear: 2 states (least informative)
- p-**adic valuations:** Modulo p^r, scaling p-schemes for $A(n)$ can be simplified into automatic schemes for $p^{\nu_p(A(n))}$ by "*forgetting the constants*".

A conjecture on Motzkin numbers modulo p^2

Q Rowland, Yassawi '15

For the Motzkin numbers, are there infinitely many primes p such that $M(n) \not\equiv 0 \pmod{p^2}$ for all $n \geqslant 0$?

- Rowland–Yassawi proved that 5 and 13 are such primes.
- They further conjectured that $31, 37, 61$ are such primes as well.

A conjecture on Motzkin numbers modulo p^2

Q Rowland, Yassawi '15 — For the Motzkin numbers, are there infinitely many primes p such that $M(n) \not\equiv 0 \pmod{p^2}$ for all $n \geqslant 0$?

- Rowland–Yassawi proved that 5 and 13 are such primes.
- They further conjectured that $31, 37, 61$ are such primes as well.

THM S 2022 — Let $p \in \{5, 13, 31, 37, 61, 79, 97, 103\}$. For all $n \in \mathbb{Z}_{\geqslant 0}$, $M(n) \not\equiv 0 \pmod{p^2}$.

- Proof by computing a scaling p-scheme modulo p^2 using

$$M(n) = \operatorname{ct}[(x^{-1} + 1 + x)^n (1 - x^2)].$$

A conjecture on Motzkin numbers modulo p^2

Q Rowland, Yassawi '15 — For the Motzkin numbers, are there infinitely many primes p such that $M(n) \not\equiv 0 \pmod{p^2}$ for all $n \geqslant 0$?

- Rowland–Yassawi proved that 5 and 13 are such primes.
- They further conjectured that $31, 37, 61$ are such primes as well.

THM S 2022 — Let $p \in \{5, 13, 31, 37, 61, 79, 97, 103\}$.
For all $n \in \mathbb{Z}_{\geqslant 0}$, $M(n) \not\equiv 0 \pmod{p^2}$.

- Proof by computing a scaling p-scheme modulo p^2 using

$$M(n) = \operatorname{ct}[(x^{-1} + 1 + x)^n (1 - x^2)].$$

- These scaling p-schemes have much fewer states than automatic ones:
  - $p = 31$: 125 rather than $28{,}081$ states
  - $p = 37$: 149 rather than $44{,}173$ states

The case $p = 13$ as an example

- SageMath implementation:
  `https://github.com/arminstraub/congruenceschemes`

EG R-Y '15 $M(n) \not\equiv 0 \pmod{13^2}$ for all $n \geqslant 0$

The case $p = 13$ as an example

- SageMath implementation:
  `https://github.com/arminstraub/congruenceschemes`

EG R-Y '15 $M(n) \not\equiv 0 \pmod{13^2}$ for all $n \geqslant 0$

```
>>> R.<x> = LaurentPolynomialRing(Zmod(13^2))
>>> S = CongruenceSchemeAutomatic(1/x+1+x, 1-x^2); S
  Linear 13-scheme with 2097 states over Ring of integers modulo 169
>>> S.impossible_values()
  {0}
```

- Takes about 10sec (vs 40min mentioned in RY paper; 30sec using Rowland's excellent Mathematica package *IntegerSequences*).

The case $p = 13$ as an example

- SageMath implementation:
  `https://github.com/arminstraub/congruenceschemes`

EG R-Y '15 $M(n) \not\equiv 0 \pmod{13^2}$ for all $n \geqslant 0$

```
>>> R.<x> = LaurentPolynomialRing(Zmod(13^2))
>>> S = CongruenceSchemeAutomatic(1/x+1+x, 1-x^2); S
  Linear 13-scheme with 2097 states over Ring of integers modulo 169
>>> S.impossible_values()
  {0}
```

- Takes about 10sec (vs 40min mentioned in RY paper; 30sec using Rowland's excellent Mathematica package *IntegerSequences*).
- The following cuts this down to half a second:

```
>>> S = CongruenceSchemeScaling(1/x+1+x, 1-x^2); S
  Linear 13-scheme with 48 states over Ring of integers modulo 169
>>> V = S.valuation_scheme(); V
  Linear 13-scheme with 5 states over Ring of integers modulo 169
>>> V.possible_values()
  {1, 13}
```

Lucas congruences

THM Lucas 1878

$$\binom{n}{k} \equiv \binom{n_0}{k_0}\binom{n_1}{k_1}\binom{n_2}{k_2}\cdots \pmod{p},$$

where n_i and k_i are the p-adic digits of n and k.

EG

$$\binom{136}{79} \equiv \binom{3}{2}\binom{5}{4}\binom{2}{1} = 3 \cdot 5 \cdot 2 \equiv 2 \pmod{7}$$

LHS $= 1009220746942993946271525627285911932800$

Lucas congruences

THM Lucas 1878

$$\binom{n}{k} \equiv \binom{n_0}{k_0}\binom{n_1}{k_1}\binom{n_2}{k_2}\cdots \pmod{p},$$

where n_i and k_i are the p-adic digits of n and k.

EG

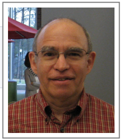
$$\binom{136}{79} \equiv \binom{3}{2}\binom{5}{4}\binom{2}{1} = 3 \cdot 5 \cdot 2 \equiv 2 \pmod{7}$$

LHS $= 1009220746942993946271525627285911932800$

- Interesting sequences like the **Apéry numbers** $1, 5, 73, 1445, \ldots$

$$A(n) = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2$$

satisfy such **Lucas congruences** as well:



THM Gessel '82

$$A(n) \equiv A(n_0)A(n_1)\cdots A(n_r) \pmod{p}$$

Application: Primes not dividing Apéry numbers

CONJ Rowland–Yassawi '15

There are infinitely many primes p such that p does not divide any Apéry number $A(n)$.

Such as $p = 2, 3, 7, 13, 23, 29, 43, 47, \ldots$

Application: Primes not dividing Apéry numbers

CONJ Rowland–Yassawi '15

There are infinitely many primes p such that p does not divide any Apéry number $A(n)$.

Such as $p = 2, 3, 7, 13, 23, 29, 43, 47, \ldots$

EG $p = 7$

- The values of Apéry numbers $A(0), A(1), \ldots, A(6)$ modulo 7 are $1, 5, 3, 3, 3, 5, 1$.

Application: Primes not dividing Apéry numbers

CONJ Rowland–Yassawi '15 There are infinitely many primes p such that p does not divide any Apéry number $A(n)$.

Such as $p = 2, 3, 7, 13, 23, 29, 43, 47, \ldots$

EG $p = 7$

- The values of Apéry numbers $A(0), A(1), \ldots, A(6)$ modulo 7 are $1, 5, 3, 3, 3, 5, 1$.
- Hence, the Lucas congruences imply that 7 does not divide any Apéry number.

Application: Primes not dividing Apéry numbers

CONJ Rowland–Yassawi '15

There are infinitely many primes p such that p does not divide any Apéry number $A(n)$.

Such as $p = 2, 3, 7, 13, 23, 29, 43, 47, \ldots$

EG $p = 7$

- The values of Apéry numbers $A(0), A(1), \ldots, A(6)$ modulo 7 are $1, 5, 3, 3, 3, 5, 1$.
- Hence, the Lucas congruences imply that 7 does not divide any Apéry number.

CONJ Malik–S '16

The proportion of primes not dividing any Apéry number $A(n)$ is $e^{-1/2} \approx 60.65\%$.

Application: Primes not dividing Apéry numbers

CONJ Rowland–Yassawi '15

There are infinitely many primes p such that p does not divide any Apéry number $A(n)$.

Such as $p = 2, 3, 7, 13, 23, 29, 43, 47, \ldots$

EG $p = 7$

- The values of Apéry numbers $A(0), A(1), \ldots, A(6)$ modulo 7 are $1, 5, 3, 3, 3, 5, 1$.
- Hence, the Lucas congruences imply that 7 does not divide any Apéry number.

CONJ Malik–S '16

The proportion of primes not dividing any Apéry number $A(n)$ is $e^{-1/2} \approx 60.65\%$.

- Heuristically, combine Lucas congruences,
- palindromic behavior of Apéry numbers, that is

$$A(n) \equiv A(p-1-n) \pmod{p},$$

- and $e^{-1/2} = \lim_{p \to \infty} \left(1 - \frac{1}{p}\right)^{(p+1)/2}$.

Lucas congruences correspond to the simplest schemes

Lucas congruences: $A(n) \equiv A(n_0)A(n_1)\cdots A(n_r) \pmod{p}$

n_i are the p-adic digits of n

PROP Henningsen S '21

Suppose $A(0) = 1$.

$A(n)$ satisfies Lucas congruences modulo p.
$\iff A(n) \pmod{p}$ can be encoded by a single-state linear p-scheme.

Lucas congruences correspond to the simplest schemes

Lucas congruences: $A(n) \equiv A(n_0) A(n_1) \cdots A(n_r) \pmod{p}$

n_i are the p-adic digits of n

PROP Henningsen S '21

Suppose $A(0) = 1$.

$A(n)$ satisfies Lucas congruences modulo p.
$\iff A(n) \pmod{p}$ can be encoded by a single-state linear p-scheme.

proof p-scheme with single state $A_0(n) \equiv A(n) \pmod{p}$:

$$A_0(pn+k) \equiv \alpha_k A_0(n) \pmod{p} \qquad \text{for all } 0 \leqslant k < p, \ n \geqslant 0$$

□

Lucas congruences correspond to the simplest schemes

Lucas congruences: $A(n) \equiv A(n_0)A(n_1)\cdots A(n_r) \pmod{p}$

n_i are the p-adic digits of n

PROP Henningsen S '21

Suppose $A(0) = 1$.

$A(n)$ satisfies Lucas congruences modulo p.
$\iff A(n) \pmod{p}$ can be encoded by a single-state linear p-scheme.

proof p-scheme with single state $A_0(n) \equiv A(n) \pmod{p}$:

$$A_0(pn + k) \equiv \alpha_k A_0(n) \pmod{p} \qquad \text{for all } 0 \leqslant k < p, \ n \geqslant 0$$

$\boxed{n = 0 :}$ $A_0(k) \equiv \alpha_k$

□

Lucas congruences correspond to the simplest schemes

Lucas congruences: $A(n) \equiv A(n_0)A(n_1)\cdots A(n_r) \pmod{p}$

n_i are the p-adic digits of n

PROP Henningsen S '21

Suppose $A(0) = 1$.

$A(n)$ satisfies Lucas congruences modulo p.
$\iff A(n) \pmod{p}$ can be encoded by a single-state linear p-scheme.

proof p-scheme with single state $A_0(n) \equiv A(n) \pmod{p}$:

$$A_0(pn+k) \equiv \alpha_k A_0(n) \pmod{p} \qquad \text{for all } 0 \leqslant k < p, \ n \geqslant 0$$

$n = 0:$ $\quad A_0(k) \equiv \alpha_k$

$$A_0(pn+k) \equiv A_0(k)A_0(n) \pmod{p}$$

□

Lucas congruences correspond to the simplest schemes

Lucas congruences: $A(n) \equiv A(n_0)A(n_1)\cdots A(n_r) \pmod p$

n_i are the p-adic digits of n

PROP (Henningsen S '21) Suppose $A(0) = 1$.

$A(n)$ satisfies Lucas congruences modulo p.
$\iff A(n) \pmod p$ can be encoded by a single-state linear p-scheme.

proof p-scheme with single state $A_0(n) \equiv A(n) \pmod p$:

$$A_0(pn+k) \equiv \alpha_k A_0(n) \pmod p \qquad \text{for all } 0 \leqslant k < p, \ n \geqslant 0$$

$\boxed{n = 0:}$ $A_0(k) \equiv \alpha_k$

$$A_0(pn+k) \equiv A_0(k)A_0(n) \pmod p$$

□

- This suggests generalizations such as:

  $A(n)$ satisfies **Lucas congruences of order k** modulo p.
  $\iff A(n) \pmod p$ can be encoded by a linear p-scheme with k states.

Generalized Lucas congruences

THM Henningsen S '21

Let $A(n) = \operatorname{ct}[P(x,y)^n Q(x,y)]$ where $P, Q \in \mathbb{Z}[x^{\pm 1}, y^{\pm 1}]$ with

$$P(x,y) = \sum_{(i,j)\in\{-1,0,1\}^2} a_{i,j} x^i y^j, \quad Q(x,y) = \alpha + \beta x + \gamma y + \delta xy.$$

THM Henningsen S '21

Let $A(n) = \operatorname{ct}[P(x,y)^n Q(x,y)]$ where $P, Q \in \mathbb{Z}[x^{\pm 1}, y^{\pm 1}]$ with

$$P(x,y) = \sum_{(i,j)\in\{-1,0,1\}^2} a_{i,j} x^i y^j, \quad Q(x,y) = \alpha + \beta x + \gamma y + \delta xy.$$

Then, for any $n \in \mathbb{Z}_{\geqslant 0}$ and $k \in \{0, 1, \ldots, p-1\}$,

$$A(pn+k) \equiv B(n) A(k) + \begin{cases} 0, & \text{if } k < p-1, \\ \tilde{A}(n), & \text{if } k = p-1, \end{cases} \pmod{p}.$$

Here, $B(n) = \operatorname{ct}[P(x,y)^n]$ and $\tilde{A}(n) = \operatorname{ct}[P(x,y)^n \tilde{Q}(x,y)]$ with:

THM Henningsen S '21

Let $A(n) = \operatorname{ct}[P(x,y)^n Q(x,y)]$ where $P, Q \in \mathbb{Z}[x^{\pm 1}, y^{\pm 1}]$ with

$$P(x,y) = \sum_{(i,j)\in\{-1,0,1\}^2} a_{i,j} x^i y^j, \quad Q(x,y) = \alpha + \beta x + \gamma y + \delta xy.$$

Then, for any $n \in \mathbb{Z}_{\geqslant 0}$ and $k \in \{0, 1, \ldots, p-1\}$,

$$A(pn+k) \equiv B(n) A(k) + \begin{cases} 0, & \text{if } k < p-1, \\ \tilde{A}(n), & \text{if } k = p-1, \end{cases} \pmod{p}.$$

Here, $B(n) = \operatorname{ct}[P(x,y)^n]$ and $\tilde{A}(n) = \operatorname{ct}[P(x,y)^n \tilde{Q}(x,y)]$ with:

- $\tilde{Q}(x,y) = Q(\sigma_x x, \sigma_y y) - \alpha + \delta \left(\frac{a_{1,0}}{2a_{1,1}}(1-\sigma_x)x + \frac{a_{0,1}}{2a_{1,1}}(1-\sigma_y)y + (1-\sigma_x\sigma_y)xy \right)$
- $\sigma_x = \left(\frac{a_{1,0}^2 - 4a_{1,-1}a_{1,1}}{p} \right) \in \{0, \pm 1\}$ $\quad p \neq 2, p \nmid a_{1,1}$
- $\sigma_y = \left(\frac{a_{0,1}^2 - 4a_{-1,1}a_{1,1}}{p} \right) \in \{0, \pm 1\}$

Generalized Lucas congruences

THM Henningsen S '21

Let $A(n) = \operatorname{ct}[P(x,y)^n Q(x,y)]$ where $P, Q \in \mathbb{Z}[x^{\pm 1}, y^{\pm 1}]$ with

$$P(x,y) = \sum_{(i,j)\in\{-1,0,1\}^2} a_{i,j} x^i y^j, \quad Q(x,y) = \alpha + \beta x + \gamma y + \delta xy.$$

Then, for any $n \in \mathbb{Z}_{\geqslant 0}$ and $k \in \{0, 1, \ldots, p-1\}$,

$$A(pn+k) \equiv B(n) A(k) + \begin{cases} 0, & \text{if } k < p-1, \\ \tilde{A}(n), & \text{if } k = p-1, \end{cases} \pmod{p}.$$

Here, $B(n) = \operatorname{ct}[P(x,y)^n]$ and $\tilde{A}(n) = \operatorname{ct}[P(x,y)^n \tilde{Q}(x,y)]$ with:

- $\tilde{Q}(x,y) = Q(\sigma_x x, \sigma_y y) - \alpha + \delta \left(\frac{a_{1,0}}{2a_{1,1}}(1-\sigma_x)x + \frac{a_{0,1}}{2a_{1,1}}(1-\sigma_y)y + (1-\sigma_x\sigma_y)xy \right)$
- $\sigma_x = \left(\frac{a_{1,0}^2 - 4a_{1,-1}a_{1,1}}{p} \right) \in \{0, \pm 1\}$ $\qquad p \neq 2, p \nmid a_{1,1}$
- $\sigma_y = \left(\frac{a_{0,1}^2 - 4a_{-1,1}a_{1,1}}{p} \right) \in \{0, \pm 1\}$

If $Q = 1$, these reduce to the usual Lucas congruences.

Application: Catalan numbers

COR Henningsen S '21

If $\underbrace{p-1,\ldots,p-1}_{s}, n_0, n_1, \ldots, n_r$ is the p-adic expansion of n, then

$$C(n) \equiv \delta(n_0, s) C(n_0) \binom{2n_1}{n_1} \cdots \binom{2n_r}{n_r} \pmod{p}$$

where $\delta(n_0, s) = \begin{cases} 1, & \text{if } s = 0, \\ -(2n_0+1), & \text{if } s \geqslant 1. \end{cases}$

Application: Catalan numbers

COR Henningsen S '21

If $\underbrace{p-1,\ldots,p-1}_{s}, n_0, n_1, \ldots, n_r$ is the p-adic expansion of n, then

$$C(n) \equiv \delta(n_0, s) C(n_0) \binom{2n_1}{n_1} \cdots \binom{2n_r}{n_r} \pmod{p}$$

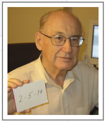
where $\delta(n_0, s) = \begin{cases} 1, & \text{if } s = 0, \\ -(2n_0+1), & \text{if } s \geqslant 1. \end{cases}$

EG Deutsch, Sagan '06

$$C(n) \equiv \begin{cases} (-1)^{\tau(n+1)}, & \text{if } n+1 \in T, \\ 0, & \text{otherwise,} \end{cases} \pmod{3},$$

where $m = m_0 + 3m_1 + 3^2 m_2 + \ldots \in T$ iff $m_1, m_2, \ldots \in \{0, 1\}$.

$\tau(m) = (\#$ of $m_1, m_2, \ldots$ equal to $1)$



COR Henningsen S '21

If $\underbrace{p-1,\ldots,p-1}_{s}, n_0, n_1, \ldots, n_r$ is the p-adic expansion of n, then

$$C(n) \equiv \delta(n_0, s) C(n_0) \binom{2n_1}{n_1} \cdots \binom{2n_r}{n_r} \pmod{p}$$

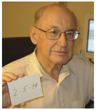
where $\delta(n_0, s) = \begin{cases} 1, & \text{if } s = 0, \\ -(2n_0+1), & \text{if } s \geqslant 1. \end{cases}$

EG Deutsch, Sagan '06

$$C(n) \equiv \begin{cases} (-1)^{\tau(n+1)}, & \text{if } n+1 \in T, \\ 0, & \text{otherwise}, \end{cases} \pmod{3},$$

where $m = m_0 + 3m_1 + 3^2 m_2 + \ldots \in T$ iff $m_1, m_2, \ldots \in \{0, 1\}$.

$\tau(m) = (\#\text{ of } m_1, m_2, \ldots \text{ equal to } 1)$



EG Henningsen S '21

$$C(n) \equiv \begin{cases} 2^{\lambda(n)}, & \text{if } n \notin Z, \\ 0, & \text{otherwise}, \end{cases} \pmod{5},$$

where $n \in Z$ iff $n_0 = 3$, or $(n_0 = 2,\ s \geqslant 1)$, or one of $n_1, n_2, \ldots \in \{3, 4\}$.

$\lambda(n) = (\#\text{ of } n_1, n_2, \ldots \text{ equal to } 1) + \begin{cases} 1, & \text{if } n_0 = 2, \text{ or if both } n_0 = 1 \text{ and } s \geqslant 1, \\ 2, & \text{if } n_0 = 0 \text{ and } s \geqslant 1. \end{cases}$

Catalan numbers: forbidden residues

EG Rowland, Yassawi '15

$C(n) \not\equiv 3 \pmod{4}$ Eu–Liu–Yeh '08

$C(n) \not\equiv 9 \pmod{16}$ Liu–Yeh '10

$C(n) \not\equiv 17, 21, 26 \pmod{32}$

$C(n) \not\equiv 10, 13, 33, 37 \pmod{64}$

Catalan numbers: forbidden residues

EG Rowland, Yassawi '15

$C(n) \not\equiv 3 \pmod 4$ — Eu–Liu–Yeh '08

$C(n) \not\equiv 9 \pmod{16}$ — Liu–Yeh '10

$C(n) \not\equiv 17, 21, 26 \pmod{32}$

$C(n) \not\equiv 10, 13, 33, 37 \pmod{64}$

Q Rowland, Yassawi '15

Let $P(r)$ be the proportion of residues not attained by $C(n)$ mod 2^r. Does $P(r) \to 1$ as $r \to \infty$?

Catalan numbers: forbidden residues

EG Rowland, Yassawi '15

$C(n) \not\equiv 3 \pmod 4$ Eu–Liu–Yeh '08

$C(n) \not\equiv 9 \pmod{16}$ Liu–Yeh '10

$C(n) \not\equiv 17, 21, 26 \pmod{32}$

$C(n) \not\equiv 10, 13, 33, 37 \pmod{64}$

Q Rowland, Yassawi '15

Let $P(r)$ be the proportion of residues not attained by $C(n)$ mod 2^r. Does $P(r) \to 1$ as $r \to \infty$?

r	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$P(r)$	0	.25	.25	.31	.41	.47	.54	.59	.65	.69	.73	.76	.79	.82
$N(r)$	0	1	2	5	13	30	69	152	332	710	1502	3133	6502	13394
$A(r)$	0	1	0	1	3	4	9	14	28	46	82	129	236	390

$N(r) = \#$ residues not attained mod 2^r

$A(r) = \#$ additional residues not attained mod $2^r = N(r) - 2N(r-1)$

Catalan numbers: forbidden residues

EG Rowland, Yassawi '15

$C(n) \not\equiv 3 \pmod 4$ — Eu–Liu–Yeh '08

$C(n) \not\equiv 9 \pmod{16}$ — Liu–Yeh '10

$C(n) \not\equiv 17, 21, 26 \pmod{32}$

$C(n) \not\equiv 10, 13, 33, 37 \pmod{64}$

Q Rowland, Yassawi '15

Let $P(r)$ be the proportion of residues not attained by $C(n)$ mod 2^r. Does $P(r) \to 1$ as $r \to \infty$?

r	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$P(r)$	0	.25	.25	.31	.41	.47	.54	.59	.65	.69	.73	.76	.79	.82
$N(r)$	0	1	2	5	13	30	69	152	332	710	1502	3133	6502	13394
$A(r)$	0	1	0	1	3	4	9	14	28	46	82	129	236	390

$N(r) = \#$ residues not attained mod 2^r

$A(r) = \#$ additional residues not attained mod $2^r = N(r) - 2N(r-1)$

CONJ Bostan '15

$C(n) \not\equiv 3 \pmod{10}$ for all $n \geqslant 0$.

$C(n) \not\equiv 1, 7, 9 \pmod{10}$ for sufficiently large n.

If true, the last digit of any sufficiently large odd Catalan number is always 5. ($n > 255$?)

THANK YOU!

Slides for this talk will be available from my website:
`http://arminstraub.com/talks`

J. Henningsen, A. Straub
Generalized Lucas congruences and linear p-schemes
Advances in Applied Mathematics, Vol. 141, 2022, p. 1-20, #102409

A. Straub
On congruence schemes for constant terms and their applications
Research in Number Theory, Vol. 8, Nr. 3, 2022, p. 1-21, #42