Lucas congruences and congruence schemes

RISC Forum
RISC (Johannes Kepler University, Linz, Austria)

Armin Straub

April 25, 2022

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`

Some goals for today

- **Lucas congruences** are interesting.
- **Diagonals** and **constant terms** are useful ways of representing integer sequences.
- **Congruence automata** are a powerful device for capturing the mod p^r values of sequences.
- **Lucas congruences** correspond to single-state (linear) congruence automata.
- Larger automata can be translated into **generalized Lucas congruences**.

- (**Apéry-like sequences** are fascinating.)

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 $= 1009220746942993946271525627285911932800$

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 $= 1009220746942993946271525627285911932800$

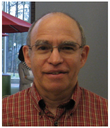
- Interesting sequences like the **Apéry numbers** $1, 5, 73, 1445, \ldots$

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

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

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

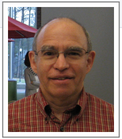
diagonal: $$\sum_{n=0}^{\infty} \binom{2n}{n} t^n = \frac{1}{\sqrt{1-4t}}$$

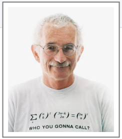
THM Gessel, Zeilberger, Lipshitz 1981–88

The diagonal of a rational function is D-finite.

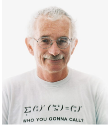
More generally, the diagonal of a D-finite function is D-finite.

$F \in K[[x_1,\ldots,x_d]]$ 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

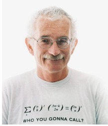


CONJ Kauers-Zeilberger 2008

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

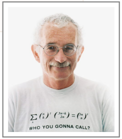
$$\frac{1}{(1-x)(1-y)+(1-x)(1-z)+\ldots+(1-z)(1-w)}.$$

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

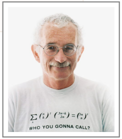
$$D(n)=\sum_{k=0}^{n}\binom{n}{k}^2\binom{2k}{n}^2.$$

- $D(n)$ 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**.

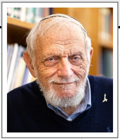
Q S-Zudilin 2015: Can we conclude the conjectured positivity from the positivity of $D(n)$ together with the (easy) positivity of $\frac{1}{1-(x+y+z)+2xyz}$?

Characterizations of diagonals

EG Diagonals of rational functions

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

Characterizations of diagonals

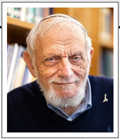


EG Diagonals of rational functions

- $F(x)$ = 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

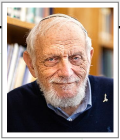
- $F(x)$ = C-finite sequences
- $F(x, y)$ = sequences with algebraic GF (Furstenberg '67)

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





EG Diagonals of rational functions

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

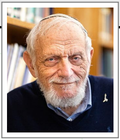
To see the latter, express the diagonal as $\frac{1}{2\pi i}\int_{|x|=\varepsilon} F\left(x, \frac{z}{x}\right)\frac{\mathrm{d}x}{x}$.

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



CONJ Christol '90 Diagonals of rational functions over $\mathbb{Q}$ = globally bounded, D-finite sequences ($\subseteq$ known)

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



EG Diagonals of rational functions

- $F(x) \quad = \quad C$-finite sequences
- $F(x, y) \quad = \quad$ 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 $c, d \in \mathbb{Z}$)

- 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**.

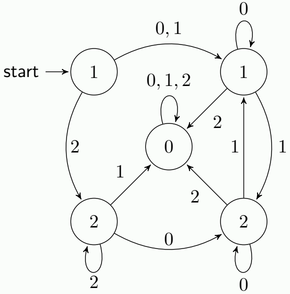
Constructive proof of results by Denef and Lipshitz '87.

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:

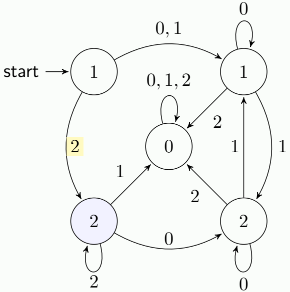
$35 = 1\ 0\ 2\ 2$ in base 3

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:

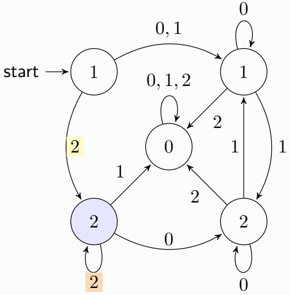
$35 = 1\ 0\ 2\ 2$ in base 3

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

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

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

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

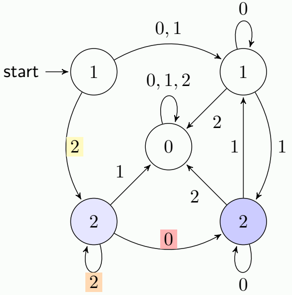
Automatic automata

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

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

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

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

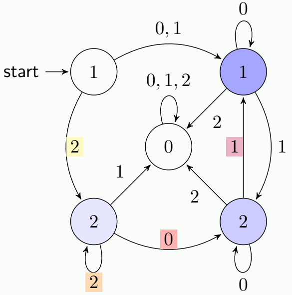
Automatic automata

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

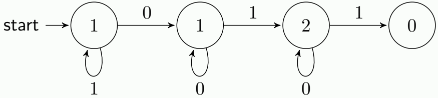
$C(2)$	$C(2) \equiv 2$
$C(8)$	$C(2\,2) \equiv 2$
	$C(0\,2\,2) \equiv 2$
$C(35)$	$C(1\,0\,2\,2) \equiv 1$

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:



Automatic automata

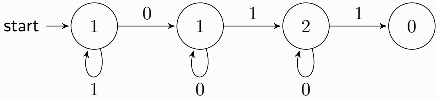
THM Rowland, Yassawi '15

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.

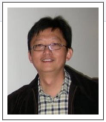
EG Rowland, Yassawi '15

Catalan numbers $C(n)$ modulo 4:



THM Eu, Liu, Yeh '08

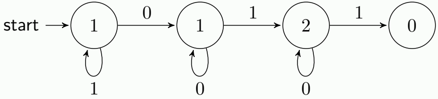
$$C(n) \equiv \begin{cases} 1, & \text{if } n = 2^a - 1 \text{ for some } a \geqslant 0, \\ 2, & \text{if } n = 2^b + 2^a - 1 \text{ for some } b > a \geqslant 0, \\ 0, & \text{otherwise,} \end{cases} \pmod{4}.$$



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.

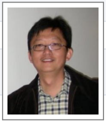
EG Rowland, Yassawi '15: Catalan numbers $C(n)$ modulo 4:



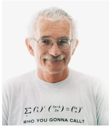
THM Eu, Liu, Yeh '08:

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

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



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

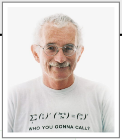
$$C(n) = \mathrm{ct}[(x^{-1} + 2 + x)^n (1 - x)]$$

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

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

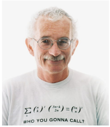
$$C(n) = \mathrm{ct}[(x^{-1} + 2 + x)^n (1 - x)]$$ Catalan numbers

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

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

All states mod p^r.

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

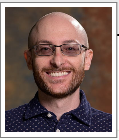
$$\sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k} = \mathrm{ct}\left[\frac{(x+1)(x+y)(x+y+1)}{xy}\right]^n$$ Apéry numbers

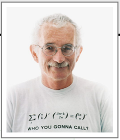
- Start with the state $A_0(n) = \mathrm{ct}[P(\boldsymbol{x})^n Q(\boldsymbol{x})]$.
- For each state $A_i(n) = \mathrm{ct}[P_i(\boldsymbol{x})^n Q_i(\boldsymbol{x})]$ and each $k \in \{0, 1, \ldots, p-1\}$,

All states mod p^r.

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

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

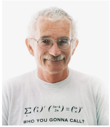
- Start with the state $A_0(n) = \mathrm{ct}[P(\boldsymbol{x})^n Q(\boldsymbol{x})]$.
- For each state $A_i(n) = \mathrm{ct}[P_i(\boldsymbol{x})^n Q_i(\boldsymbol{x})]$ and each $k \in \{0, 1, \ldots, p-1\}$,

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** $A(n) = \mathrm{ct}[P(\boldsymbol{x})^n Q(\boldsymbol{x})]$.

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.

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

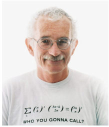
$$\equiv \mathrm{ct}[P_j(\boldsymbol{x})^n \; Q_j(\boldsymbol{x})]$$

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

Repeat until done!

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** $A(n) = \mathrm{ct}[P(\boldsymbol{x})^n Q(\boldsymbol{x})]$.

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 $k \in \{0, 1, \ldots, p-1\}$,

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

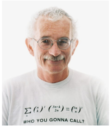
where the RHS is either a previous state or a new one.

Repeat until done!

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.

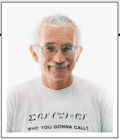
Repeat until done!

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 $A_0(n) = \mathrm{ct}[P(\boldsymbol{x})^n Q(\boldsymbol{x})]$.

All states mod p^r.

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

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

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.

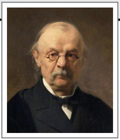
Repeat until done!

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.

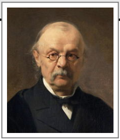
Linear vs. automatic schemes



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

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

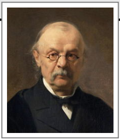
Linear vs. automatic schemes



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

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

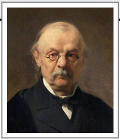
Linear vs. automatic schemes



- 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

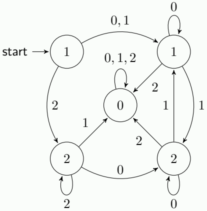


- The Catalan numbers $C(n)$ have the constant term expression:

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

EG
mod 3

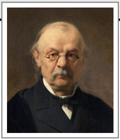
automatic 3-scheme



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

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

Linear vs. automatic schemes

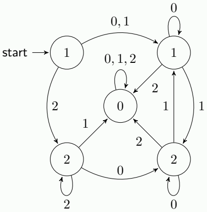


- The Catalan numbers $C(n)$ have the constant term expression:

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

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

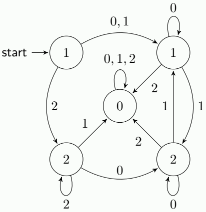
Linear vs. automatic schemes

- 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: $A_0(0) = A_1(0) = 1$

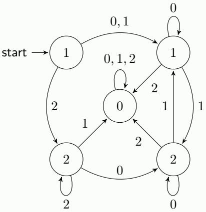
Linear vs. automatic schemes

- 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: $A_0(0) = A_1(0) = 1$

Lucas congruences correspond to the simplest schemes

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

PROP Henningsen S '21

Suppose $A(0) = 1$.

$A(n)$ satisfies Lucas congruences modulo p.
$\Longleftrightarrow A(n) \pmod{p}$ 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

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 $A_0(n) \equiv A(n) \pmod{p}$:

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

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

□

Lucas congruences correspond to the simplest schemes

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

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 $A_0(n) \equiv A(n) \pmod{p}$:

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

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

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

□

- 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.

THM Henningsen S '21

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

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

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:

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:

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

Generalized Lucas congruences

THM Henningsen S '21

Let $A(n) = \mathrm{ct}[P(x,y)^n Q(x,y)]$ 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, $B(n) = \mathrm{ct}[P(x,y)^n]$ and $\tilde{A}(n) = \mathrm{ct}[P(x,y)^n \tilde{Q}(x,y)]$ 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

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

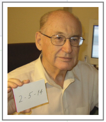
where $\delta(n_0, s) = \begin{cases} 1, & \text{if } s = 0, \\ -(2n_0+1), & \text{if } s \geqslant 1. \end{cases}$

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 $1)$



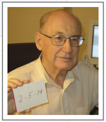
Application: Catalan numbers

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 $1)$

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 $n_1, n_2, \ldots \in \{3,4\}$.
$\lambda(n) = (\#$ of $n_1, n_2, \ldots$ 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 mod 10

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. ($n > 255$?)

Catalan numbers mod 10

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. ($n > 255$?)

- $C(n)$ is odd iff $n = 2^k - 1$ for some k.

Catalan numbers mod 10

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. ($n > 255$?)

- $C(n)$ is odd iff $n = 2^k - 1$ for some k.
- For such n, the generalized Lucas congruences mod 5 simplify to:

(since the first digit n_0 cannot be 4)

$$C(n) \equiv \begin{cases} 2^{\lambda(n)}, & \text{if } n_0, n_1, \ldots \notin \{3, 4\}, \\ 0, & \text{otherwise}, \end{cases} \pmod{5},$$

where $\lambda(n) = (\#$ of $n_0 - 1, n_1, n_2, \ldots$ equal to $1)$.

A victory for the French peasant. . . *

- The **Apéry numbers** $1, 5, 73, 1445, \ldots$

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

satisfy

$$(n+1)^3 u_{n+1} = (2n+1)(17n^2+17n+5)u_n - n^3 u_{n-1}.$$

THM Apéry '78: $\zeta(3) = \sum_{n=1}^{\infty} \frac{1}{n^3}$ is irrational.

* Someone's "sour comment" after Henri Cohen's report on Apéry's proof at the '78 ICM in Helsinki.

A victory for the French peasant...*

- The **Apéry numbers** $1, 5, 73, 1445, \ldots$

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

satisfy

$$(n+1)^3 u_{n+1} = (2n+1)(17n^2+17n+5)u_n - n^3 u_{n-1}.$$

THM (Apéry '78) $\zeta(3) = \sum_{n=1}^{\infty} \frac{1}{n^3}$ is irrational.

proof The same recurrence is satisfied by the "near"-integers

$$B(n) = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2 \left(\sum_{j=1}^{n} \frac{1}{j^3} + \sum_{m=1}^{k} \frac{(-1)^{m-1}}{2m^3 \binom{n}{m}\binom{n+m}{m}} \right).$$

Then, $\frac{B(n)}{A(n)} \to \zeta(3)$. But too fast for $\zeta(3)$ to be rational. □

* Someone's "sour comment" after Henri Cohen's report on Apéry's proof at the '78 ICM in Helsinki.

A victory for the French peasant. . . *

- The **Apéry numbers** $1, 5, 73, 1445, \ldots$

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

satisfy

$$(n+1)^3 u_{n+1} = (2n+1)(17n^2+17n+5)u_n - n^3 u_{n-1}.$$

THM Apéry '78 $\zeta(3) = \sum_{n=1}^{\infty} \frac{1}{n^3}$ is irrational.

> *After a few days of fruitless effort the specific problem was mentioned to Don Zagier (Bonn), and with irritating speed he showed that indeed the sequence satisfies the recurrence.*
>
> **Alfred van der Poorten** — *A proof that Euler missed. . .* **(1979)**

* Someone's "sour comment" after Henri Cohen's report on Apéry's proof at the '78 ICM in Helsinki.

A victory for the French peasant. . . *

- The **Apéry numbers** $1, 5, 73, 1445, \ldots$

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

satisfy

$$(n+1)^3 u_{n+1} = (2n+1)(17n^2 + 17n + 5)u_n - n^3 u_{n-1}.$$

THM Apéry '78: $\zeta(3) = \sum_{n=1}^{\infty} \frac{1}{n^3}$ is irrational.

> *After a few days of fruitless effort the specific problem was mentioned to Don Zagier (Bonn), and with irritating speed he showed that indeed the sequence satisfies the recurrence.*
>
> **Alfred van der Poorten** — *A proof that Euler missed. . .* **(1979)**

Nowadays, there are excellent implementations of this **creative telescoping**, including:

- **HolonomicFunctions** by Koutschan (Mathematica)
- **Sigma** by Schneider (Mathematica)
- **ore_algebra** by Kauers, Jaroschek, Johansson, Mezzarobba (Sage)

(These are just the ones I use on a regular basis. . .

* Someone's "sour comment" after Henri Cohen's report on Apéry's proof at the '78 ICM in Helsinki.

Zagier's search and Apéry-like numbers

- Recurrence for Apéry numbers is the case $(a, b, c) = (17, 5, 1)$ of

$$(n+1)^3 u_{n+1} = (2n+1)(an^2 + an + b)u_n - cn^3 u_{n-1}.$$

Q **Beukers, Zagier** Are there other tuples (a, b, c) for which the solution defined by $u_{-1} = 0$, $u_0 = 1$ is integral?

Zagier's search and Apéry-like numbers

- Recurrence for Apéry numbers is the case $(a, b, c) = (17, 5, 1)$ of

$$(n+1)^3 u_{n+1} = (2n+1)(an^2 + an + b)u_n - cn^3 u_{n-1}.$$

Q (Beukers, Zagier): Are there other tuples (a, b, c) for which the solution defined by $u_{-1} = 0$, $u_0 = 1$ is integral?

- Essentially, only 14 tuples (a, b, c) found. (Almkvist–Zudilin)
  - 4 hypergeometric and 4 Legendrian solutions (with generating functions

$$ {}_3F_2\left(\left.\begin{matrix}\frac{1}{2}, \alpha, 1-\alpha \\ 1, 1\end{matrix}\right| 4C_\alpha z\right), \qquad \frac{1}{1 - C_\alpha z}\, {}_2F_1\left(\left.\begin{matrix}\alpha, 1-\alpha \\ 1\end{matrix}\right| \frac{-C_\alpha z}{1 - C_\alpha z}\right)^2, $$

    with $\alpha = \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{6}$ and $C_\alpha = 2^4, 3^3, 2^6, 2^4 \cdot 3^3$)
  - 6 sporadic solutions

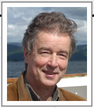
- Similar (and intertwined) story for:
  - $(n+1)^2 u_{n+1} = (an^2 + an + b)u_n - cn^2 u_{n-1}$ (Beukers, Zagier)
  - $(n+1)^3 u_{n+1} = (2n+1)(an^2 + an + b)u_n - n(cn^2 + d)u_{n-1}$ (Cooper)

The six sporadic Apéry-like numbers

$$(n+1)^3 u_{n+1} = (2n+1)(an^2+an+b)u_n - cn^3 u_{n-1}$$

(a,b,c)	$A(n)$	
$(17,5,1)$	$\sum_k \binom{n}{k}^2 \binom{n+k}{n}^2$	Apéry numbers
$(12,4,16)$	$\sum_k \binom{n}{k}^2 \binom{2k}{n}^2$	Kauers–Zeilberger diagonal
$(10,4,64)$	$\sum_k \binom{n}{k}^2 \binom{2k}{k} \binom{2(n-k)}{n-k}$	Domb numbers
$(7,3,81)$	$\sum_k (-1)^k 3^{n-3k} \binom{n}{3k} \binom{n+k}{n} \frac{(3k)!}{k!^3}$	Almkvist–Zudilin numbers
$(11,5,125)$	$\sum_k (-1)^k \binom{n}{k}^3 \binom{4n-5k}{3n}$	
$(9,3,-27)$	$\sum_{k,l} \binom{n}{k}^2 \binom{n}{l} \binom{k}{l} \binom{k+l}{n}$	

Apéry numbers have remarkable properties

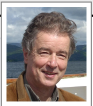


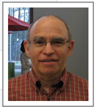
THM Beukers '87

$$\underbrace{\frac{\eta^7(2\tau)\eta^7(3\tau)}{\eta^5(\tau)\eta^5(6\tau)}}_{\text{modular form}} = \sum_{n\geqslant 0} A(n) \underbrace{\left(\frac{\eta^{12}(\tau)\eta^{12}(6\tau)}{\eta^{12}(2\tau)\eta^{12}(3\tau)}\right)^n}_{\text{modular function}}$$

$1 + 5q + 13q^2 + 23q^3 + O(q^4)$ $\qquad$ $q - 12q^2 + 66q^3 + O(q^4)$ $\qquad$ $q = e^{2\pi i\tau}$

Apéry numbers have remarkable properties





THM Beukers '87

$$\underbrace{\frac{\eta^7(2\tau)\eta^7(3\tau)}{\eta^5(\tau)\eta^5(6\tau)}}_{\text{modular form}} = \sum_{n\geqslant 0} A(n) \underbrace{\left(\frac{\eta^{12}(\tau)\eta^{12}(6\tau)}{\eta^{12}(2\tau)\eta^{12}(3\tau)}\right)^n}_{\text{modular function}}$$

$1 + 5q + 13q^2 + 23q^3 + O(q^4)$ $\quad$ $q - 12q^2 + 66q^3 + O(q^4)$

THM Gessel '82

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

n_i are the p-adic digits of n

Apéry numbers have remarkable properties

THM Beukers '87

$$\underbrace{\frac{\eta^7(2\tau)\eta^7(3\tau)}{\eta^5(\tau)\eta^5(6\tau)}}_{\text{modular form}} = \sum_{n\geqslant 0} A(n) \underbrace{\left(\frac{\eta^{12}(\tau)\eta^{12}(6\tau)}{\eta^{12}(2\tau)\eta^{12}(3\tau)}\right)^n}_{\text{modular function}}$$

$1+5q+13q^2+23q^3+O(q^4)$ $\qquad$ $q-12q^2+66q^3+O(q^4)$

THM Gessel '82

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

n_i are the p-adic digits of n

THM Coster '88

$$A(p^r m) \equiv A(p^{r-1}m) \pmod{p^{3r}}$$

Apéry numbers have remarkable properties

THM Beukers '87

$$\underbrace{\frac{\eta^7(2\tau)\eta^7(3\tau)}{\eta^5(\tau)\eta^5(6\tau)}}_{\text{modular form}} = \sum_{n\geqslant 0} A(n) \underbrace{\left(\frac{\eta^{12}(\tau)\eta^{12}(6\tau)}{\eta^{12}(2\tau)\eta^{12}(3\tau)}\right)^n}_{\text{modular function}}$$

$1 + 5q + 13q^2 + 23q^3 + O(q^4)$ $\qquad$ $q - 12q^2 + 66q^3 + O(q^4)$

THM Gessel '82

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

n_i are the p-adic digits of n

THM Coster '88

$$A(p^r m) \equiv A(p^{r-1} m) \pmod{p^{3r}}$$

THM Ahlgren–Ono '00

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

$$f(\tau) = \sum_{n\geqslant 1} c(n) q^n = \eta(2\tau)^4 \eta(4\tau)^4 \in S_4(\Gamma_0(8))$$





Apéry numbers have remarkable properties






THM
Beukers '87

$$\underbrace{\frac{\eta^7(2\tau)\eta^7(3\tau)}{\eta^5(\tau)\eta^5(6\tau)}}_{\text{modular form}} = \sum_{n\geqslant 0} A(n) \underbrace{\left(\frac{\eta^{12}(\tau)\eta^{12}(6\tau)}{\eta^{12}(2\tau)\eta^{12}(3\tau)}\right)^n}_{\text{modular function}}$$

$1 + 5q + 13q^2 + 23q^3 + O(q^4)$ $\qquad$ $q - 12q^2 + 66q^3 + O(q^4)$

THM
Gessel '82

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

n_i are the p-adic digits of n

THM
Coster '88

$$A(p^r m) \equiv A(p^{r-1}m) \pmod{p^{3r}}$$

THM
Ahlgren–Ono '00

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

$$f(\tau) = \sum_{n\geqslant 1} c(n)q^n = \eta(2\tau)^4\eta(4\tau)^4 \in S_4(\Gamma_0(8))$$

THM
Zagier '16

$$A\left(-\tfrac{1}{2}\right) = \frac{16}{\pi^2} L(f, 2)$$

Apéry numbers have remarkable properties

THM Beukers '87

$$\underbrace{\frac{\eta^7(2\tau)\eta^7(3\tau)}{\eta^5(\tau)\eta^5(6\tau)}}_{\text{modular form}} = \sum_{n\geqslant 0} A(n) \underbrace{\left(\frac{\eta^{12}(\tau)\eta^{12}(6\tau)}{\eta^{12}(2\tau)\eta^{12}(3\tau)}\right)^n}_{\text{modular function}}$$

$1+5q+13q^2+23q^3+O(q^4)$ $\qquad$ $q-12q^2+66q^3+O(q^4)$

THM Gessel '82

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

n_i are the p-adic digits of n

THM Coster '88

$$A(p^r m) \equiv A(p^{r-1} m) \pmod{p^{3r}}$$

THM Ahlgren–Ono '00

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

$$f(\tau) = \sum_{n\geqslant 1} c(n)q^n = \eta(2\tau)^4\eta(4\tau)^4 \in S_4(\Gamma_0(8))$$

THM Zagier '16

$$A\left(-\tfrac{1}{2}\right) = \frac{16}{\pi^2} L(f,2)$$

- These extend to **all other** known Apéry-like numbers!!???

! = proven
? = partially known

Approaches to proving Lucas congruences

- From suitable expressions as a binomial sum. Gessel '82, McIntosh '92

Apéry numbers: $\sum_k \binom{n}{k}^2 \binom{n+k}{n}^2$

Sequence (η): $\sum_k (-1)^k \binom{n}{k}^3 \binom{4n-5k}{3n}$

Approaches to proving Lucas congruences

- From suitable expressions as a binomial sum. Gessel '82, McIntosh '92

Apéry numbers: $\sum_k \binom{n}{k}^2 \binom{n+k}{n}^2$

Sequence (η): $\sum_k (-1)^k \binom{n}{k}^3 \binom{4n-5k}{3n}$

- From suitable constant term expressions. Samol–van Straten '09, Mellit–Vlasenko '16

THM Samol, van Straten '09: $A(n) = \mathrm{ct}[P(\boldsymbol{x})^n]$ satisfies the Lucas congruences for any p, if the Newton polytope of $P \in \mathbb{Z}[\boldsymbol{x}^{\pm 1}]$ has the origin as its only interior integral point. (In fact, we get the stronger Dwork congruences.)

$$P = \frac{(x+y)(z+1)(x+y+z)(y+z+1)}{xyz}$$

$$\left(1 - \frac{1}{xy(1+z)^5}\right) \frac{(1+x)(1+y)(1+z)^4}{z^3}$$

Approaches to proving Lucas congruences

- From suitable expressions as a binomial sum. Gessel '82, McIntosh '92

Apéry numbers: $\sum_k \binom{n}{k}^2 \binom{n+k}{n}^2$

Sequence (η): $\sum_k (-1)^k \binom{n}{k}^3 \binom{4n-5k}{3n}$

- From suitable constant term expressions. Samol–van Straten '09, Mellit–Vlasenko '16

THM Samol, van Straten '09: $A(n) = \operatorname{ct}[P(\boldsymbol{x})^n]$ satisfies the Lucas congruences for any p, if the Newton polytope of $P \in \mathbb{Z}[\boldsymbol{x}^{\pm 1}]$ has the origin as its only interior integral point. (In fact, we get the stronger Dwork congruences.)

$$P = \frac{(x+y)(z+1)(x+y+z)(y+z+1)}{xyz}$$

$$\left(1 - \frac{1}{xy(1+z)^5}\right) \frac{(1+x)(1+y)(1+z)^4}{z^3}$$

- From suitable diagonal expressions. Rowland–Yassawi '15

  For instance, diagonals of $1/Q(\boldsymbol{x})$ for $Q(\boldsymbol{x}) \in \mathbb{Z}[\boldsymbol{x}]$ with $Q(\boldsymbol{x})$ linear in each variable and $Q(\boldsymbol{0}) = 1$.

Challenge: finding constant term expressions

THM Malik–S '16: All of the $6+6+3$ known sporadic sequences satisfy Lucas congruences modulo every prime.

- Proof using binomial sums and McIntosh's technique for all but 2 sequences.
- Proof is long and technical for the sequences (η) and s_{18}.

Challenge: finding constant term expressions

THM Malik–S '16 All of the $6+6+3$ known sporadic sequences satisfy Lucas congruences modulo every prime.

- Proof using binomial sums and McIntosh's technique for all but 2 sequences.
- Proof is long and technical for the sequences (η) and s_{18}.

THM Gorodetsky '21 Each sporadic sequence, except possibly (η), can be expressed as $\operatorname{ct}[P(\boldsymbol{x})^n]$ with the Newton polytope of $P \in \mathbb{Z}[\boldsymbol{x}^{\pm 1}]$ having the origin as its only interior integral point.

EG Gorodetsky '21 (η): $$\frac{(zx+xy-yz-x-1)(xy+yz-zx-y-1)(yz+zx-xy-z-1)}{xyz}$$

$(1,0,0)$, $(1,1,0)$ and their permutations are interior points.

Challenge: finding constant term expressions

THM Malik–S '16 — All of the $6+6+3$ known sporadic sequences satisfy Lucas congruences modulo every prime.

- Proof using binomial sums and McIntosh's technique for all but 2 sequences.
- Proof is long and technical for the sequences (η) and s_{18}.

THM Gorodetsky '21 — Each sporadic sequence, except possibly (η), can be expressed as $\operatorname{ct}[P(\boldsymbol{x})^n]$ with the Newton polytope of $P \in \mathbb{Z}[\boldsymbol{x}^{\pm 1}]$ having the origin as its only interior integral point.

EG Gorodetsky '21 — (η): $\dfrac{(zx+xy-yz-x-1)(xy+yz-zx-y-1)(yz+zx-xy-z-1)}{xyz}$

$(1,0,0)$, $(1,1,0)$ and their permutations are interior points.

Q Algorithmic tools to find useful constant term expressions?

Some goals for today

- **Lucas congruences** are interesting.
- **Diagonals** and **constant terms** are useful ways of representing integer sequences.
- **Congruence automata** are a powerful device for capturing the mod p^r values of sequences.
- **Lucas congruences** correspond to single-state (linear) congruence automata.
- Larger automata can be translated into **generalized Lucas congruences**.

- (**Apéry-like sequences** are fascinating.)

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
arXiv:2111.08641