Gessel-Lucas congruences, constant terms, and modular forms

Southern Regional Number Theory Conference
LSU

Armin Straub

March 7, 2026

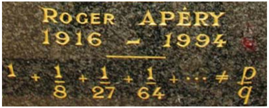
University of South Alabama

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.

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



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

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

$$\binom{145}{37} \equiv \binom{2}{0}\binom{6}{5}\binom{5}{2} = 1 \cdot 6 \cdot 10 \equiv 4 \pmod{7}$$

LHS $= 44141658097075862739392390650979600$

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

$$\binom{145}{37} \equiv \binom{2}{0}\binom{6}{5}\binom{5}{2} = 1\cdot 6\cdot 10 \equiv 4 \pmod{7}$$

LHS $= 4414165809707586273939239065097960 0$

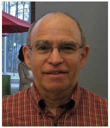
- Interesting sequences like the **Apéry numbers** $1, 5, 73, 1445, \ldots$

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

satisfy such **Lucas congruences** as well:

THM Gessel '82

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



- Equivalently: $A(pn+k) \equiv A(n)A(k) \pmod{p}$

Here and elsewhere: $0 \leqslant k < p$

- 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.

- 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. □

Apéry numbers and the irrationality of $\zeta(3)$

- 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.

Q Beukers, Zagier, Almkvist, Zudilin, Cooper: Are there other tuples (a, b, c) for which the recurrence

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

has an integral solution?

- 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)
- $6+6+3$ **sporadic sequences** known.

The six (basic) sporadic Apéry-like numbers of order 3

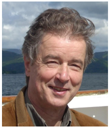
$$(n+1)^3 u_{n+1} = (2n+1)(an^2+an+b)u_n - cn^3 u_{n-1}$$

(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
$(11,5,125)$	$\sum_k (-1)^k \binom{n}{k}^3 \binom{4n-5k}{3n}$	
$(9,3,-27)$	$\sum_{k,l} \binom{n}{k}^2 \binom{n}{l} \binom{k}{l} \binom{k+l}{n}$	

Modularity of Apéry-like numbers

- Beukers ('87) observed that the Apéry numbers $1, 5, 73, 1145, \ldots$

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



satisfy:

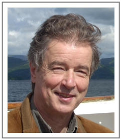
$$\underbrace{\frac{\eta^7(2\tau)\eta^7(3\tau)}{\eta^5(\tau)\eta^5(6\tau)}}_{\text{modular form}} = \sum_{n \geqslant 0} A(n) \underbrace{\left(\frac{\eta^{12}(\tau)\eta^{12}(6\tau)}{\eta^{12}(2\tau)\eta^{12}(3\tau)} \right)^n}_{\text{modular function}}$$

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

Modularity of Apéry-like numbers

- Beukers ('87) observed that the Apéry numbers $1, 5, 73, 1145, \ldots$

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



satisfy:

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

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

FACT Not at all evidently, such a **modular parametrization** exists for all known Apéry-like numbers!

- Context:
  - $f(\tau)$ modular form of weight k
  - $x(\tau)$ modular function
  - $y(x)$ such that $y(x(\tau)) = f(\tau)$

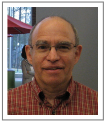
Then $y(x)$ satisfies a linear differential equation of order $k+1$.

- Lucas congruences: $A(pn+k) \equiv A(n)A(k) \pmod{p}$

THM Malik–S '16: All of the $6+6+3$ known sporadic sequences satisfy Lucas congruences modulo every prime. (Proof long and technical for 2 sequences)

- Lucas congruences: $A(pn+k) \equiv A(n)A(k) \pmod{p}$

THM Malik–S '16: All of the $6+6+3$ known sporadic sequences satisfy Lucas congruences modulo every prime. (Proof long and technical for 2 sequences)



- In the case of the Apéry numbers, Gessel ('82) observed that these congruences can be extended modulo p^2.

THM S '24: All of the $6+6+3$ known sporadic sequences satisfy **Gessel–Lucas congruences** modulo every odd prime:

$$A(pn+k) \equiv A(k)A(n) + pnA'(k)A(n) \pmod{p^2}$$

- Here, $A'(n)$ is the formal derivative of $A(n)$.
  These are rational numbers!

The formal derivative of recurrence sequences: example

- $A(n) = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}$ is the unique solution with $A(0) = 1$ to:

$$(n+1)^2 A(n+1) = (11n^2 + 11n + 3) A(n) + n^2 A(n-1)$$

- Then $A'(n)$ is the unique solution with $A'(0) = 0$ to:

$$(n+1)^2 A'(n+1) = (11n^2 + 11n + 3) A'(n) + n^2 A'(n-1)$$
$$- 2(n+1) A(n+1) + 11(2n+1) A(n) + 2n A(n-1)$$

The formal derivative of recurrence sequences: example

- $A(n) = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}$ is the unique solution with $A(0) = 1$ to:

$$(n+1)^2 A(n+1) = (11n^2 + 11n + 3)A(n) + n^2 A(n-1)$$

- Then $A'(n)$ is the unique solution with $A'(0) = 0$ to:

$$(n+1)^2 A'(n+1) = (11n^2 + 11n + 3)A'(n) + n^2 A'(n-1) \\ - 2(n+1)A(n+1) + 11(2n+1)A(n) + 2nA(n-1)$$

EG $A'(1), A'(2), \ldots = 5, \frac{75}{2}, \frac{1855}{6}, \frac{10875}{4}, \frac{299387}{12}, \frac{943397}{4}, \frac{63801107}{28}, \ldots$

The formal derivative of recurrence sequences: example

- $A(n) = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}$ is the unique solution with $A(0) = 1$ to:

$$(n+1)^2 A(n+1) = (11n^2 + 11n + 3)A(n) + n^2 A(n-1)$$

- Then $A'(n)$ is the unique solution with $A'(0) = 0$ to:

$$\begin{aligned}(n+1)^2 A'(n+1) &= (11n^2 + 11n + 3)A'(n) + n^2 A'(n-1) \\ &\quad - 2(n+1)A(n+1) + 11(2n+1)A(n) + 2nA(n-1)\end{aligned}$$

EG $A'(1), A'(2), \ldots = 5,\ \frac{75}{2},\ \frac{1855}{6},\ \frac{10875}{4},\ \frac{299387}{12},\ \frac{943397}{4},\ \frac{63801107}{28},\ \ldots$

- In this particular case, $A'(n)$ can also be taken as a usual derivative:

$$A'(n) = \frac{\mathrm{d}}{\mathrm{d}n} \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k} = 5 \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k} (H_n - H_k)$$

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 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
Suppose the origin is the only interior integral point of the Newton polytope of $P \in \mathbb{Z}[\boldsymbol{x}^{\pm 1}]$.
Then $A(n) = \mathrm{ct}[P(\boldsymbol{x})^n]$ satisfies Lucas 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 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: Suppose the origin is the only interior integral point of the Newton polytope of $P \in \mathbb{Z}[\boldsymbol{x}^{\pm 1}]$.
Then $A(n) = \operatorname{ct}[P(\boldsymbol{x})^n]$ satisfies Lucas 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 $Q(\mathbf{0}) = 1$.

- 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: Suppose the origin is the only interior integral point of the Newton polytope of $P \in \mathbb{Z}[\boldsymbol{x}^{\pm 1}]$.
Then $A(n) = \operatorname{ct}[P(\boldsymbol{x})^n]$ satisfies Lucas 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 $Q(\mathbf{0}) = 1$.

- From suitable **modular parametrizations**. Beukers–Tsai–Ye '25

Lucas congruences in terms of the GF

- Given $F(x) = \sum_{n=0}^{\infty} A(n) x^n$, we write $F_p(x) = \sum_{n=0}^{p-1} A(n) x^n$ for its p-**truncation**.

LEM $A(n)$ satisfies Lucas congruences modulo p

$\iff$ $\dfrac{1}{F^{p-1}(x)}$ modulo p is a polynomial of degree $< p$.

proof

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

$$\iff \quad F(x) \equiv F(x^p) F_p(x) \pmod{p}$$

□

Lucas congruences in terms of the GF

- Given $F(x) = \sum_{n=0}^{\infty} A(n) x^n$, we write $F_p(x) = \sum_{n=0}^{p-1} A(n) x^n$ for its p-**truncation**.

LEM $A(n)$ satisfies Lucas congruences modulo p

$\iff \quad \frac{1}{F^{p-1}(x)}$ modulo p is a polynomial of degree $< p$.

proof

$$\begin{aligned} & A(pn+k) \equiv A(n)A(k) && \pmod{p} \\ \iff \quad & F(x) \equiv F(x^p) F_p(x) && \pmod{p} \\ \iff \quad & F_p(x) \equiv \frac{F(x)}{F(x^p)} && \pmod{p} \end{aligned}$$

□

Lucas congruences in terms of the GF

- Given $F(x) = \sum_{n=0}^{\infty} A(n)x^n$, we write $F_p(x) = \sum_{n=0}^{p-1} A(n)x^n$ for its p-**truncation**.

LEM $A(n)$ satisfies Lucas congruences modulo p

$\iff$ $\dfrac{1}{F^{p-1}(x)}$ modulo p is a polynomial of degree $< p$.

proof

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

$$\iff \quad F(x) \equiv F(x^p)F_p(x) \pmod{p}$$

$$\iff \quad F_p(x) \equiv \frac{F(x)}{F(x^p)} \pmod{p}$$

(by little Fermat) $$\equiv \frac{F(x)}{F^p(x)}$$

□

Lucas congruences in terms of the GF

- Given $F(x) = \sum_{n=0}^{\infty} A(n)x^n$, we write $F_p(x) = \sum_{n=0}^{p-1} A(n)x^n$ for its p-**truncation**.

LEM $A(n)$ satisfies Lucas congruences modulo p

$\iff \quad \dfrac{1}{F^{p-1}(x)}$ modulo p is a polynomial of degree $< p$.

proof

$$\begin{aligned} & A(pn+k) \equiv A(n)A(k) && \pmod{p} \\ \iff \quad & F(x) \equiv F(x^p)F_p(x) && \pmod{p} \\ \iff \quad & F_p(x) \equiv \frac{F(x)}{F(x^p)} && \pmod{p} \\ \text{(by little Fermat)} \quad & \equiv \frac{F(x)}{F^p(x)} = \frac{1}{F^{p-1}(x)} \end{aligned}$$

□

Lucas congruences in terms of the GF

- Given $F(x) = \sum_{n=0}^{\infty} A(n) x^n$, we write $F_p(x) = \sum_{n=0}^{p-1} A(n) x^n$ for its p-**truncation**.

LEM $A(n)$ satisfies Lucas congruences modulo p

$\iff$ $\dfrac{1}{F^{p-1}(x)}$ modulo p is a polynomial of degree $< p$.

proof

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

$$\iff \quad F(x) \equiv F(x^p) F_p(x) \pmod{p}$$

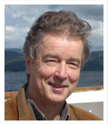
$$\iff \quad F_p(x) \equiv \frac{F(x)}{F(x^p)} \pmod{p}$$

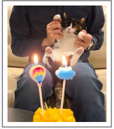
(by little Fermat) $$\equiv \frac{F(x)}{F^p(x)} = \frac{1}{F^{p-1}(x)}$$

Since the first p coefficients of ... always match, the final congruence is equivalent to the RHS being a polynomial of degree $\leqslant p-1$. □

Lucas congruences via modular forms

- Suppose $F(x) = \sum_{n=0}^{\infty} A(n) x^n$ has **modular parametrization**: $F(x)$ is a modular form for some modular function $x(\tau)$.





THM Beukers–Tsai–Ye '25

Suppose that:

- $x(\tau) = q + q^2\mathbb{Z}[[q]]$ with $q = e^{2\pi i\tau}$ is a **Hauptmodul** for $\Gamma = \Gamma_0(N)$ (or Atkin–Lehner extension).
- $F(x(\tau)) = 1 + q\mathbb{Z}[[q]]$ is a weight 2 modular form for Γ.
- $F(x(\tau))$ has a unique zero at $[\tau_0]$ of order $\leqslant 1$, where $[\tau_0]$ is the (unique) pole of $x(\tau)$.

Then $A(n)$ satisfies the Lucas congruences for all primes p.

Lucas congruences via modular forms

- Suppose $F(x) = \sum_{n=0}^{\infty} A(n) x^n$ has **modular parametrization**:
  $F(x)$ is a modular form for some modular function $x(\tau)$.

THM Beukers–Tsai–Ye '25

Suppose that:

- $x(\tau) = q + q^2 \mathbb{Z}[[q]]$ with $q = e^{2\pi i \tau}$ is a **Hauptmodul** for $\Gamma = \Gamma_0(N)$ (or Atkin–Lehner extension).
- $F(x(\tau)) = 1 + q\mathbb{Z}[[q]]$ is a weight 2 modular form for Γ.
- $F(x(\tau))$ has a unique zero at $[\tau_0]$ of order $\leqslant 1$, where $[\tau_0]$ is the (unique) pole of $x(\tau)$.

Then $A(n)$ satisfies the Lucas congruences for all primes p.

proof

$$\frac{1}{F^{p-1}(x)} \equiv \qquad\qquad \pmod{p}$$

□

Lucas congruences via modular forms

- Suppose $F(x) = \sum_{n=0}^{\infty} A(n)x^n$ has **modular parametrization**:

  $F(x)$ is a modular form for some modular function $x(\tau)$.

THM Beukers–Tsai–Ye '25

Suppose that:

- $x(\tau) = q + q^2\mathbb{Z}[[q]]$ with $q = \mathrm{e}^{2\pi i\tau}$ is a **Hauptmodul** for $\Gamma = \Gamma_0(N)$ (or Atkin–Lehner extension).
- $F(x(\tau)) = 1 + q\mathbb{Z}[[q]]$ is a weight 2 modular form for Γ.
- $F(x(\tau))$ has a unique zero at $[\tau_0]$ of order $\leqslant 1$, where $[\tau_0]$ is the (unique) pole of $x(\tau)$.

Then $A(n)$ satisfies the Lucas congruences for all primes p.

proof

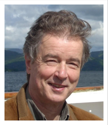
$$\frac{1}{F^{p-1}(x)} \equiv \frac{E(\tau)}{F^{p-1}(x)} \pmod{p}$$

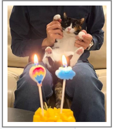
- $E(\tau)$ is chosen to be a modular form for Γ with weight $2(p-1)$ such that $E(\tau) \equiv 1 \pmod{p}$.

□

Lucas congruences via modular forms

- Suppose $F(x) = \sum_{n=0}^{\infty} A(n) x^n$ has **modular parametrization**:
  $F(x)$ is a modular form for some modular function $x(\tau)$.





THM Beukers–Tsai–Ye '25

Suppose that:

- $x(\tau) = q + q^2\mathbb{Z}[[q]]$ with $q = e^{2\pi i\tau}$ is a **Hauptmodul** for $\Gamma = \Gamma_0(N)$ (or Atkin–Lehner extension).
- $F(x(\tau)) = 1 + q\mathbb{Z}[[q]]$ is a weight 2 modular form for Γ.
- $F(x(\tau))$ has a unique zero at $[\tau_0]$ of order $\leqslant 1$, where $[\tau_0]$ is the (unique) pole of $x(\tau)$.

Then $A(n)$ satisfies the Lucas congruences for all primes p.

proof

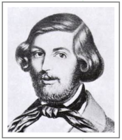
$$\frac{1}{F^{p-1}(x)} \equiv \frac{E(\tau)}{F^{p-1}(x)} = \mathrm{poly}(x) \pmod{p}$$

- $E(\tau)$ is chosen to be a modular form for Γ with weight $2(p-1)$ such that $E(\tau) \equiv 1 \pmod{p}$.
- The modular function has a unique pole at $[\tau_0]$ of order $\leqslant p-1$.

□

- Needed: weight $2(p-1)$ modular form $E(\tau)$ for Γ with $E(\tau) \equiv 1 \pmod{p}$.

EG The normalized **Eisenstein series**



$$E_k(\tau) = 1 + \frac{2k}{B_k} \sum_{n=1}^{\infty} \frac{n^{k-1} q^n}{1 - q^n}$$

is a modular form for $\Gamma_0(1)$ of even weight $k \geqslant 2$.

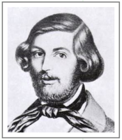
Since $1/B_{p-1} \equiv 0 \pmod{p}$, we have $E_{p-1}(\tau) \equiv 1 \pmod{p}$.

Lucas congruences via modular forms, cont'd

- Needed: weight $2(p-1)$ modular form $E(\tau)$ for Γ with $E(\tau) \equiv 1 \pmod{p}$.

EG The normalized **Eisenstein series**

$$E_k(\tau) = 1 + \frac{2k}{B_k} \sum_{n=1}^{\infty} \frac{n^{k-1} q^n}{1 - q^n}$$



is a modular form for $\Gamma_0(1)$ of even weight $k \geqslant 2$.

Since $1/B_{p-1} \equiv 0 \pmod{p}$, we have $E_{p-1}(\tau) \equiv 1 \pmod{p}$.

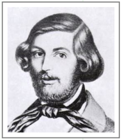
- If $p \geqslant 5$ and $\Gamma = \Gamma_0(N)$, we can select:

  $E(\tau) := E_{p-1}(\tau)^2$

- Needed: weight $2(p-1)$ modular form $E(\tau)$ for Γ with $E(\tau) \equiv 1 \pmod{p}$.

EG The normalized **Eisenstein series**

$$E_k(\tau) = 1 + \frac{2k}{B_k} \sum_{n=1}^{\infty} \frac{n^{k-1} q^n}{1 - q^n}$$



is a modular form for $\Gamma_0(1)$ of even weight $k \geqslant 2$.

Since $1/B_{p-1} \equiv 0 \pmod{p}$, we have $E_{p-1}(\tau) \equiv 1 \pmod{p}$.

- If $p \geqslant 5$ and $\Gamma = \Gamma_0(N)$, we can select:

  $E(\tau) := E_{p-1}(\tau)^2$

- If $p \geqslant 5$ and Γ is $\Gamma_0(N)$ extended by $\tau \to -\frac{1}{N\tau}$:

  $E(\tau) := \frac{1}{2} \left[E_{p-1}(\tau)^2 + N^{p-1} E_{p-1}(N\tau)^2 \right]$

Conclusions

THM
S '24

The known sporadic sequences satisfy the **Gessel–Lucas congruences**

$$A(pn+k) \equiv A(k)A(n) + pnA'(k)A(n) \pmod{p^2}.$$

- These generalize:
  - Lucas congruences: $A(pn+k) \equiv A(k)A(n) \pmod{p}$
  - **Supercongruences:** $A(pn) \equiv A(n) \pmod{p^2}$
- Beukers, Tsai, Ye are working on modular forms proof of Gessel–Lucas congruences.
- In terms of **linear p-schemes**:
  - Lucas congruences correspond to single-state schemes.
  - Gessel–Lucas congruences are instances of 2-state schemes.

  It would be of interest to study **few-state p-schemes** systematically.
- Are there interesting q-**analogs**?
  - q-Lucas congruences have been studied. Olive '65, Désarménien '82
  - q-analogs known for some supercongruences. S '19, Gorodetsky '19

THANK YOU!

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

Frits Beukers, Wei-Lun Tsai, Dongxi Ye
Lucas congruences using modular forms
Bulletin of the London Mathematical Society, Vol. 57, 2025, p. 69-78

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

Armin Straub
Gessel-Lucas congruences for sporadic sequences
Monatshefte für Mathematik, Vol. 203, 2024, p. 883–898

Time?

Bonus material:

Lucas and **Gessel–Lucas** congruences are natural from the point of view of **congruence automata**

Sporadic sequences mod p^r are automatic

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.

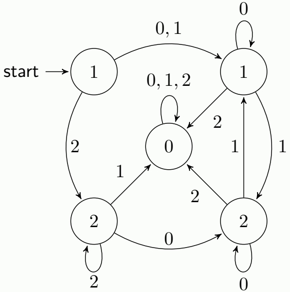
Sporadic sequences mod p^r are automatic

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:

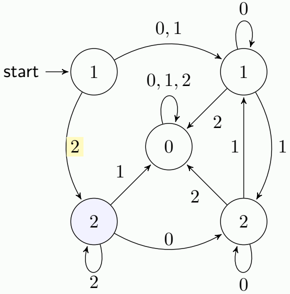
$35 = 1\ 0\ 2\ 2$ in base 3

Sporadic sequences mod p^r are automatic

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

$C(2)$

$C(2) \equiv 2$

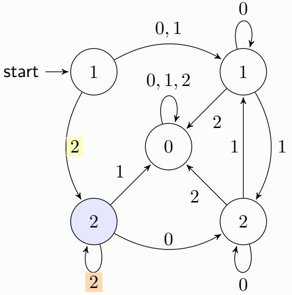
Sporadic sequences mod p^r are automatic

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

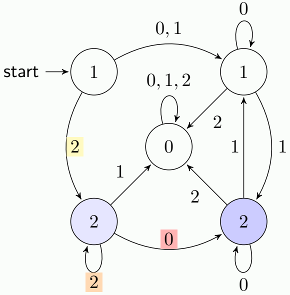
$C(2)$ $\quad C(2) \equiv 2$

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

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

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

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

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

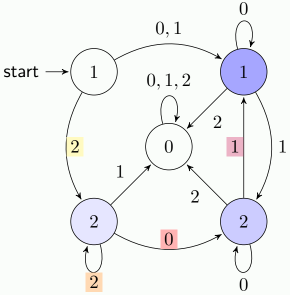
Sporadic sequences mod p^r are automatic

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:



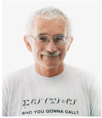
$$C(35) = 3{,}116{,}285{,}494{,}907{,}301{,}262$$
$$\equiv 1 \pmod 3)$$

Instead via automaton:

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

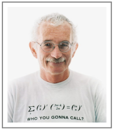
$C(2)$	$C(2) \equiv 2$
$C(8)$	$C(2\ 2) \equiv 2$
	$C(0\ 2\ 2) \equiv 2$
$C(35)$	$C(1\ 0\ 2\ 2) \equiv 1$

- The Catalan numbers $C(n)$ modulo 3 can be described:
  - by an automaton with 4 states (plus a zero state)
  - by a **linear** 3**-scheme** with 2 states (Rowland–Zeilberger '14)



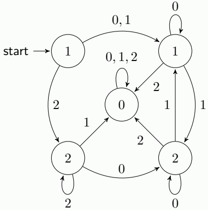
Linear congruence schemes

- The Catalan numbers $C(n)$ modulo 3 can be described:
  - by an automaton with 4 states (plus a zero state)
  - by a **linear** 3**-scheme** with 2 states (Rowland–Zeilberger '14)



EG mod 3

automatic 3-scheme

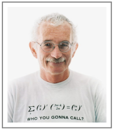


$$\begin{aligned} A_0(3n) &= A_1(n) & A_2(3n) &= A_3(n) \\ A_0(3n+1) &= A_1(n) & A_2(3n+1) &= 0 \\ A_0(3n+2) &= A_2(n) & A_2(3n+2) &= A_2(n) \\ A_1(3n) &= A_1(n) & A_3(3n) &= A_3(n) \\ A_1(3n+1) &= A_3(n) & A_3(3n+1) &= A_1(n) \\ A_1(3n+2) &= 0 & A_3(3n+2) &= 0 \end{aligned}$$

Initial conditions:

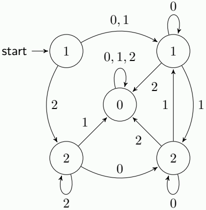
$A_0(0) = A_1(0) = 1, \quad A_2(0) = A_3(0) = 2$

- The Catalan numbers $C(n)$ modulo 3 can be described:
  - by an automaton with 4 states (plus a zero state)
  - by a **linear 3-scheme** with 2 states (Rowland–Zeilberger '14)



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

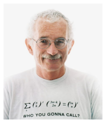
linear 3-scheme

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

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

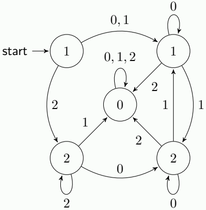
Linear congruence schemes

- The Catalan numbers $C(n)$ modulo 3 can be described:
  - by an automaton with 4 states (plus a zero state)
  - by a **linear 3-scheme** with 2 states (Rowland–Zeilberger '14)



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

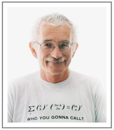
linear 3-scheme

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

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

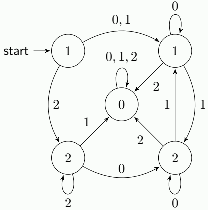
Linear congruence schemes

- The Catalan numbers $C(n)$ modulo 3 can be described:
  - by an automaton with 4 states (plus a zero state)
  - by a **linear 3-scheme** with 2 states (Rowland–Zeilberger '14)



EG mod 3

automatic 3-scheme



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

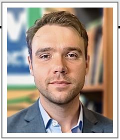
Initial conditions:
$A_0(0) = A_1(0) = 1, \quad A_2(0) = A_3(0) = 2$

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

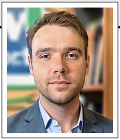


Lucas congruences:

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

PROP Henningsen S '22

$A(n) \pmod{p}$ satisfies a single-state linear p-scheme (and $A(0)=1$).
$\iff A(n)$ satisfies Lucas congruences modulo p.



Lucas congruences:

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

PROP Henningsen S '22 — $A(n) \pmod{p}$ satisfies a single-state linear p-scheme (and $A(0)=1$).
$\iff$ $A(n)$ satisfies Lucas congruences modulo p.

Gessel–Lucas congruences:

$$A(pn+k) \equiv A(k)A(n) + pnA'(k)A(n) \pmod{p^2}$$

Note Gessel–Lucas congruences yield explicit 2-state linear p-schemes.

The formal derivative of recurrence sequences

- Suppose $A(n)$ is the unique solution for all $n \geqslant 0$ to

$$\sum_{j=0}^{r} c_j(n) A(n-j) = 0 \qquad \text{with } A(0) = 1 \text{ and } A(j) = 0 \text{ for } j < 0.$$

The $c_j(n)$ are polynomials with $c_0(n) \in n^2\mathbb{Z}[n]$ and $c_0(n) \neq 0$ for $n > 0$.

The formal derivative of recurrence sequences

- Suppose $A(n)$ is the unique solution for all $n \geqslant 0$ to

$$\sum_{j=0}^{r} c_j(n) A(n-j) = 0 \qquad \text{with } A(0) = 1 \text{ and } A(j) = 0 \text{ for } j < 0.$$

  The $c_j(n)$ are polynomials with $c_0(n) \in n^2\mathbb{Z}[n]$ and $c_0(n) \neq 0$ for $n > 0$.
- Then the **formal derivative** $A'(n)$ is the unique solution to

$$\sum_{j=0}^{r} c_j(n) A'(n-j) + \sum_{j=0}^{r} c_j'(n) A(n-j) = 0 \qquad \text{with } A'(j) = 0 \text{ for } j \leqslant 0.$$

The formal derivative of recurrence sequences

- Suppose $A(n)$ is the unique solution for all $n \geqslant 0$ to

$$\sum_{j=0}^{r} c_j(n) A(n-j) = 0 \qquad \text{with } A(0) = 1 \text{ and } A(j) = 0 \text{ for } j < 0.$$

  The $c_j(n)$ are polynomials with $c_0(n) \in n^2\mathbb{Z}[n]$ and $c_0(n) \neq 0$ for $n > 0$.

- Then the **formal derivative** $A'(n)$ is the unique solution to

$$\sum_{j=0}^{r} c_j(n) A'(n-j) + \sum_{j=0}^{r} c_j'(n) A(n-j) = 0 \qquad \text{with } A'(j) = 0 \text{ for } j \leqslant 0.$$

Note Let $F(x) = \sum_{n \geqslant 0} A(n) x^n$ and $G(x) = \sum_{n \geqslant 1} A'(n) x^n$.

Then the corresponding differential equation satisfied by $F(x)$ is also solved by $\log(x) F(x) + G(x)$.

THANK YOU!

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

Frits Beukers, Wei-Lun Tsai, Dongxi Ye
Lucas congruences using modular forms
Bulletin of the London Mathematical Society, Vol. 57, 2025, p. 69-78

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

Armin Straub
Gessel-Lucas congruences for sporadic sequences
Monatshefte für Mathematik, Vol. 203, 2024, p. 883–898