

Wholesale congruences for sequences arising in combinatorics

Eric Rowland
Hofstra University

Joint work with Reem Yassawi

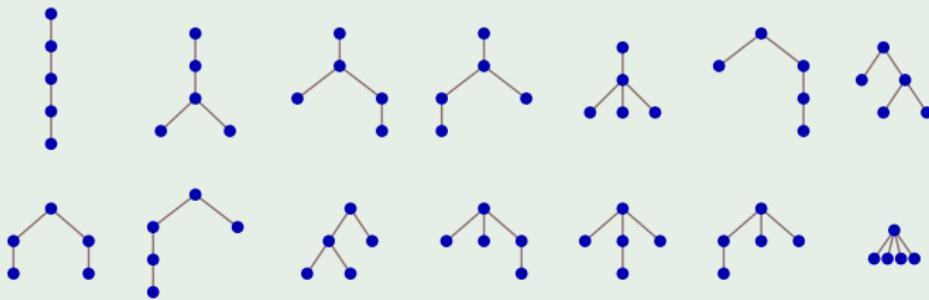
The Open University Pure Mathematics Colloquium
2022–09–14

What do combinatorial sequences look like modulo a prime power?

What do combinatorial sequences look like modulo a prime power?

Example

How many plane trees have n edges?



$$C(4) = 14$$

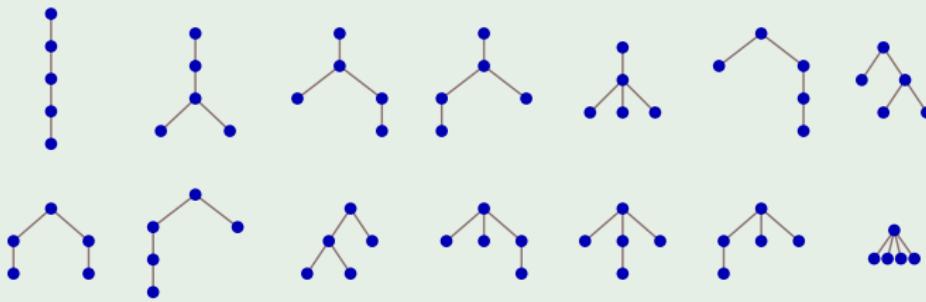
Catalan numbers:

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

What do combinatorial sequences look like modulo a prime power?

Example

How many plane trees have n edges?



$$C(4) = 14$$

Catalan numbers:

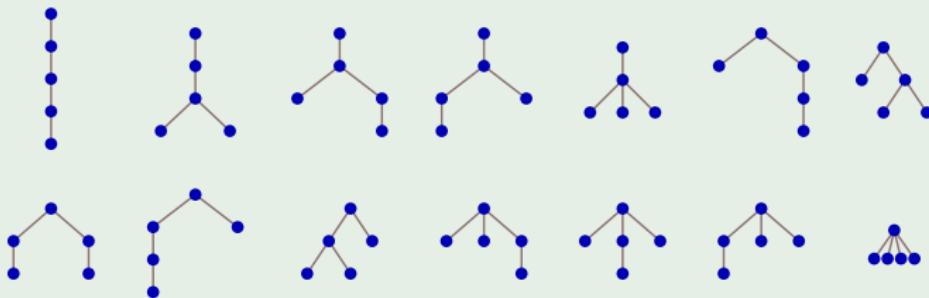
$$C(n)_{n \geq 0} = 1, 1, 2, 5, 14, 42, 132, 429, \dots$$

$$\text{Modulo 2: } 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, \dots$$

What do combinatorial sequences look like modulo a prime power?

Example

How many plane trees have n edges?



$$C(4) = 14$$

Catalan numbers:

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

$$\text{Modulo 2: } 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, \dots$$

$C(n)$ is odd if and only if $n + 1$ is a power of 2.

(follows from Kummer 1852)

Catalan numbers modulo 4: 1, 1, 2, 1, 2, 2, 0, 1, 2, 2, 0, 2, 0, 0, 0, 1, ...

Theorem (Eu–Liu–Yeh 2008)

For all $n \geq 0$,

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

Catalan numbers modulo 4: 1, 1, 2, 1, 2, 2, 0, 1, 2, 2, 0, 2, 0, 0, 0, 1, ...

Theorem (Eu–Liu–Yeh 2008)

For all $n \geq 0$,

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

In particular, $C(n) \not\equiv 3 \pmod{4}$.

Catalan numbers modulo 4: 1, 1, 2, 1, 2, 2, 0, 1, 2, 2, 0, 2, 0, 0, 0, 1, ...

Theorem (Eu–Liu–Yeh 2008)

For all $n \geq 0$,

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

In particular, $C(n) \not\equiv 3 \pmod{4}$.

Catalan numbers modulo 8: 1, 1, 2, 5, 6, 2, 4, 5, 6, 6, 4, 2, 4, 4, 0, 5, ...

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

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

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

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

$$c_n \equiv_{16} \begin{cases} 1 & \text{if } d(\alpha) = 0 \text{ and } \begin{cases} \beta \leq 1, \\ \beta = 2, \\ \beta \geq 3, \end{cases} \\ 5 & \text{if } d(\alpha) = 1, \alpha = 1 \text{ and } \begin{cases} \beta = 0 \text{ or } \beta \geq 2, \\ \beta = 1, \end{cases} \\ 13 & \text{if } d(\alpha) = 1, \alpha \geq 2 \text{ and } \begin{cases} (\alpha = 2, \beta \geq 2) \text{ or } (\alpha \geq 3, \beta \leq 1), \\ (\alpha = 2, \beta \leq 1) \text{ or } (\alpha \geq 3, \beta \geq 2), \end{cases} \\ 2 & \text{if } d(\alpha) = 2 \text{ and } \begin{cases} zr(\alpha) \equiv_2 0, \\ zr(\alpha) = 1, \end{cases} \\ 10 & \text{if } d(\alpha) = 3, \\ 14 & \text{if } d(\alpha) \geq 4. \end{cases}$$

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

They also determined $C(n) \bmod 64$.

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

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

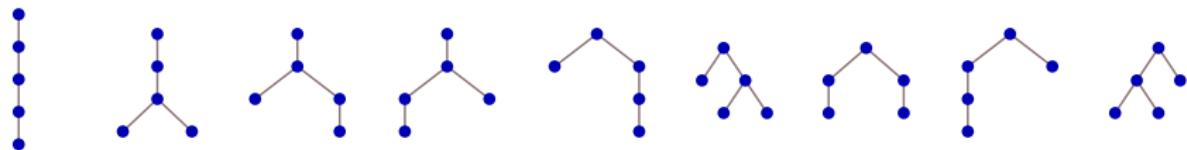
$$c_n \equiv_{16} \begin{cases} 1 & \text{if } d(\alpha) = 0 \text{ and } \begin{cases} \beta \leq 1, \\ \beta = 2, \\ \beta \geq 3, \end{cases} \\ 5 \\ 13 \\ 2 & \text{if } d(\alpha) = 1, \alpha = 1 \text{ and } \begin{cases} \beta = 0 \text{ or } \beta \geq 2, \\ \beta = 1, \end{cases} \\ 10 \\ 6 &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

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

They also determined $C(n) \bmod 64$.

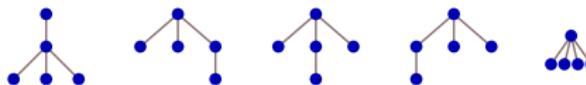
What is the right framework?

How many plane trees with n edges have the property that each vertex has at most 2 children?

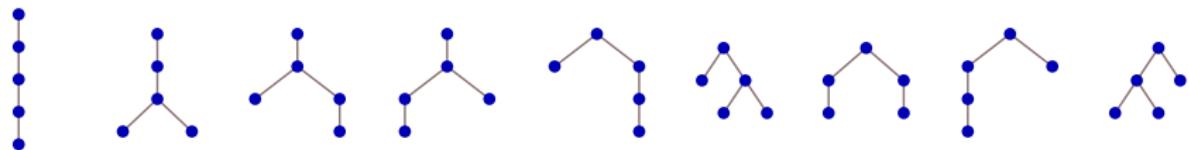


$$M(4) = 9$$

Excluded:

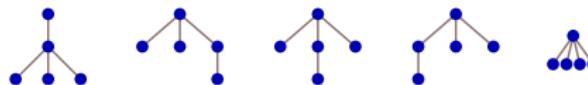


How many plane trees with n edges have the property that each vertex has at most 2 children?



$$M(4) = 9$$

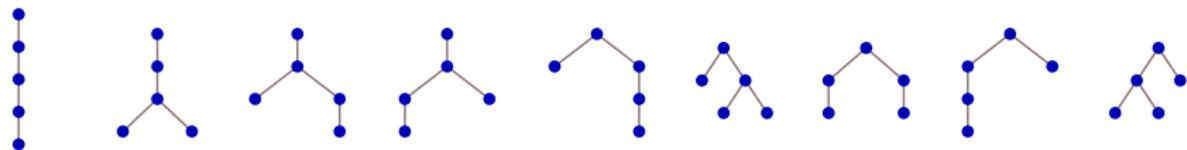
Excluded:



Motzkin numbers:

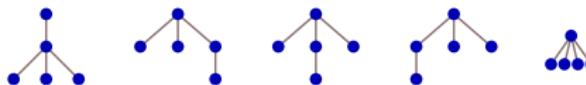
$$M(n)_{n \geq 0} = 1, 1, 2, 4, 9, 21, 51, 127, \dots$$

How many plane trees with n edges have the property that each vertex has at most 2 children?



$$M(4) = 9$$

Excluded:

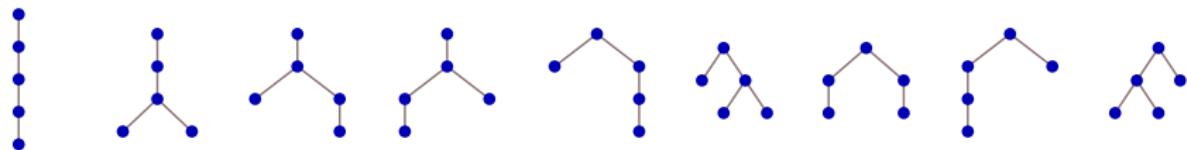


Motzkin numbers:

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

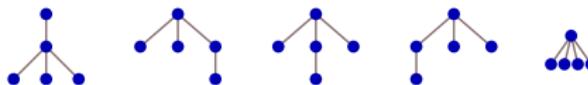
Modulo 8: 1, 1, 2, 4, 1, 5, 3, 7, 3, 3, 4, 6, 7, 3, 2, 4, ...

How many plane trees with n edges have the property that each vertex has at most 2 children?



$$M(4) = 9$$

Excluded:



Motzkin numbers:

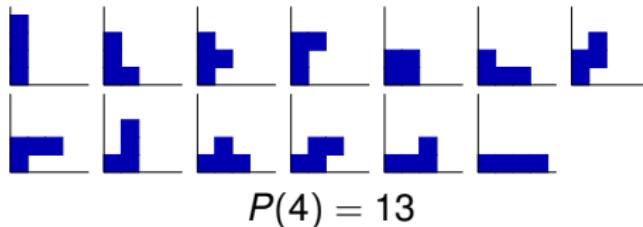
$$M(n)_{n \geq 0} = 1, 1, 2, 4, 9, 21, 51, 127, \dots$$

$$\text{Modulo 8: } 1, 1, 2, 4, 1, 5, 3, 7, 3, 3, 4, 6, 7, 3, 2, 4, \dots$$

Theorem (Eu–Liu–Yeh; conj. by Deutsch–Sagan–Amdeberhan)

$$M(n) \not\equiv 0 \pmod{8} \text{ for all } n \geq 0.$$

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



Number of restricted hexagonal polyominoes:

$H(n)_{n \geq 0} = 1, 1, 3, 10, 36, 137, 543, 2219, \dots$

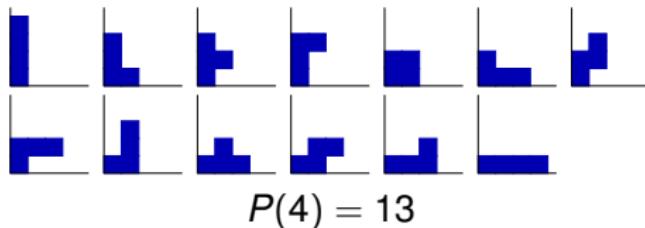
Riordan numbers: $R(n)_{n \geq 0} = 1, 0, 1, 1, 3, 6, 15, 36, \dots$

Theorem (Deutsch–Sagan 2006)

There exists a set $C = \{1, 3, 4, 5, 7, \dots\}$ with the property that

- $P(n)$ is even if and only if $n \in 2C$,
- $H(n)$ is even if and only if $n \in 4C - 1$ or $n \in 4C$, and
- $R(n)$ is even if and only if $n \in 2C - 1$.

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



Number of restricted hexagonal polyominoes:

$H(n)_{n \geq 0} = 1, 1, 3, 10, 36, 137, 543, 2219, \dots$

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

Theorem (Deutsch–Sagan 2006)

There exists a set $C = \{1, 3, 4, 5, 7, \dots\}$ with the property that

- $P(n)$ is even if and only if $n \in 2C$,
- $H(n)$ is even if and only if $n \in 4C - 1$ or $n \in 4C$, and
- $R(n)$ is even if and only if $n \in 2C - 1$.

Can we obtain and prove such results automatically?

Algebraic sequences

$s(n)_{n \geq 0}$ is **algebraic** if there is a nonzero polynomial $P(x, y)$ such that

$$P\left(x, \sum_{n \geq 0} s(n)x^n\right) = 0.$$

$C(n)_{n \geq 0}, M(n)_{n \geq 0}, P(n)_{n \geq 0}, H(n)_{n \geq 0}, R(n)_{n \geq 0}$ are all algebraic.

Example

For the Catalan numbers...

$y = \sum_{n \geq 0} C(n)x^n$ satisfies $xy^2 - y + 1 = 0$ over \mathbb{Q} .

Algebraic sequences

$s(n)_{n \geq 0}$ is **algebraic** if there is a nonzero polynomial $P(x, y)$ such that

$$P\left(x, \sum_{n \geq 0} s(n)x^n\right) = 0.$$

$C(n)_{n \geq 0}, M(n)_{n \geq 0}, P(n)_{n \geq 0}, H(n)_{n \geq 0}, R(n)_{n \geq 0}$ are all algebraic.

Example

For the Catalan numbers...

$y = \sum_{n \geq 0} C(n)x^n$ satisfies $xy^2 - y + 1 = 0$ over \mathbb{Q} .

$y = \sum_{n \geq 0} (C(n) \bmod 3)x^n$ satisfies $xy^2 + 2y + 1 = 0$ over \mathbb{F}_3 .

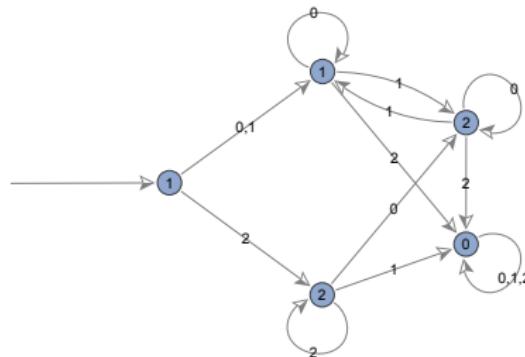
\mathbb{F}_p denotes the finite field with p elements.

Automatic sequences

$s(n)_{n \geq 0}$ is ***p*-automatic** if there is an automaton that outputs $s(n)$ when fed the base- p digits of n .

Convention in this talk: start with the least significant digit.

This automaton computes $C(n) \bmod 3$:



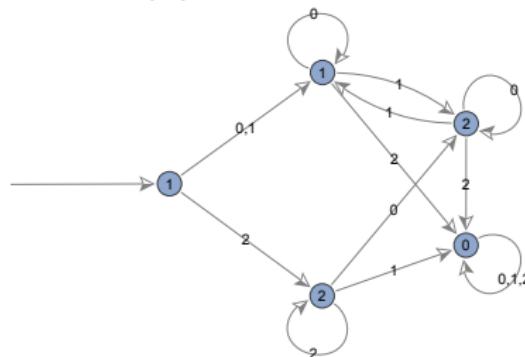
$$C(9) \equiv ? \pmod{3}.$$

Automatic sequences

$s(n)_{n \geq 0}$ is ***p*-automatic** if there is an automaton that outputs $s(n)$ when fed the base- p digits of n .

Convention in this talk: start with the least significant digit.

This automaton computes $C(n) \bmod 3$:



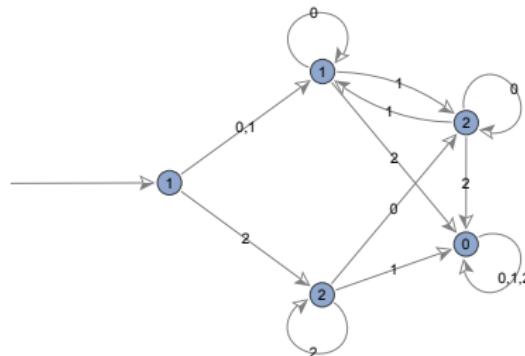
$C(9) \equiv ? \pmod{3}$. Since $9 = 100_3$, $C(9) \equiv$

Automatic sequences

$s(n)_{n \geq 0}$ is ***p*-automatic** if there is an automaton that outputs $s(n)$ when fed the base- p digits of n .

Convention in this talk: start with the least significant digit.

This automaton computes $C(n) \bmod 3$:



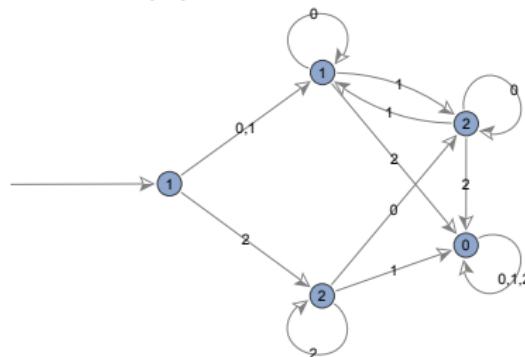
$C(9) \equiv ? \pmod{3}$. Since $9 = 100_3$, $C(9) \equiv \boxed{2} \pmod{3}$.

Automatic sequences

$s(n)_{n \geq 0}$ is ***p-automatic*** if there is an automaton that outputs $s(n)$ when fed the base- p digits of n .

Convention in this talk: start with the least significant digit.

This automaton computes $C(n) \bmod 3$:

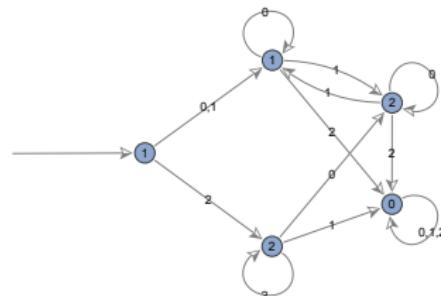


$C(9) \equiv ? \pmod{3}$. Since $9 = 100_3$, $C(9) \equiv \boxed{2} \pmod{3}$.

$(C(n) \bmod 3)_{n \geq 0} = 1, 1, 2, 2, 2, 0, 0, 0, 2, 2, \dots$ is ***3-automatic***.

Two representations: polynomials and automata.

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

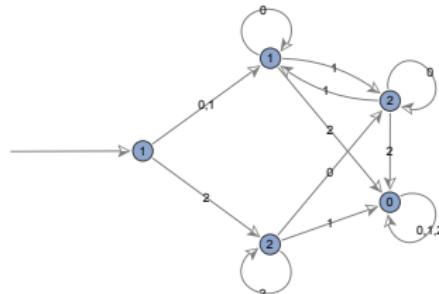


Polynomial: easy to get from the polynomial over \mathbb{Q} .

Automaton: direct information about $s(n)$.

Two representations: polynomials and automata.

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



Polynomial: easy to get from the polynomial over \mathbb{Q} .

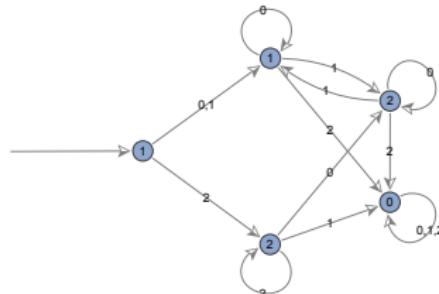
Automaton: direct information about $s(n)$.

Theorem (Christol 1979/1980)

A sequence $s(n)_{n \geq 0}$ of elements in \mathbb{F}_p is algebraic if and only if it is p -automatic.

Two representations: polynomials and automata.

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



Polynomial: easy to get from the polynomial over \mathbb{Q} .

Automaton: direct information about $s(n)$.

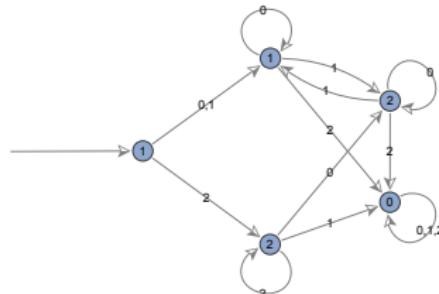
Theorem (Christol 1979/1980)

A sequence $s(n)_{n \geq 0}$ of elements in \mathbb{F}_p is algebraic if and only if it is p -automatic.

How do we convert a polynomial into an automaton?

Two representations: polynomials and automata.

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



Polynomial: easy to get from the polynomial over \mathbb{Q} .

Automaton: direct information about $s(n)$.

Theorem (Christol 1979/1980)

A sequence $s(n)_{n \geq 0}$ of elements in \mathbb{F}_p is algebraic if and only if it is p -automatic.

How do we convert a polynomial into an automaton?

How does the automaton size depend on the polynomial degree?

How to tell whether a sequence is p -automatic?

Let $r \in \{0, 1, \dots, p - 1\}$.

The **Cartier operator** Λ_r picks out every p th term, starting with $s(r)$:

$$\Lambda_r(s(n)_{n \geq 0}) := s(pn + r)_{n \geq 0}$$

How to tell whether a sequence is p -automatic?

Let $r \in \{0, 1, \dots, p - 1\}$.

The **Cartier operator** Λ_r picks out every p th term, starting with $s(r)$:

$$\Lambda_r(s(n)_{n \geq 0}) := s(pn + r)_{n \geq 0}$$

Iteratively apply $\Lambda_0, \Lambda_1, \dots, \Lambda_{p-1}$ to $s(n)_{n \geq 0}$.

Create one state in the automaton for each distinct sequence.

How to tell whether a sequence is p -automatic?

Let $r \in \{0, 1, \dots, p - 1\}$.

The **Cartier operator** Λ_r picks out every p th term, starting with $s(r)$:

$$\Lambda_r(s(n)_{n \geq 0}) := s(pn + r)_{n \geq 0}$$

Iteratively apply $\Lambda_0, \Lambda_1, \dots, \Lambda_{p-1}$ to $s(n)_{n \geq 0}$.

Create one state in the automaton for each distinct sequence.

Let $s(n) = (C(n) \bmod 3)$. $s(n)_{n \geq 0} = 1, 1, 2, 2, 2, 0, 0, 0, 2, \dots$

How to tell whether a sequence is p -automatic?

Let $r \in \{0, 1, \dots, p - 1\}$.

The **Cartier operator** Λ_r picks out every p th term, starting with $s(r)$:

$$\Lambda_r(s(n)_{n \geq 0}) := s(pn + r)_{n \geq 0}$$

Iteratively apply $\Lambda_0, \Lambda_1, \dots, \Lambda_{p-1}$ to $s(n)_{n \geq 0}$.

Create one state in the automaton for each distinct sequence.

Let $s(n) = (C(n) \bmod 3)$. $s(n)_{n \geq 0} = 1, 1, 2, 2, 2, 0, 0, 0, 2, \dots$

$$\Lambda_0(s(n)_{n \geq 0}) = s(3n + 0)_{n \geq 0} = 1, 2, 0, 2, 1, 0, 0, 0, 0, \dots$$

How to tell whether a sequence is p -automatic?

Let $r \in \{0, 1, \dots, p - 1\}$.

The **Cartier operator** Λ_r picks out every p th term, starting with $s(r)$:

$$\Lambda_r(s(n)_{n \geq 0}) := s(pn + r)_{n \geq 0}$$

Iteratively apply $\Lambda_0, \Lambda_1, \dots, \Lambda_{p-1}$ to $s(n)_{n \geq 0}$.

Create one state in the automaton for each distinct sequence.

Let $s(n) = (C(n) \bmod 3)$. $s(n)_{n \geq 0} = 1, 1, 2, 2, 2, 0, 0, 0, 2, \dots$

$\Lambda_0(s(n)_{n \geq 0}) = s(3n + 0)_{n \geq 0} = 1, 2, 0, 2, 1, 0, 0, 0, 0, \dots$ new!

How to tell whether a sequence is p -automatic?

Let $r \in \{0, 1, \dots, p - 1\}$.

The **Cartier operator** Λ_r picks out every p th term, starting with $s(r)$:

$$\Lambda_r(s(n)_{n \geq 0}) := s(pn + r)_{n \geq 0}$$

Iteratively apply $\Lambda_0, \Lambda_1, \dots, \Lambda_{p-1}$ to $s(n)_{n \geq 0}$.

Create one state in the automaton for each distinct sequence.

Let $s(n) = (C(n) \bmod 3)$. $s(n)_{n \geq 0} = 1, 1, 2, 2, 2, 0, 0, 0, 2, \dots$

$$\Lambda_0(s(n)_{n \geq 0}) = s(3n + 0)_{n \geq 0} = 1, 2, 0, 2, 1, 0, 0, 0, 0, \dots \quad \text{new!}$$

$$\Lambda_1(s(n)_{n \geq 0}) = s(3n + 1)_{n \geq 0} = 1, 2, 0, 2, 1, 0, 0, 0, 0, \dots$$

How to tell whether a sequence is p -automatic?

Let $r \in \{0, 1, \dots, p - 1\}$.

The **Cartier operator** Λ_r picks out every p th term, starting with $s(r)$:

$$\Lambda_r(s(n)_{n \geq 0}) := s(pn + r)_{n \geq 0}$$

Iteratively apply $\Lambda_0, \Lambda_1, \dots, \Lambda_{p-1}$ to $s(n)_{n \geq 0}$.

Create one state in the automaton for each distinct sequence.

Let $s(n) = (C(n) \bmod 3)$. $s(n)_{n \geq 0} = 1, 1, 2, 2, 2, 0, 0, 0, 2, \dots$

$$\Lambda_0(s(n)_{n \geq 0}) = s(3n + 0)_{n \geq 0} = 1, 2, 0, 2, 1, 0, 0, 0, 0, \dots \quad \text{new!}$$

$$\Lambda_1(s(n)_{n \geq 0}) = s(3n + 1)_{n \geq 0} = 1, 2, 0, 2, 1, 0, 0, 0, 0, \dots = \Lambda_0(s(n)_{n \geq 0})$$

How to tell whether a sequence is p -automatic?

Let $r \in \{0, 1, \dots, p - 1\}$.

The **Cartier operator** Λ_r picks out every p th term, starting with $s(r)$:

$$\Lambda_r(s(n)_{n \geq 0}) := s(pn + r)_{n \geq 0}$$

Iteratively apply $\Lambda_0, \Lambda_1, \dots, \Lambda_{p-1}$ to $s(n)_{n \geq 0}$.

Create one state in the automaton for each distinct sequence.

Let $s(n) = (C(n) \bmod 3)$. $s(n)_{n \geq 0} = 1, 1, 2, 2, 2, 0, 0, 0, 2, \dots$

$$\Lambda_0(s(n)_{n \geq 0}) = s(3n + 0)_{n \geq 0} = 1, 2, 0, 2, 1, 0, 0, 0, 0, \dots \quad \text{new!}$$

$$\Lambda_1(s(n)_{n \geq 0}) = s(3n + 1)_{n \geq 0} = 1, 2, 0, 2, 1, 0, 0, 0, 0, \dots = \Lambda_0(s(n)_{n \geq 0})$$

$$\Lambda_2(s(n)_{n \geq 0}) = s(3n + 2)_{n \geq 0} = 2, 0, 2, 1, 0, 0, 0, 0, 2, \dots$$

How to tell whether a sequence is p -automatic?

Let $r \in \{0, 1, \dots, p - 1\}$.

The **Cartier operator** Λ_r picks out every p th term, starting with $s(r)$:

$$\Lambda_r(s(n)_{n \geq 0}) := s(pn + r)_{n \geq 0}$$

Iteratively apply $\Lambda_0, \Lambda_1, \dots, \Lambda_{p-1}$ to $s(n)_{n \geq 0}$.

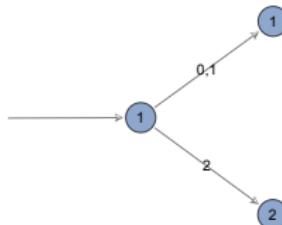
Create one state in the automaton for each distinct sequence.

Let $s(n) = (C(n) \bmod 3)$. $s(n)_{n \geq 0} = 1, 1, 2, 2, 2, 0, 0, 0, 2, \dots$

$$\Lambda_0(s(n)_{n \geq 0}) = s(3n + 0)_{n \geq 0} = 1, 2, 0, 2, 1, 0, 0, 0, 0, \dots \quad \text{new!}$$

$$\Lambda_1(s(n)_{n \geq 0}) = s(3n + 1)_{n \geq 0} = 1, 2, 0, 2, 1, 0, 0, 0, 0, \dots = \Lambda_0(s(n)_{n \geq 0})$$

$$\Lambda_2(s(n)_{n \geq 0}) = s(3n + 2)_{n \geq 0} = 2, 0, 2, 1, 0, 0, 0, 0, 2, \dots \quad \text{new!}$$



Label each state with the initial term of the corresponding sequence.

$$\Lambda_0(\Lambda_0(s(n)_{n \geq 0})) = 1, 2, 0, 2, 1, 0, 0, 0, 0, 2, \dots$$

$$\Lambda_0(\Lambda_0(s(n)_{n \geq 0})) = 1, 2, 0, 2, 1, 0, 0, 0, 0, 2, \dots = \Lambda_0(s(n)_{n \geq 0})$$

$$\Lambda_0(\Lambda_0(s(n)_{n \geq 0})) = 1, 2, 0, 2, 1, 0, 0, 0, 0, 2, \dots = \Lambda_0(s(n)_{n \geq 0})$$
$$\Lambda_1(\Lambda_0(s(n)_{n \geq 0})) = 2, 1, 0, 1, 2, 0, 0, 0, 0, 1, \dots \quad \text{new!}$$

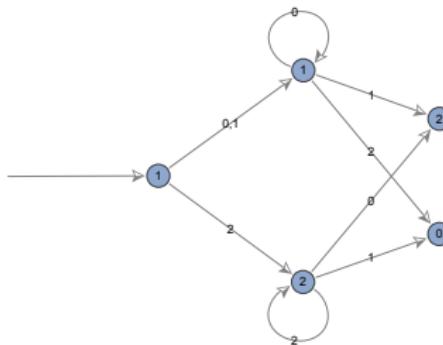
$$\begin{aligned}\Lambda_0(\Lambda_0(s(n)_{n \geq 0})) &= 1, 2, 0, 2, 1, 0, 0, 0, 0, 2, \dots = \Lambda_0(s(n)_{n \geq 0}) \\ \Lambda_1(\Lambda_0(s(n)_{n \geq 0})) &= 2, 1, 0, 1, 2, 0, 0, 0, 0, 1, \dots \quad \text{new!} \\ \Lambda_2(\Lambda_0(s(n)_{n \geq 0})) &= 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, \dots \quad \text{new!}\end{aligned}$$

$$\Lambda_0(\Lambda_0(s(n)_{n \geq 0})) = 1, 2, 0, 2, 1, 0, 0, 0, 0, 2, \dots = \Lambda_0(s(n)_{n \geq 0})$$

$$\Lambda_1(\Lambda_0(s(n)_{n \geq 0})) = 2, 1, 0, 1, 2, 0, 0, 0, 0, 1, \dots \quad \text{new!}$$

$$\Lambda_2(\Lambda_0(s(n)_{n \geq 0})) = 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, \dots \quad \text{new!}$$

$$\Lambda_r(\Lambda_2(s(n)_{n \geq 0})) \quad \dots$$

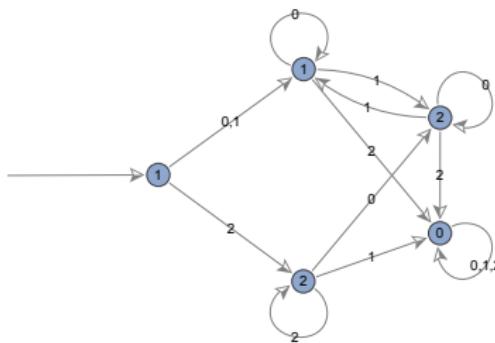


$$\Lambda_0(\Lambda_0(s(n)_{n \geq 0})) = 1, 2, 0, 2, 1, 0, 0, 0, 0, 2, \dots = \Lambda_0(s(n)_{n \geq 0})$$

$$\Lambda_1(\Lambda_0(s(n)_{n \geq 0})) = 2, 1, 0, 1, 2, 0, 0, 0, 0, 1, \dots \quad \text{new!}$$

$$\Lambda_2(\Lambda_0(s(n)_{n \geq 0})) = 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, \dots \quad \text{new!}$$

$$\Lambda_r(\Lambda_2(s(n)_{n \geq 0})) \dots$$



Eilenberg 1974:

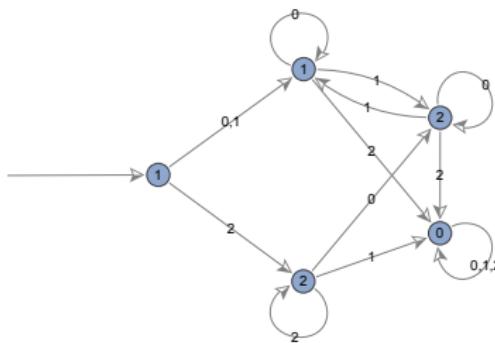
A sequence is p -automatic if and only if this process terminates.

$$\Lambda_0(\Lambda_0(s(n)_{n \geq 0})) = 1, 2, 0, 2, 1, 0, 0, 0, 0, 2, \dots = \Lambda_0(s(n)_{n \geq 0})$$

$$\Lambda_1(\Lambda_0(s(n)_{n \geq 0})) = 2, 1, 0, 1, 2, 0, 0, 0, 0, 1, \dots \quad \text{new!}$$

$$\Lambda_2(\Lambda_0(s(n)_{n \geq 0})) = 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, \dots \quad \text{new!}$$

$$\Lambda_r(\Lambda_2(s(n)_{n \geq 0})) \dots$$



Eilenberg 1974:

A sequence is p -automatic if and only if this process terminates.

But we can't tell if sequences are equal from finitely many terms!

Use a different representation: diagonals of rational functions.

$\sum_{n \geq 1} (C(n) \bmod 3)x^n$ is the **diagonal** of

$$\frac{y \frac{\partial P}{\partial y}(xy, y)}{P(xy, y)/y} = \frac{y(2xy^2 + (2xy + 2))}{xy^2 + (2xy + 2) + x} = \begin{aligned} & 0x^0y^0 + 1x^0y^1 + 0x^0y^2 + 0x^0y^3 + 0x^0y^4 + 0x^0y^5 + \dots \\ & + 0x^1y^0 + 1x^1y^1 + 0x^1y^2 + 2x^1y^3 + 0x^1y^4 + 0x^1y^5 + \dots \\ & + 0x^2y^0 + 1x^2y^1 + 2x^2y^2 + 0x^2y^3 + 1x^2y^4 + 2x^2y^5 + \dots \\ & + 0x^3y^0 + 1x^3y^1 + 1x^3y^2 + 2x^3y^3 + 0x^3y^4 + 1x^3y^5 + \dots \\ & + 0x^4y^0 + 1x^4y^1 + 0x^4y^2 + 2x^4y^3 + 2x^4y^4 + 0x^4y^5 + \dots \\ & + 0x^5y^0 + 1x^5y^1 + 2x^5y^2 + 0x^5y^3 + 0x^5y^4 + 0x^5y^5 + \dots \\ & + \dots . \end{aligned}$$

Theorem (Furstenberg 1967)

Let K be a field, and let $P(x, y) \in K[x, y]$ such that $\frac{\partial P}{\partial y}(0, 0) \neq 0$. If $F(x) \in K[\![x]\!]$ satisfies $F(0) = 0$ and $P(x, F(x)) = 0$, then

$$F(x) = \text{diag}\left(\frac{y \frac{\partial P}{\partial y}(xy, y)}{P(xy, y)/y}\right).$$

We have embedded $s(n)_{n \geq 1}$ into a series $\frac{S_0}{Q} := \frac{y(2xy^2 + (2xy+2))}{xy^2 + (2xy+2) + x}$.
Construct an automaton by iterating $\lambda_{r,r}(S) := \Lambda_{r,r}(S \cdot Q^{p-1})$.

We have embedded $s(n)_{n \geq 1}$ into a series $\frac{S_0}{Q} := \frac{y(2xy^2 + (2xy+2))}{xy^2 + (2xy+2) + x}$.
Construct an automaton by iterating $\lambda_{r,r}(S) := \Lambda_{r,r}(S \cdot Q^{p-1})$.

$$\lambda_{0,0}(S_0) = xy^2 + xy \quad \text{new!}$$

We have embedded $s(n)_{n \geq 1}$ into a series $\frac{S_0}{Q} := \frac{y(2xy^2 + (2xy+2))}{xy^2 + (2xy+2) + x}$.
Construct an automaton by iterating $\lambda_{r,r}(S) := \Lambda_{r,r}(S \cdot Q^{p-1})$.

$$\lambda_{0,0}(S_0) = xy^2 + xy \quad \text{new!}$$

$$\lambda_{1,1}(S_0) = 2 \quad \text{new!}$$

We have embedded $s(n)_{n \geq 1}$ into a series $\frac{S_0}{Q} := \frac{y(2xy^2 + (2xy+2))}{xy^2 + (2xy+2) + x}$.
Construct an automaton by iterating $\lambda_{r,r}(S) := \Lambda_{r,r}(S \cdot Q^{p-1})$.

$$\lambda_{0,0}(S_0) = xy^2 + xy \quad \text{new!}$$

$$\lambda_{1,1}(S_0) = 2 \quad \text{new!}$$

$$\lambda_{2,2}(S_0) = y + 1 \quad \text{new!}$$

We have embedded $s(n)_{n \geq 1}$ into a series $\frac{S_0}{Q} := \frac{y(2xy^2 + (2xy+2))}{xy^2 + (2xy+2) + x}$.
Construct an automaton by iterating $\lambda_{r,r}(S) := \Lambda_{r,r}(S \cdot Q^{p-1})$.

$$\lambda_{0,0}(S_0) = xy^2 + xy \quad \text{new!}$$

$$\lambda_{1,1}(S_0) = 2 \quad \text{new!}$$

$$\lambda_{2,2}(S_0) = y + 1 \quad \text{new!}$$

$$\lambda_{0,0}(xy^2 + xy) = xy^2 + xy = \lambda_{0,0}(S_0)$$

We have embedded $s(n)_{n \geq 1}$ into a series $\frac{S_0}{Q} := \frac{y(2xy^2 + (2xy+2))}{xy^2 + (2xy+2) + x}$.
 Construct an automaton by iterating $\lambda_{r,r}(S) := \Lambda_{r,r}(S \cdot Q^{p-1})$.

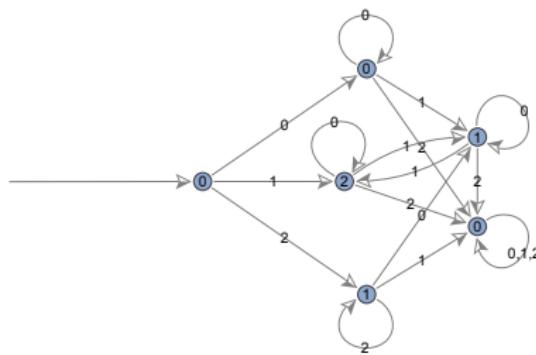
$$\lambda_{0,0}(S_0) = xy^2 + xy \quad \text{new!}$$

$$\lambda_{1,1}(S_0) = 2 \quad \text{new!}$$

$$\lambda_{2,2}(S_0) = y + 1 \quad \text{new!}$$

$$\lambda_{0,0}(xy^2 + xy) = xy^2 + xy = \lambda_{0,0}(S_0) \quad \dots$$

Create one state in the automaton for each distinct polynomial.



The automaton may not be minimal.

Prime power moduli

This algorithm can be adapted to work modulo p^α .

Theorem (Denef–Lipshitz 1987)

Let $\alpha \geq 1$. Let $R(\mathbf{x}), Q(\mathbf{x}) \in \mathbb{Z}_p[\mathbf{x}]$ such that $Q(0, \dots, 0) \not\equiv 0 \pmod{p}$.

Then the coefficient sequence of $\left(\text{diag } \frac{R(\mathbf{x})}{Q(\mathbf{x})} \right) \pmod{p^\alpha}$ is p -automatic.

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

Prime power moduli

This algorithm can be adapted to work modulo p^α .

Theorem (Denef–Lipshitz 1987)

Let $\alpha \geq 1$. Let $R(\mathbf{x}), Q(\mathbf{x}) \in \mathbb{Z}_p[\mathbf{x}]$ such that $Q(0, \dots, 0) \not\equiv 0 \pmod{p}$.

Then the coefficient sequence of $\left(\text{diag } \frac{R(\mathbf{x})}{Q(\mathbf{x})} \right) \pmod{p^\alpha}$ is p -automatic.

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

Ad in 3

Prime power moduli

This algorithm can be adapted to work modulo p^α .

Theorem (Denef–Lipshitz 1987)

Let $\alpha \geq 1$. Let $R(\mathbf{x}), Q(\mathbf{x}) \in \mathbb{Z}_p[\mathbf{x}]$ such that $Q(0, \dots, 0) \not\equiv 0 \pmod{p}$.

Then the coefficient sequence of $\left(\text{diag } \frac{R(\mathbf{x})}{Q(\mathbf{x})} \right) \pmod{p^\alpha}$ is p -automatic.

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

Ad in 2

Prime power moduli

This algorithm can be adapted to work modulo p^α .

Theorem (Denef–Lipshitz 1987)

Let $\alpha \geq 1$. Let $R(\mathbf{x}), Q(\mathbf{x}) \in \mathbb{Z}_p[\mathbf{x}]$ such that $Q(0, \dots, 0) \not\equiv 0 \pmod{p}$.

Then the coefficient sequence of $\left(\text{diag } \frac{R(\mathbf{x})}{Q(\mathbf{x})} \right) \pmod{p^\alpha}$ is p -automatic.

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

Ad in 1

youtube.com/EricRowland

The screenshot shows the YouTube channel page for Eric Rowland. At the top, there is a navigation bar with a menu icon, the YouTube logo, a search bar, a microphone icon, a three-dot menu, and a 'SIGN IN' button. Below the navigation bar is a decorative banner with a grid pattern of small video thumbnails. To the left of the main content area is a sidebar with icons for Home, Explore, Shorts, Subscriptions, Library, and History. The main content area features a profile picture of Eric Rowland, his name 'Eric Rowland', and '5.96K subscribers'. A red 'SUBSCRIBE' button is visible. Below this, a navigation menu has 'HOME' selected. The 'Uploads' section is shown, featuring a video thumbnail for 'p-adic numbers' with the title '1 Billion is Tiny in an Alternate Universe (Intro to p-adic Numbers) #SoME2', 346K views, and a timestamp of 21:53. A caption below the video describes p-adic numbers as bizarre alternative number systems useful in number theory.

Eric Rowland

5.96K subscribers

SUBSCRIBE

HOME VIDEOS PLAYLISTS COMMUNITY CHANNELS ABOUT

Uploads

p-adic numbers

1 Billion is Tiny in an Alternate Universe (Intro to p-adic Numbers)
#SoME2

346K views • 1 month ago

The p-adic numbers are bizarre alternative number systems that are extremely useful in number theory. They arise by changing our notion of what it means for a number to be large. As a real...

21:53 CC

youtube.com/EricRowland

The screenshot shows the YouTube channel page for Eric Rowland. At the top, there is a navigation bar with a menu icon, the YouTube logo, a search bar, a microphone icon, a three-dot menu, and a 'SIGN IN' button. Below the navigation bar is a decorative banner with a grid pattern of small video thumbnails. To the left of the main content area is a sidebar with icons for Home, Explore, Shorts, Subscriptions, Library, and History. The main content area features a circular profile picture of Eric Rowland, his name 'Eric Rowland', and '5.96K subscribers'. A red 'SUBSCRIBE' button is visible. Below this, a navigation menu has 'HOME' selected. The 'Uploads' section is shown, featuring a video thumbnail for 'p-adic numbers' with the title '1 Billion is Tiny in an Alternate Universe (Intro to p-adic Numbers) #SoME2', 346K views, and a timestamp of 21:53. A caption below the video describes p-adic numbers as bizarre alternative number systems useful in number theory. At the bottom right of the main content area is a 'Skip ad' button.

Skip ad ►

Prime power moduli

This algorithm can be adapted to work modulo p^α .

Theorem (Denef–Lipshitz 1987)

Let $\alpha \geq 1$. Let $R(\mathbf{x}), Q(\mathbf{x}) \in \mathbb{Z}_p[\mathbf{x}]$ such that $Q(0, \dots, 0) \not\equiv 0 \pmod{p}$.

Then the coefficient sequence of $\left(\text{diag } \frac{R(\mathbf{x})}{Q(\mathbf{x})} \right) \pmod{p^\alpha}$ is p -automatic.

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

Prime power moduli

This algorithm can be adapted to work modulo p^α .

Theorem (Denef–Lipshitz 1987)

Let $\alpha \geq 1$. Let $R(\mathbf{x}), Q(\mathbf{x}) \in \mathbb{Z}_p[\mathbf{x}]$ such that $Q(0, \dots, 0) \not\equiv 0 \pmod{p}$.

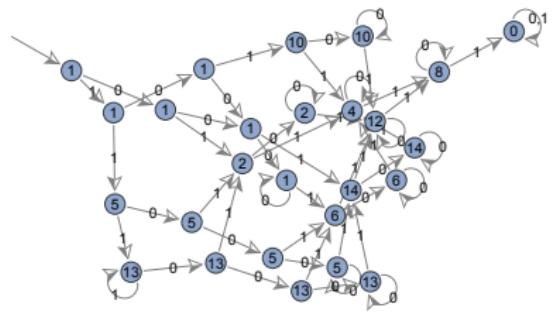
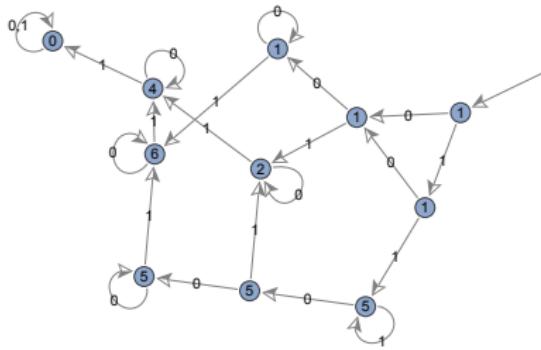
Then the coefficient sequence of $\left(\text{diag } \frac{R(\mathbf{x})}{Q(\mathbf{x})} \right) \pmod{p^\alpha}$ is p -automatic.

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

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

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

Catalan numbers modulo 8 and modulo 16:



Theorem (Liu–Yeh)

$C(n) \not\equiv 9 \pmod{16}$ for all $n \geq 0$.

Proof: Compute the automaton.

Catalan numbers modulo 2^α :

Theorem (Rowland–Yassawi 2015)

For all $n \geq 0$,

- $C(n) \not\equiv 17, 21, 26 \pmod{32}$,
- $C(n) \not\equiv 10, 13, 33, 37 \pmod{64}$,
- $C(n) \not\equiv 18, 54, 61, 65, 66, 69, 98, 106, 109 \pmod{128}$.

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

Open question

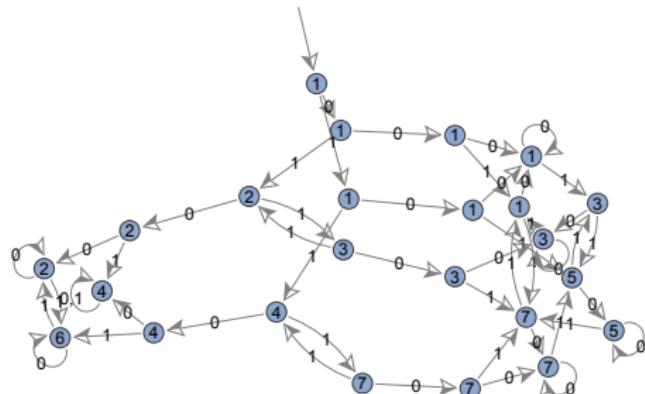
Does the density of residues modulo 2^α that are attained by some Catalan number tend to 0 as α gets large?

For the Motzkin numbers...

Theorem (Eu–Liu–Yeh; conj. by Deutsch–Sagan–Amdeberhan)

$M(n) \not\equiv 0 \pmod{8}$ for all $n \geq 0$.

Proof: $M(n) \pmod{8}$ is computed by the following automaton.

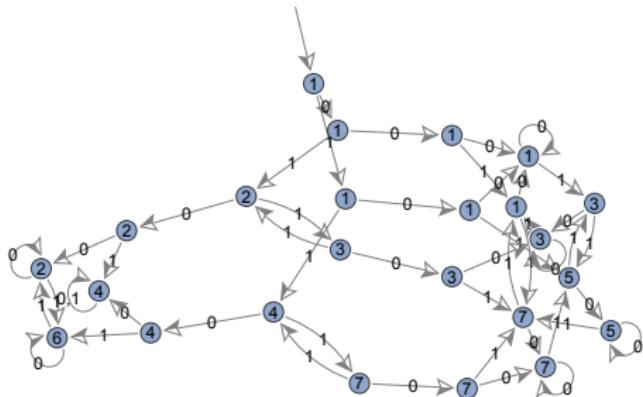


For the Motzkin numbers...

Theorem (Eu–Liu–Yeh; conj. by Deutsch–Sagan–Amdeberhan)

$M(n) \not\equiv 0 \pmod{8}$ for all $n \geq 0$.

Proof: $M(n) \pmod{8}$ is computed by the following automaton.



Theorem (Rowland–Yassawi)

$M(n) \not\equiv 0 \pmod{5^2}$ and $M(n) \not\equiv 0 \pmod{13^2}$ for all $n \geq 0$.

Apéry numbers

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

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

Apéry numbers

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

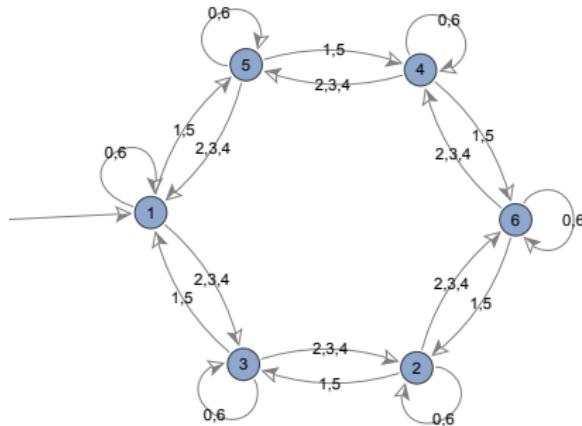
$$A(n)_{n \geq 0} = 1, 5, 73, 1445, 33001, 819005, 21460825, \dots$$

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

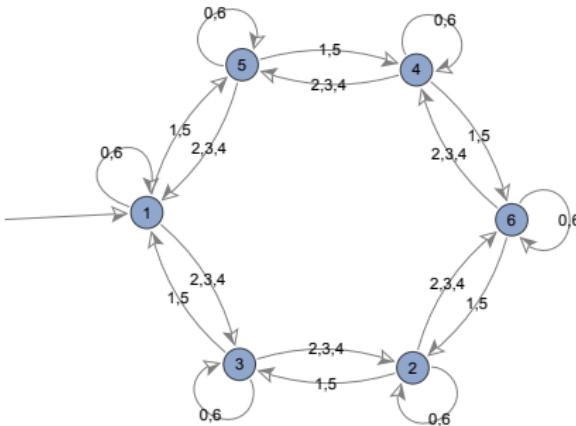
$$\frac{1}{(1-w-x)(1-y-z)-wxyz}.$$

Therefore $(A(n) \bmod p^\alpha)_{n \geq 0}$ is p -automatic.

$A(n)$ modulo 7: 1, 5, 3, 3, 3, 5, 1, 5, 4, 1, 1, ...



$A(n)$ modulo 7: 1, 5, 3, 3, 3, 5, 1, 5, 4, 1, 1, ...



Theorem (Gessel 1982)

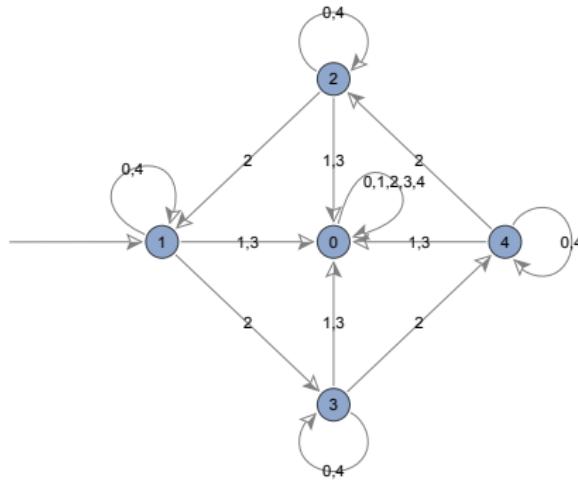
Let p be a prime. The Apéry numbers satisfy the *Lucas congruence*

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

for all $n \geq 0$ and all $d \in \{0, 1, \dots, p-1\}$.

$$A(2039) = A(5642_7) \equiv A(5)A(6)A(4)A(2) \equiv 5 \cdot 1 \cdot 3 \cdot 3 \equiv 3 \pmod{7}$$

$A(n)$ modulo 5: 1, 0, 3, 0, 1, 0, 0, 0, 0, 0, 3, ...



If the base-5 representation of n contains 1 or 3, then $A(n) \equiv 0 \pmod{5}$.

$A(n)$ modulo $2^\alpha \dots$

Gessel proved the conjecture of Chowla–Cowles–Cowles (1980) that

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

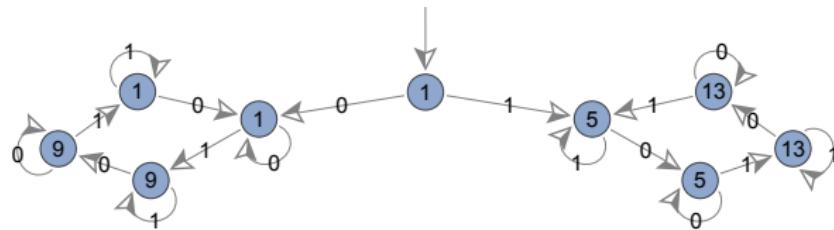
Gessel asked whether $A(n)$ is periodic modulo 16.

$A(n)$ modulo $2^\alpha \dots$

Gessel proved the conjecture of Chowla–Cowles–Cowles (1980) that

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

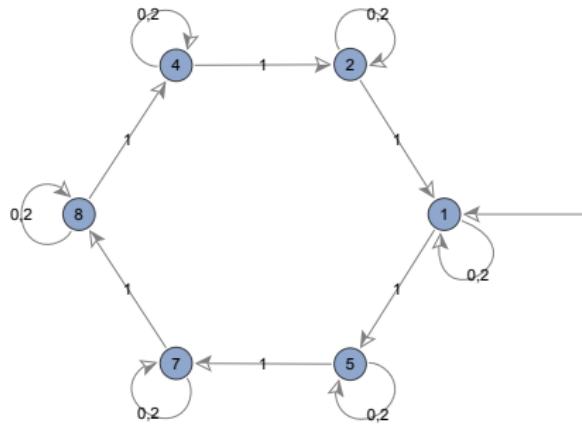
Gessel asked whether $A(n)$ is periodic modulo 16.



Theorem (Rowland–Yassawi)

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

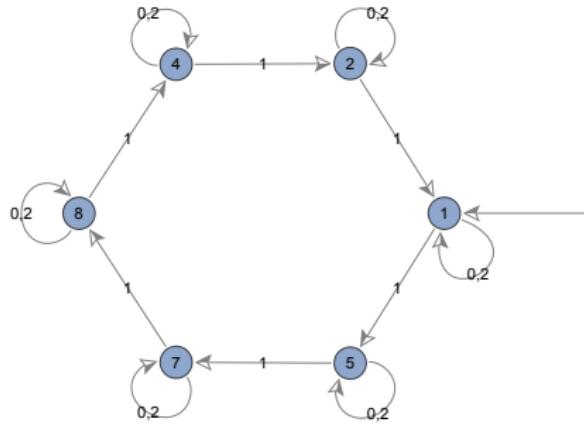
$A(n)$ modulo 9:



Theorem (Gessel)

$A(3n + d) \equiv A(n)A(d) \pmod{9}$ for all $n \geq 0$ and all $d \in \{0, 1, 2\}$.

$A(n)$ modulo 9:

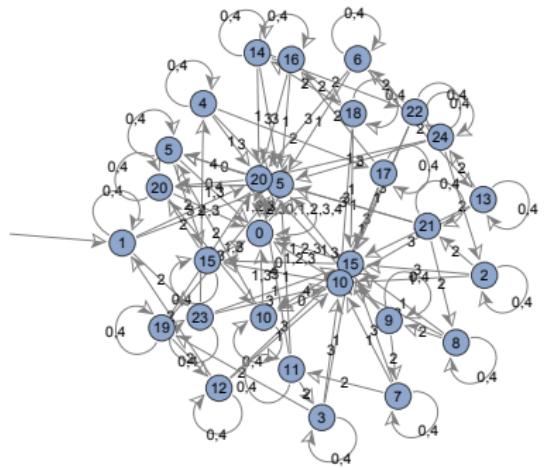


Theorem (Gessel)

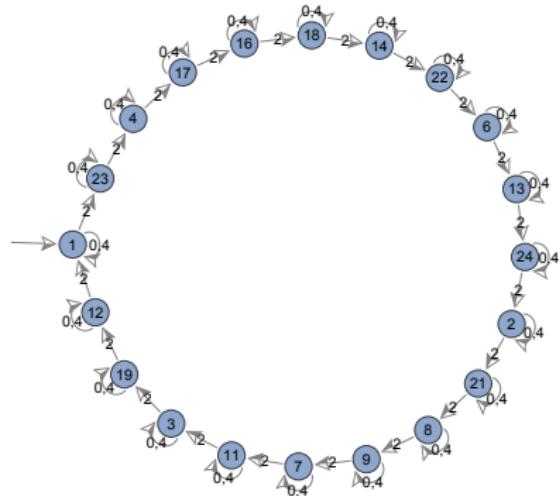
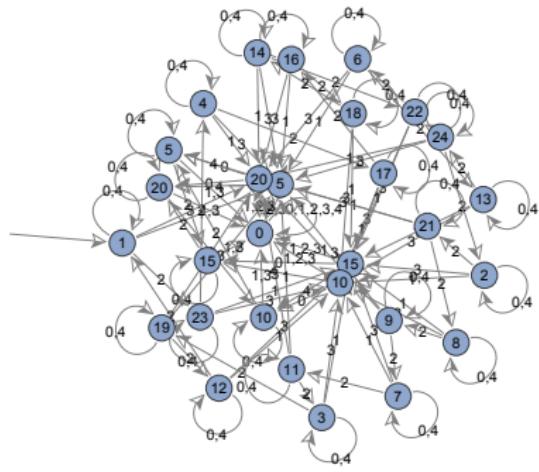
$$A(3n+d) \equiv A(n)A(d) \pmod{9} \text{ for all } n \geq 0 \text{ and all } d \in \{0, 1, 2\}.$$

For $p \geq 5$, the Lucas congruence does not always hold modulo p^2 .

$A(n)$ modulo 25:

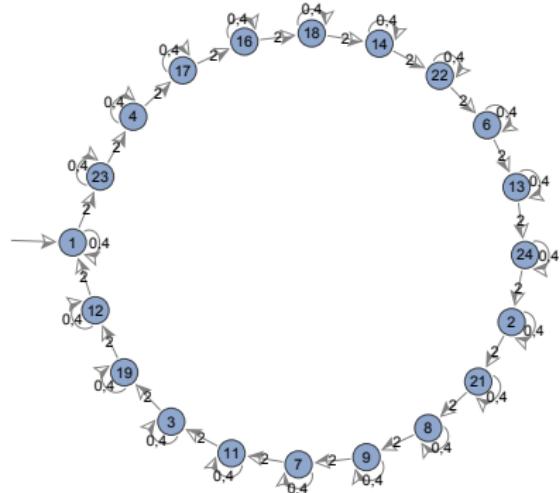
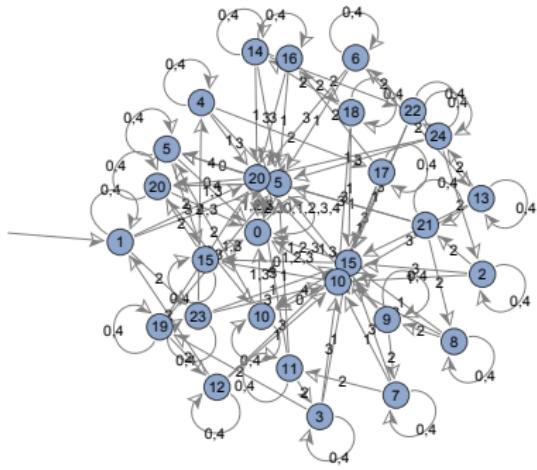


$A(n)$ modulo 25:



Restrict the digit set.

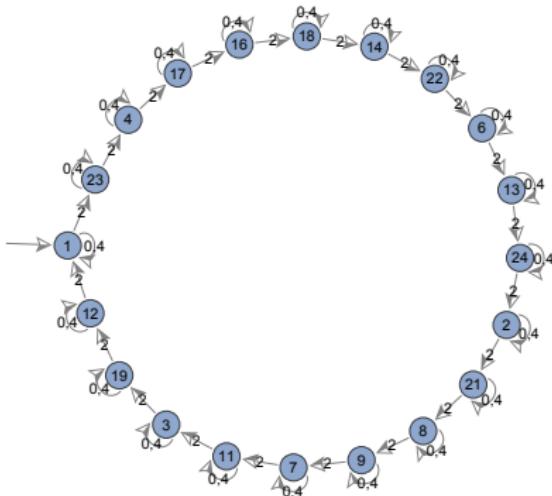
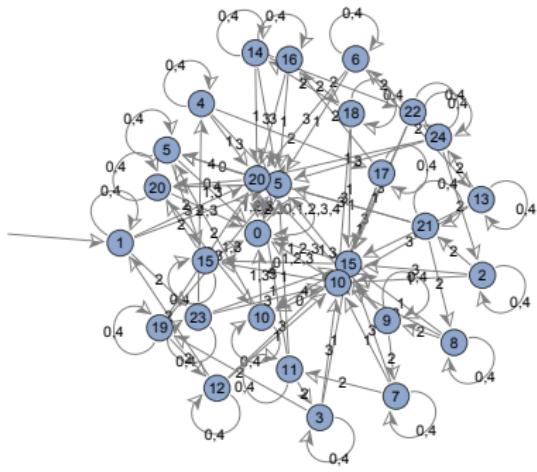
$A(n)$ modulo 25:



Restrict the digit set.

$$A(2) = 73 \equiv -2 \pmod{25}$$

$A(n)$ modulo 25:



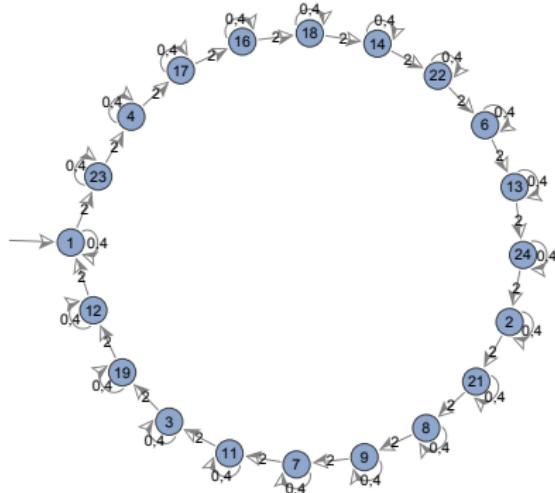
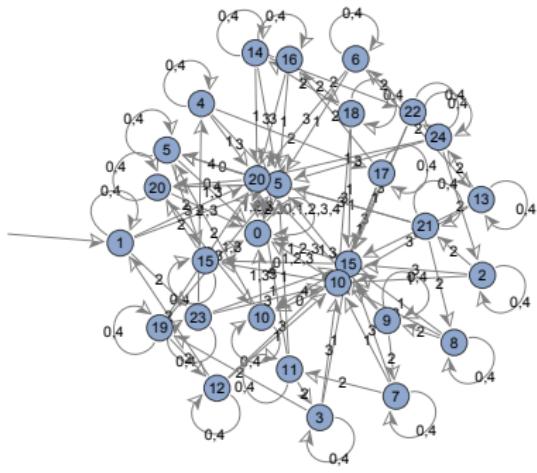
Restrict the digit set.

$$A(2) = 73 \equiv -2 \pmod{25}$$

Theorem (Rowland–Yassawi)

$$A(5n+d) \equiv A(n)A(d) \pmod{25} \text{ for all } n \geq 0 \text{ and all } d \in \{0, 2, 4\}.$$

$A(n)$ modulo 25:



Restrict the digit set.

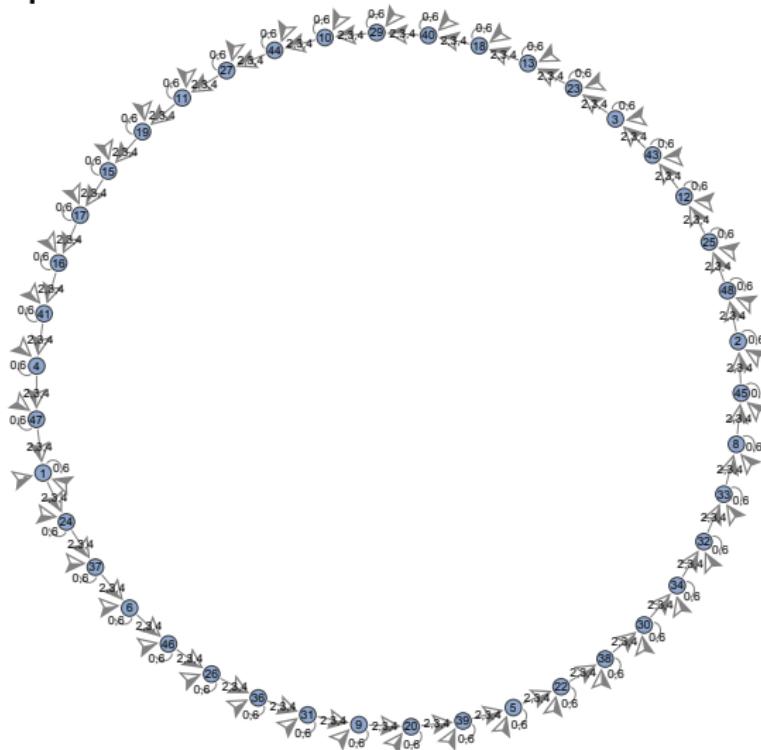
$$A(2) = 73 \equiv -2 \pmod{25}$$

Theorem (Rowland–Yassawi)

$$A(5n + d) \equiv A(n)A(d) \pmod{25} \text{ for all } n \geq 0 \text{ and all } d \in \{0, 2, 4\}.$$

Which digits support a Lucas congruence for $A(n)$ modulo p^2 ?

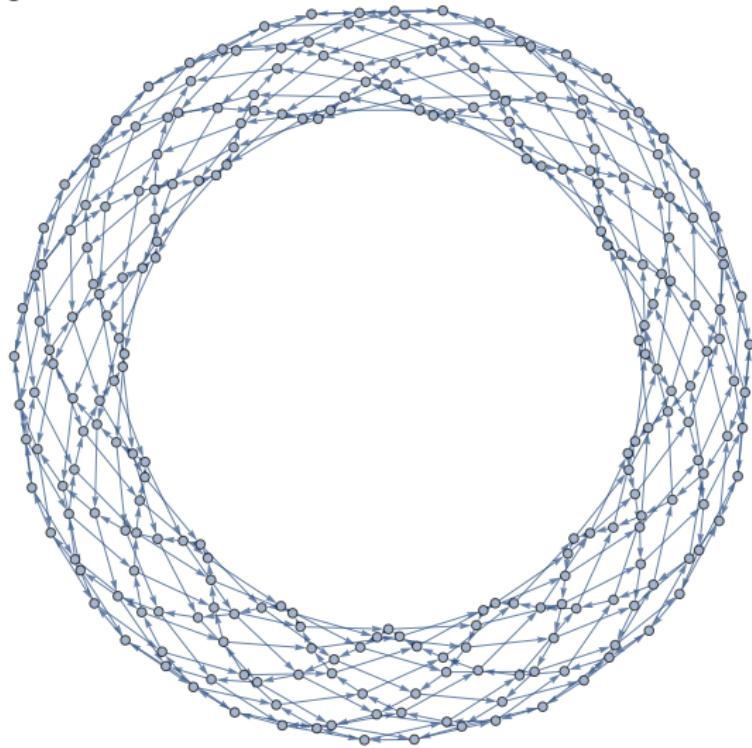
$A(n)$ modulo 7^2 :



digit set: $\{0, 2, 3, 4, 6\}$

$$(A(0), A(2), A(3), A(4), A(6)) \equiv (1, 24, 24, 24, 1) \pmod{7^2}$$

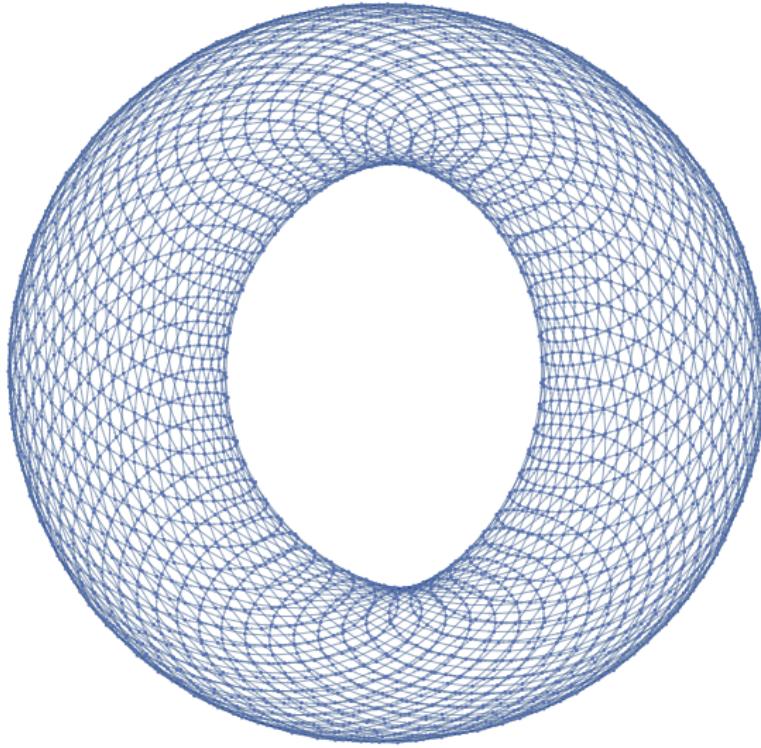
$A(n)$ modulo 23^2 :



digit set: $\{0, 7, 11, 15, 22\}$

$$(A(0), A(7), A(11), A(15), A(22)) \equiv (1, 415, 473, 415, 1) \pmod{23^2}$$

$A(n)$ modulo 59^2 :



digit set: $\{0, 6, 29, 52, 58\}$

$$(A(0), A(6), A(29), A(52), A(58)) \equiv (1, 460, 2813, 460, 1) \pmod{59^2}$$

Theorem (Malik–Straub 2016)

$A(d) \equiv A(p - 1 - d) \pmod{p}$ for each $d \in \{0, 1, \dots, p - 1\}$.

$$(A(0), A(1), \dots, A(10)) \equiv (1, 5, 7, 4, 1, 0, 1, 4, 7, 5, 1) \pmod{11}$$

Theorem (Malik–Straub 2016)

$A(d) \equiv A(p - 1 - d) \pmod{p}$ for each $d \in \{0, 1, \dots, p - 1\}$.

$$(A(0), A(1), \dots, A(10)) \equiv (1, 5, 7, 4, 1, 0, 1, 4, 7, 5, 1) \pmod{11}$$

Let $D(p) := \left\{ d \in \{0, 1, \dots, p - 1\} : A(d) \equiv A(p - 1 - d) \pmod{p^2} \right\}$.

In particular, $\{0, \frac{p-1}{2}, p-1\} \subseteq D(p)$. $\{0, 2, 4\} \subseteq D(5)$

Theorem (Rowland–Yassawi–Krattenthaler 2021)

Let p be a prime and $d \in \{0, 1, \dots, p - 1\}$. The congruence

$$A(pn + d) \equiv A(n)A(d) \pmod{p^2}$$

holds for all $n \geq 0$ if and only if $d \in D(p)$.

Primes p with $|D(p)| \geq 4$:

p	$D(p)$
7	{0, 2, 3, 4, 6}
23	{0, 7, 11, 15, 22}
43	{0, 5, 18, 21, 24, 37, 42}
59	{0, 6, 29, 52, 58}
79	{0, 18, 39, 60, 78}
103	{0, 17, 51, 85, 102}
107	{0, 14, 21, 47, 53, 59, 85, 92, 106}
127	{0, 17, 63, 109, 126}
131	{0, 62, 65, 68, 130}
139	{0, 68, 69, 70, 138}
151	{0, 19, 75, 131, 150}
167	{0, 35, 64, 83, 102, 131, 166}

Primes p with $|D(p)| \geq 4$:

p	$D(p)$
7	{0, 2, 3, 4, 6}
23	{0, 7, 11, 15, 22}
43	{0, 5, 18, 21, 24, 37, 42}
59	{0, 6, 29, 52, 58}
79	{0, 18, 39, 60, 78}
103	{0, 17, 51, 85, 102}
107	{0, 14, 21, 47, 53, 59, 85, 92, 106}
127	{0, 17, 63, 109, 126}
131	{0, 62, 65, 68, 130}
139	{0, 68, 69, 70, 138}
151	{0, 19, 75, 131, 150}
167	{0, 35, 64, 83, 102, 131, 166}

Heuristic probability that $|D(p)| \geq 4$:

$$1 - \left(1 - \frac{1}{p}\right)^{(p-3)/2}$$

Primes p with $|D(p)| \geq 4$:

p	$D(p)$
7	{0, 2, 3, 4, 6}
23	{0, 7, 11, 15, 22}
43	{0, 5, 18, 21, 24, 37, 42}
59	{0, 6, 29, 52, 58}
79	{0, 18, 39, 60, 78}
103	{0, 17, 51, 85, 102}
107	{0, 14, 21, 47, 53, 59, 85, 92, 106}
127	{0, 17, 63, 109, 126}
131	{0, 62, 65, 68, 130}
139	{0, 68, 69, 70, 138}
151	{0, 19, 75, 131, 150}
167	{0, 35, 64, 83, 102, 131, 166}

Heuristic probability that $|D(p)| \geq 4$:

$$1 - \left(1 - \frac{1}{p}\right)^{(p-3)/2} \rightarrow 1 - \frac{1}{\sqrt{e}} \approx .393$$

How does the size of the automaton (number of states) depend on the x -degree (**height**) and y -degree (**degree**) of the polynomial?

Theorem (Bridy 2017)

Let $s(n)_{n \geq 0}$ be an algebraic sequence of elements in \mathbb{F}_p .

If its minimal polynomial has height h , degree d , and genus g , then the number of states in its minimal automaton is at most

$$(1 + o(1))p^{h+d+g-1},$$

where $o(1)$ tends to 0 as any of p, h, d, g gets large.

The genus satisfies $g \leq (h - 1)(d - 1)$; generically $g = (h - 1)(d - 1)$.

Corollary

The number of states is at most $(1 + o(1))p^{hd}$.

How does the size of the automaton (number of states) depend on the x -degree (**height**) and y -degree (**degree**) of the polynomial?

Theorem (Bridy 2017)

Let $s(n)_{n \geq 0}$ be an algebraic sequence of elements in \mathbb{F}_p .

If its minimal polynomial has height h , degree d , and genus g , then the number of states in its minimal automaton is at most

$$(1 + o(1))p^{h+d+g-1},$$

where $o(1)$ tends to 0 as any of p, h, d, g gets large.

The genus satisfies $g \leq (h-1)(d-1)$; generically $g = (h-1)(d-1)$.

Corollary

The number of states is at most $(1 + o(1))p^{hd}$.

Can we get this bound without algebraic geometry?

How does the size of the automaton (number of states) depend on the x -degree (**height**) and y -degree (**degree**) of the polynomial?

Theorem (Bridy 2017)

Let $s(n)_{n \geq 0}$ be an algebraic sequence of elements in \mathbb{F}_p .

If its minimal polynomial has height h , degree d , and genus g , then the number of states in its minimal automaton is at most

$$(1 + o(1))p^{h+d+g-1},$$

where $o(1)$ tends to 0 as any of p, h, d, g gets large.

The genus satisfies $g \leq (h-1)(d-1)$; generically $g = (h-1)(d-1)$.

Corollary

The number of states is at most $(1 + o(1))p^{hd}$.

Can we get this bound without algebraic geometry? Yes.

How does the size of the automaton (number of states) depend on the x -degree (**height**) and y -degree (**degree**) of the polynomial?

Theorem (Bridy 2017)

Let $s(n)_{n \geq 0}$ be an algebraic sequence of elements in \mathbb{F}_p .

If its minimal polynomial has height h , degree d , and genus g , then the number of states in its minimal automaton is at most

$$(1 + o(1))p^{h+d+g-1},$$

where $o(1)$ tends to 0 as any of p, h, d, g gets large.

The genus satisfies $g \leq (h-1)(d-1)$; generically $g = (h-1)(d-1)$.

Corollary

The number of states is at most $(1 + o(1))p^{hd}$.

Can we get this bound without algebraic geometry? Yes.

Is the bound sharp?

How does the size of the automaton (number of states) depend on the x -degree (**height**) and y -degree (**degree**) of the polynomial?

Theorem (Bridy 2017)

Let $s(n)_{n \geq 0}$ be an algebraic sequence of elements in \mathbb{F}_p .

If its minimal polynomial has height h , degree d , and genus g , then the number of states in its minimal automaton is at most

$$(1 + o(1))p^{h+d+g-1},$$

where $o(1)$ tends to 0 as any of p, h, d, g gets large.

The genus satisfies $g \leq (h-1)(d-1)$; generically $g = (h-1)(d-1)$.

Corollary

The number of states is at most $(1 + o(1))p^{hd}$.

Can we get this bound without algebraic geometry? Yes.

Is the bound sharp? We suspect yes.

Corollary

The number of states is at most $(1 + o(1))p^{hd}$.

The factor $1 + o(1)$ cannot be removed.

Example

Let $p = 2$ and

$$P = (x^3 + x^2 + 1)y^3 + (x^3 + 1)y^2 + (x^3 + x^2 + x + 1)y + x^3 + x^2$$

with $h = 3$ and $d = 3$. The number of states is $532 > 512 = p^{hd}$.