Congruences for some sequences arising in combinatorics

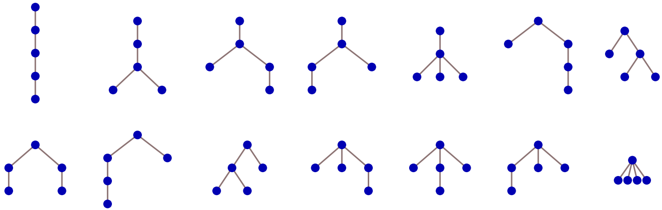
Eric Rowland
Hofstra University

Joint work with Reem Yassawi

Queen's University Mathematics and Statistics Colloquium
Online, 2021–09–24

What do combinatorial sequences look like modulo m?

How many plane trees have n edges?



$C(4) = 14$

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

Modulo 2: $1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, \ldots$

Theorem (follows from Kummer 1852)

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

Catalan numbers modulo 4: $1, 1, 2, 1, 2, 2, 0, 1, 2, 2, 0, 2, 0, 0, 0, 1, \dots$

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, $C(n) \not\equiv 3 \mod 4$.

Catalan numbers modulo 8: $1, 1, 2, 5, 6, 2, 4, 5, 6, 6, 4, 2, 4, 4, 0, 5, \dots$

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

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

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

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

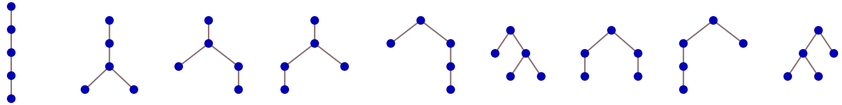
$$c_n \equiv_{16} \begin{cases} \left.\begin{matrix} 1 \\ 5 \\ 13 \end{matrix}\right\} & \textit{if} \quad d(\alpha) = 0 \textit{ and } \begin{cases} \beta \le 1, \\ \beta = 2, \\ \beta \ge 3, \end{cases} \\ \left.\begin{matrix} 2 \\ 10 \end{matrix}\right\} & \textit{if} \quad d(\alpha) = 1,\ \alpha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

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

They also determined $C(n)$ mod 64.

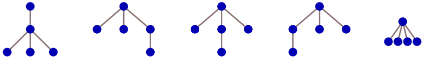
Can we obtain and prove such results automatically?
What is the right framework?

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



$M(4) = 9$

Excluded:



Motzkin numbers:

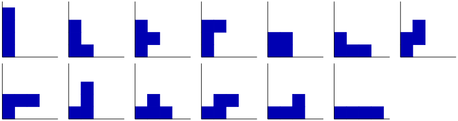
$M(n)_{n \geq 0} = 1, 1, 2, 4, 9, 21, 51, 127, \ldots$

Modulo 8: $1, 1, 2, 4, 1, 5, 3, 7, 3, 3, 4, 6, 7, 3, 2, 4, \ldots$

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

$M(n) \not\equiv 0 \mod 8$ *for all* $n \geq 0$.

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



$P(4) = 13$

Number of restricted hexagonal polyominoes:
$H(n)_{n\geq 0} = 1, 1, 3, 10, 36, 137, 543, 2219, \ldots$

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

Theorem (Deutsch–Sagan 2006)

There exists a set $C = \{1, 3, 4, 5, 7, \ldots\}$ 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 $n \in 2C - 1$.*

Algebraic sequences

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

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

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 $\mathbb{F}_3$.

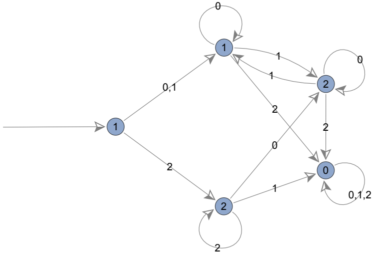
$\mathbb{F}_q$ denotes the finite field with q elements.

Automatic sequences

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

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

This automaton computes $C(n)$ mod 3:



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

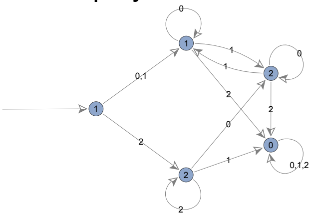
$(C(n) \bmod 3)_{n \geq 0} = 1, 1, 2, 2, 2, 0, 0, 0, 2, 2, \ldots$ is 3-automatic.

Theorem (Christol 1979/1980)

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

Two ways to represent such sequences: polynomials and automata.

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



How do we convert between them in a space-efficient way?

How to construct an automaton?

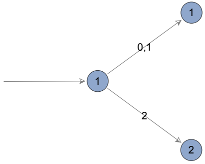
Let $r \in \{0, 1, \ldots, q-1\}$.
The Cartier operator Λ_r picks out every qth term, starting with $s(r)$:

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

Iteratively apply $\Lambda_0, \Lambda_1, \ldots, \Lambda_{q-1}$ to $s(n)_{n\geq 0}$.
Create one state in the automaton for each distinct sequence.

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

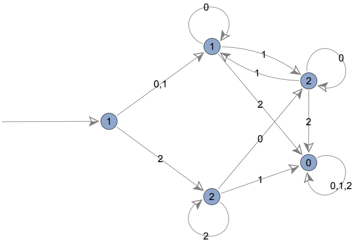
$$\begin{aligned}
\Lambda_0(s(n)_{n\geq 0}) &= s(3n+0)_{n\geq 0} = 1, 2, 0, 2, 1, 0, 0, 0, 0, \ldots && \text{new!} \\
\Lambda_1(s(n)_{n\geq 0}) &= s(3n+1)_{n\geq 0} = 1, 2, 0, 2, 1, 0, 0, 0, 0, \ldots && = \Lambda_0(s(n)_{n\geq 0}) \\
\Lambda_2(s(n)_{n\geq 0}) &= s(3n+2)_{n\geq 0} = 2, 0, 2, 1, 0, 0, 0, 0, 2, \ldots && \text{new!}
\end{aligned}$$



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

$$\Lambda_0(\Lambda_0(s(n)_{n\geq 0})) = 1,2,0,2,1,0,0,0,0,2,\ldots = \Lambda_0(s(n)_{n\geq 0})$$
$$\Lambda_1(\Lambda_0(s(n)_{n\geq 0})) = 2,1,0,1,2,0,0,0,0,1,\ldots \quad \text{new!}$$
$$\Lambda_2(\Lambda_0(s(n)_{n\geq 0})) = 0,0,0,0,0,0,0,0,0,0,\ldots \quad \text{new!}$$

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



A sequence is q-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

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

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

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

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 $\lambda_{r,r}(S) := \Lambda_{r,r}\left(S \cdot Q^{q-1}\right)$.

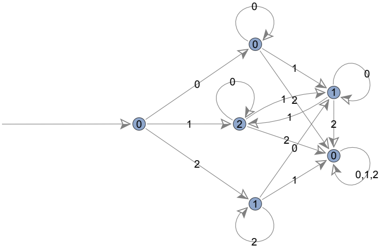
$\lambda_{0,0}(S_0) = xy^2 + xy$ new!

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

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

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

If two numerators are equal, the corresponding diagonals are equal.



The automaton may not be minimal.

Prime power moduli

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

Theorem (Denef–Lipshitz 1987)

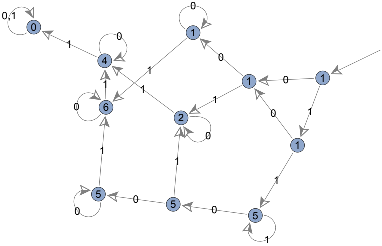
Let $\alpha \geq 1$. Let $R(\mathbf{x}), Q(\mathbf{x}) \in \mathbb{Z}_p[\mathbf{x}]$ such that $Q(0, \dots, 0) \not\equiv 0 \mod p$. Then the coefficient sequence of $\left(\operatorname{diag} \frac{R(\mathbf{x})}{Q(\mathbf{x})}\right) \bmod p^\alpha$ is p-automatic.

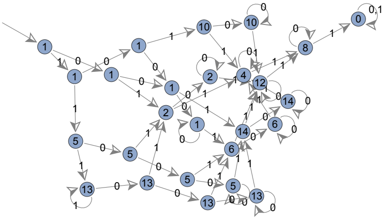
$\mathbb{Z}_p$ denotes the set of p-adic integers.

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

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

Catalan numbers modulo 8 and modulo 16:





Theorem (Liu–Yeh)

$C(n) \not\equiv 9 \mod 16$ for all $n \geq 0$.

Catalan numbers modulo 2^α:

Theorem (Rowland–Yassawi 2015)

For all $n \geq 0$*,*

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

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

Open question

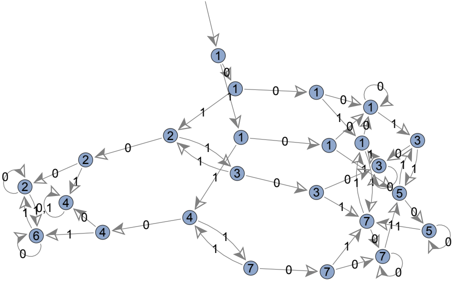
Does the density of residues modulo 2^α that are attained by some Catalan number tend to 0 as α gets large?

For the Motzkin numbers…

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

$M(n) \not\equiv 0 \mod 8$ *for all* $n \geq 0$.

Automated proof:



Theorem (Rowland–Yassawi)

$M(n) \not\equiv 0 \mod 5^2$ *and* $M(n) \not\equiv 0 \mod 13^2$ *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.

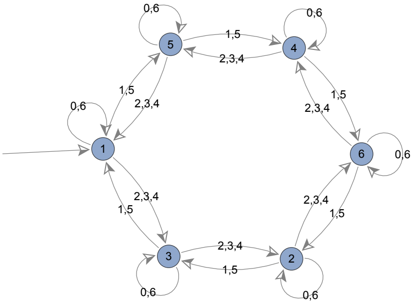
$A(n)_{n \geq 0} = 1, 5, 73, 1445, 33001, 819005, 21460825, \ldots$

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:



Theorem (Gessel 1982)

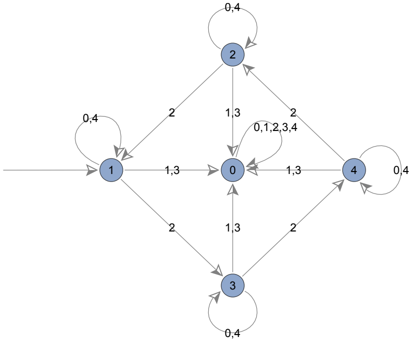
Let p be a prime. The Apéry numbers satisfy the Lucas congruence

$$A(pn + d) \equiv A(n)A(d) \mod p$$

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

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

$A(n)$ modulo 5:



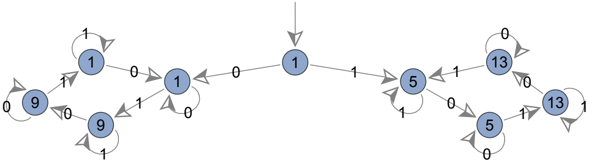
If the base-5 representation of n contains 1 or 3, then $A(n) \equiv 0 \mod 5$.

$A(n)$ modulo 2^α...

Gessel proved the conjecture of Chowla–Cowles–Cowles that

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

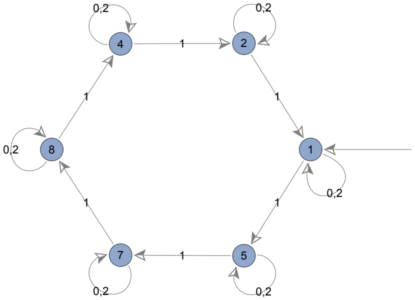
Gessel asked whether $A(n)$ is periodic modulo 16.



Theorem (Rowland–Yassawi)

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

$A(n)$ modulo 9:

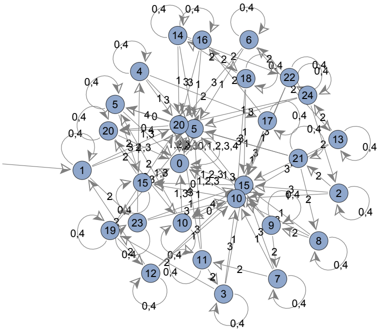


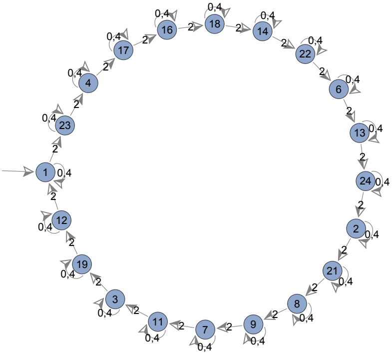
Theorem (Gessel)

$A(3n + d) \equiv A(n)A(d) \mod 9$ *for all* $n \geq 0$ *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:





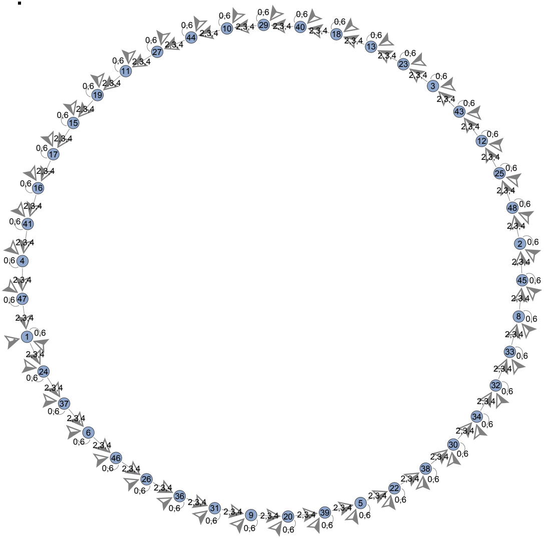
Restrict the digit set.

Theorem (Rowland–Yassawi)

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

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

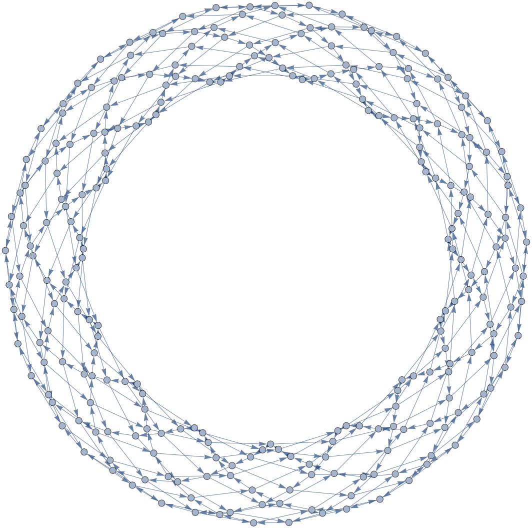
$A(n)$ modulo 7^2:



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

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

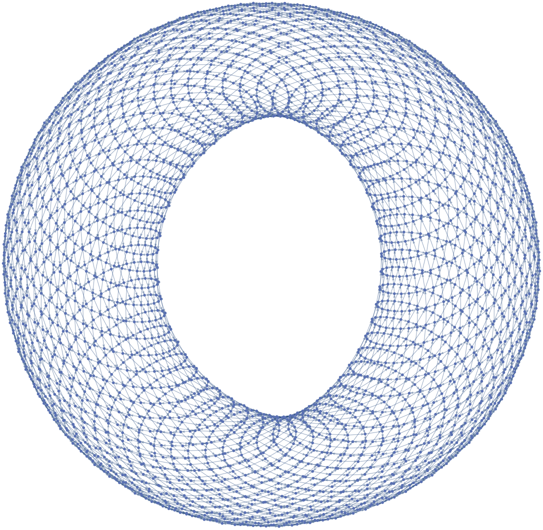
$A(n)$ modulo 23^2:



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

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

$A(n)$ modulo 59^2:



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

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

Theorem (Malik–Straub 2016)

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

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

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

Theorem (Rowland–Yassawi 2021)

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

$$A(pn+d) \equiv A(n)A(d) \mod p^2$$

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	$\{0, 35, 64, 83, 102, 131, 166\}$

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 $\mathbb{F}_q$.
If its minimal polynomial has height h, degree d, and genus g, then the number of states in its minimal automaton is at most

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

where $o(1)$ tends to 0 as any of q, 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 $(1 + o(1))q^{hd}$.

Can we get this bound without algebraic geometry? Yes.

Is the bound sharp? We suspect yes.

Corollary

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

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

Example

Let $q = 2$ 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 $532 > 512 = q^{hd}$.