Computing a finite automaton for an integer sequence modulo p^α

Eric Rowland

Joint work with Reem Yassawi and Doron Zeilberger

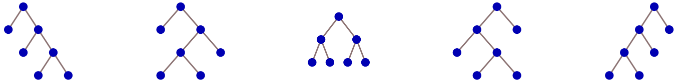
Hofstra University

2017 April 27

Catalan numbers modulo 2

What do integer sequences look like modulo p^α?

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

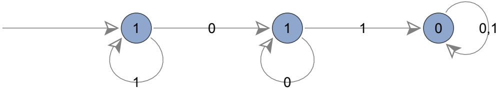


$C(3) = 5$

$(C(n) \bmod 2)_{n\geq 0} = 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, \ldots$

Theorem (follows from Kummer 1852)

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



Catalan numbers modulo 4 and 8

Theorem (Eu–Liu–Yeh 2008)

For all $n \geq 0$,

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

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*

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

Benefits

By computing an automaton for a sequence modulo p^α, we can...

- Compute the nth term modulo p^α quickly.
- Compute the forbidden residues modulo p^α.
- Compute the frequencies of the residues (if they exist).
- Decide whether the sequence of residues is eventually periodic.
- etc.

$C(n)_{n\geq 0}$ is algebraic:
$y = 1 + 1x + 2x^2 + 5x^3 + 14x^4 + 42x^5 + 132x^6 + \cdots$ satisfies

$$x\,y^2 - y + 1 = 0$$

in $\mathbb{Q}[\![x]\!]$.

What about $C(n)$ mod 2?

Benefits

By computing an automaton for a sequence modulo p^α, we can...

- Compute the nth term modulo p^α quickly.
- Compute the forbidden residues modulo p^α.
- Compute the frequencies of the residues (if they exist).
- Decide whether the sequence of residues is eventually periodic.
- etc.

$C(n)_{n\geq 0}$ is algebraic:
$y = 1 + 1x + 0x^2 + 1x^3 + \ \ 0x^4 + \ \ 0x^5 + \ \ \ \ 0x^6 + \cdots$ satisfies

$$x\,y^2 + y + 1 = 0$$

in $\mathbb{F}_2[\![x]\!]$.
What about $C(n)$ mod 2? Also algebraic. $\overset{\text{Christol}}{\Longrightarrow}$ 2-automatic.

An algebraic sequence, reduced modulo p, is p-automatic.

Sequences modulo p^α

Prime powers?

The proof of Christol's theorem depends on $(a+b)^p = a^p + b^p$.

The diagonal of a formal power series (in two variables) is

$$\mathcal{D}\left(\sum_{n,m\geq 0} a_{n,m} x^n y^m\right) := \sum_{n\geq 0} a_{n,n} x^n.$$

Theorem (Denef–Lipshitz 1987)

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

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

Algebraic sequences are diagonals of rational power series.

Algebraic $\to$ diagonal

Theorem (Furstenberg 1967)

Let $f(x) \in \mathbb{Q}[\![x]\!]$ and $P(x,y) \in \mathbb{Q}[x,y]$ such that $P(x, f(x)) = 0$. If $f(0) = 0$ and $\frac{\partial P}{\partial y}(0,0) \neq 0$, then

$$f(x) = \mathcal{D}\left(\frac{y\frac{\partial P}{\partial y}(xy,y)}{\frac{1}{y}P(xy,y)}\right).$$

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

$y = 0 + \sum_{n\geq 1} C(n)x^n$ satisfies $P(x,y) = 0$, where

$$P(x,y) := x(y+1)^2 - (y+1) + 1 \qquad \frac{\partial P}{\partial y}(x,y) = 2x(y+1) - 1$$
$$P(xy,y) = xy^3 + 2xy^2 + xy - y \qquad \frac{\partial P}{\partial y}(xy,y) = 2xy(y+1) - 1$$

Check: $\frac{\partial P}{\partial y}(0,0) = -1 \neq 0$.

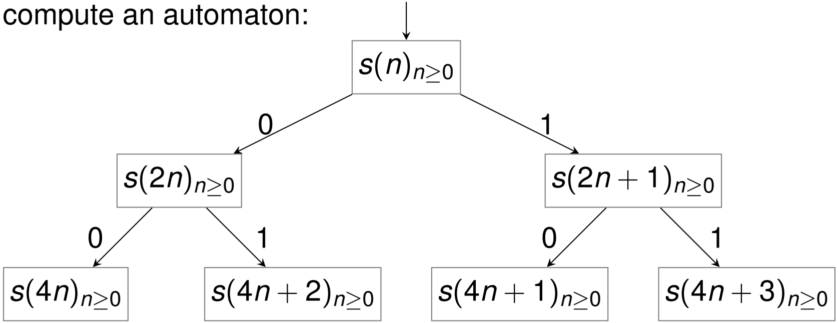
$$\boxed{\sum_{n\geq 1} C(n)x^n = \mathcal{D}\left(\frac{y(2xy^2+2xy-1)}{xy^2+2xy+x-1}\right)}$$

States are kernel sequences

Sure enough:

$$1 + \frac{y(2xy^2 + 2xy - 1)}{xy^2 + 2xy + x - 1} = \begin{array}{l} 1x^0y^0 + 1x^0y + 0x^0y^2 + 0x^0y^3 + 0x^0y^4 + \cdots \\ + 0x^1y^0 + 1x^1y + 0x^1y^2 - 1x^1y^3 + 0x^1y^4 + \cdots \\ + 0x^2y^0 + 1x^2y + 2x^2y^2 + 0x^2y^3 - 2x^2y^4 + \cdots \\ + 0x^3y^0 + 1x^3y + 4x^3y^2 + 5x^3y^3 + 0x^3y^4 + \cdots \\ + 0x^4y^0 + 1x^4y + 6x^4y^2 + 14x^4y^3 + 14x^4y^4 + \cdots \\ + \cdots \end{array}$$

To compute an automaton:



Cartier operator

Let $0 \leq d \leq p-1$. The Cartier operator on $\mathbb{Z}_p[\![x,y]\!]$ is defined by

$$\Lambda_d \left(\sum_{n,m \geq 0} a_{n,m} x^n y^m \right) := \sum_{n,m \geq 0} a_{pn+d,pm+d} x^n y^m.$$

Proposition

$$\Lambda_d \left(\frac{R(\mathbf{x})}{Q(\mathbf{x})^{p^\alpha}} \right) \equiv \frac{\Lambda_d(R(\mathbf{x}))}{Q(\mathbf{x})^{p^{\alpha-1}}} \mod p^\alpha.$$

For $C(n)$ mod 2…

$$1 + \frac{y(2xy^2+2xy-1)}{xy^2+2xy+x-1} \equiv \frac{xy^2+x+y+1}{xy^2+x+1} \mod 2$$
$$= \frac{xy^2+x+y+1}{xy^2+x+1} \cdot \frac{(xy^2+x+1)^1}{(xy^2+x+1)^1} \equiv \frac{x^2y^4+x^2+xy^3+xy+y+1}{(xy^2+x+1)^2}$$

Apply Λ_0, Λ_1:

$$\frac{xy^2+x+1}{xy^2+x+1} \qquad \frac{y+1}{xy^2+x+1}$$

We can simply work with the numerators.

Computation

Initial "state" (numerator):

$$xy^2 + x + y + 1$$

Images under $s(x, y) \mapsto \Lambda_d(s(x, y) \cdot Q(x, y)) \bmod 2$:

$$xy^2 + x + 1 \qquad\qquad y + 1$$

Two new states.

Images of $xy^2 + x + 1$:

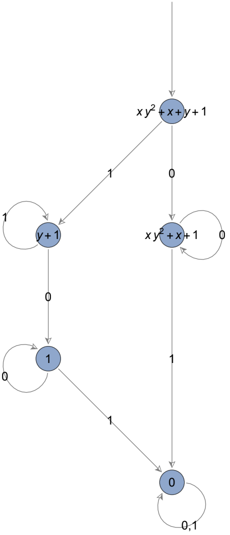
$$xy^2 + x + 1 \qquad\qquad 0$$

Images of $y + 1$:

$$1 \qquad\qquad y + 1$$

Two new states, so keep going...

But there are only finitely many possible states.



Algorithm

Given a power series satisfying $P(x, y) = 0$, compute $\frac{R(\mathbf{x})}{Q(\mathbf{x})} = \frac{y \frac{\partial P}{\partial y}(xy, y)}{\frac{1}{y} P(xy, y)}$.

Compute an automaton for the coefficients of $\mathcal{D}\left(\frac{R(\mathbf{x})}{Q(\mathbf{x})}\right)$ mod p^α:

1. Start with initial state $R(\mathbf{x}) \cdot Q(\mathbf{x})^{p^{\alpha-1}-1} \in (\mathbb{Z}/(p^\alpha\mathbb{Z}))[\mathbf{x}]$.
2. For each new state $s(\mathbf{x})$ and each $d \in \{0, \ldots, p-1\}$, draw the edge

$$s(\mathbf{x}) \xrightarrow{d} \Lambda_d \left(s(\mathbf{x}) \cdot Q(\mathbf{x})^{p^\alpha - p^{\alpha-1}} \right).$$

3. Iterate, and stop when all images have been computed.
4. Assign the output of each state $s(\mathbf{x})$ to be $s(0, \ldots, 0)$.

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

$$\frac{1}{(1 - x_1 - x_2)(1 - x_3 - x_4) - x_1 x_2 x_3 x_4}.$$

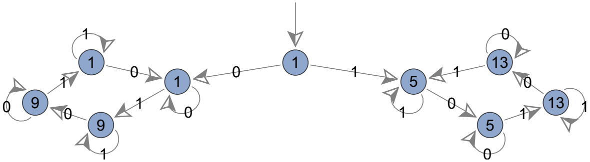
Therefore $(A(n) \bmod p^\alpha)_{n \geq 0}$ is p-automatic.

Apéry numbers modulo 16

Gessel (1982) 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.



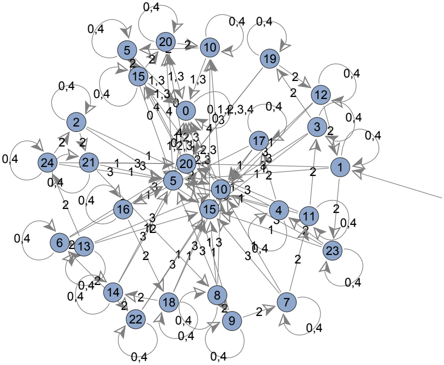
Theorem

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

Apéry numbers modulo 25

Theorem (special case of a conjecture of Beukers 1995)

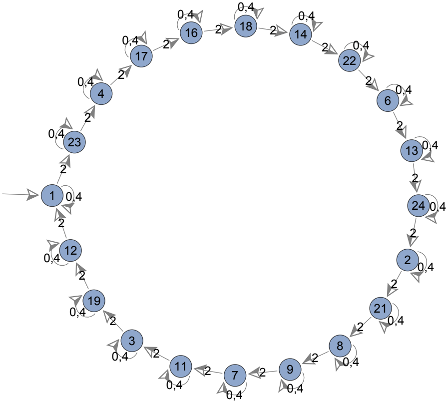
If there are at least two 1*s and* 3*s in the base-*5 *representation of* n*, then* $A(n) \equiv 0 \mod 5^2$.



Apéry numbers modulo 25

Theorem

Let $|n|_d$ be the number of d's in the base-5 representation of n.
If $|n|_1 = |n|_3 = 0$, then $A(n) \equiv A(2)^{|n|_2} \mod 25$.



Why is 25 special?

Constant terms of Laurent polynomials

$C(n)$ is the coefficient of x^0 in $(1-x)\left(\frac{1}{x}+2+x\right)^n$:

n	$(1-x)\left(\frac{1}{x}+2+x\right)^n$
0	$1 - x$
1	$\frac{1}{x} + 1 - x - x^2$
2	$\frac{1}{x^2} + \frac{3}{x} + 2 - 2x - 3x^2 - x^3$
3	$\frac{1}{x^3} + \frac{5}{x^2} + \frac{9}{x} + 5 - 5x - 9x^2 - 5x^3 - x^4$

Other kernel sequences…

$$\begin{aligned} C(2n) \bmod 2 &= [x^0]\left((1+x)\left(\tfrac{1}{x}+x\right)^{2n}\right) \\ &= [x^0]\left((1+x)\left(\frac{1}{x^2}+x^2\right)^{n}\right) \\ &= [x^0]\left(1\cdot\left(\frac{1}{x^2}+x^2\right)^{n}\right) \\ &= [x^0]\left(\tfrac{1}{x}+x\right)^{n} \end{aligned}$$

Constant terms of Laurent polynomials

A kernel sequence is represented by a pair of polynomials.
Again there are only finitely many:

$$
\begin{aligned}
C(n) \bmod 2 &= [x^0]\left((1+x)\left(\tfrac{1}{x}+x\right)^n\right) \\
C(2n) \bmod 2 &= [x^0]\left(\tfrac{1}{x}+x\right)^n \\
C(2n+1) \bmod 2 &= C(n) \bmod 2 \\
C(4n) \bmod 2 &= C(2n) \bmod 2 \\
C(4n+2) \bmod 2 &= 0
\end{aligned}
$$