Automatic sequences and p-adic asymptotics

Eric Rowland
Hofstra University

SIAM Conference on Discrete Mathematics
Open problems in combinatorics on words
University of Colorado, Denver, 2018–6–7

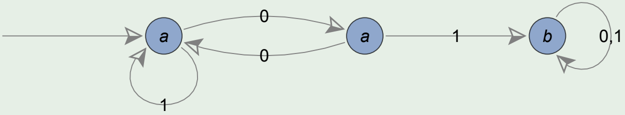
Automatic sequences

Let $p \geq 2$.

A sequence $s(n)_{n \geq 0}$ is p-automatic if there exists an automaton which outputs $s(n)$ when fed the base-p digits of n (least significant digit first).

Example

Let $p = 2$.

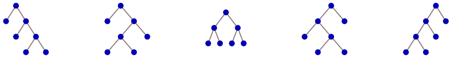


n	0	1	2	3	4	5	6	7	$\cdots$
$s(n)$	a	a	b	a	a	b	b	a	$\cdots$

Algebraic characterization

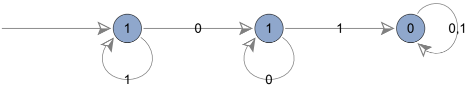
Christol's theorem

Let $s(n)_{n\geq 0}$ be a sequence of elements in $\mathbb{F}_p$. Then $s(n)_{n\geq 0}$ is p-automatic if and only if $\sum_{n\geq 0} s(n)x^n$ is algebraic over $\mathbb{F}_p(x)$.



$y = 1 + 1x + 2x^2 + 5x^3 + 14x^4 + 42x^5 + 132x^6 + \cdots$ satisfies
$xy^2 - y + 1 = 0$ in $\mathbb{Q}[\![x]\!]$.

The proof is constructive.



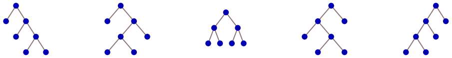
Corollary:
An algebraic sequence of integers, reduced modulo p, is p-automatic.

modulo p^α?

Algebraic characterization

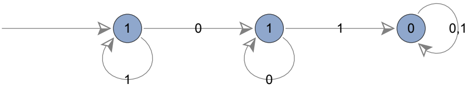
Christol's theorem

Let $s(n)_{n\geq 0}$ be a sequence of elements in $\mathbb{F}_p$. Then $s(n)_{n\geq 0}$ is p-automatic if and only if $\sum_{n\geq 0} s(n)x^n$ is algebraic over $\mathbb{F}_p(x)$.



$y = 1 + 1x + 0x^2 + 1x^3 + \ 0x^4 + \ 0x^5 + \quad 0x^6 + \cdots$ satisfies $xy^2 + y + 1 = 0$ in $\mathbb{F}_2[\![x]\!]$.

The proof is constructive.



Corollary:
An algebraic sequence of integers, reduced modulo p, is p-automatic.

modulo p^α?

Catalan numbers modulo 4 and 8

Theorem (Eu–Liu–Yeh 2008)

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

In particular, $C(n) \not\equiv 3 \mod 4$ for all $n \geq 0$.

Theorem (Eu–Liu–Yeh 2008)

$$C(n) \bmod 8 = \begin{cases} 1 & \text{if } n = 0 \text{ or } n = 1 \\ 2 & \text{if } n = 2^{a+1} + 2^a - 1 \text{ for some } a \geq 0 \\ 4 & \text{if } n = 2^c + 2^b + 2^a - 1 \text{ for some } c > b > a \geq 0 \\ 5 & \text{if } n = 2^a - 1 \text{ for some } a \geq 2 \\ 6 & \text{if } n = 2^b + 2^a - 1 \text{ for some } b - 2 \geq a \geq 0 \\ 0 & \text{otherwise.} \end{cases}$$

These are 2-automatic sequences.

Diagonals of rational power series

Theorem (Denef–Lipshitz 1987)

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

Furstenberg 1967:
Algebraic sequences can be realized as diagonals of rational functions.

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.

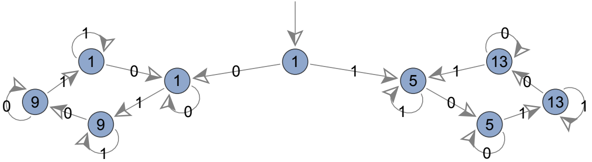
Apéry numbers

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

Gessel 1982: $A(n) \bmod 8 = \begin{cases} 1 & \text{if } n \text{ is even} \\ 5 & \text{if } n \text{ is odd.} \end{cases}$

Is $A(n)$ periodic modulo 16?

$A(n)$ is the nth diagonal coefficient of $\frac{1}{(1-x_1-x_2)(1-x_3-x_4)-x_1x_2x_3x_4}$.



Theorem (Rowland–Yassawi 2015)

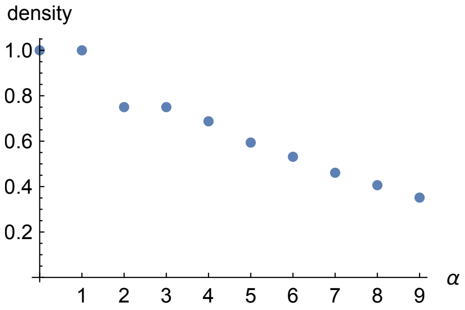
The sequence $(A(n) \bmod 16)_{n\geq 0}$ is not eventually periodic.

Catalan numbers modulo 2^α

Theorem

For all $n \geq 0$,

- $C(n) \not\equiv 3 \mod 4$,
- $C(n) \not\equiv 9 \mod 16$ *(in addition to $C(n) \not\equiv 3, 7, 11, 15 \mod 16$)*,
- $C(n) \not\equiv 17, 21, 26 \mod 32$,
- $C(n) \not\equiv 10, 13, 33, 37 \mod 64$.



What is the limiting density

$$\lim_{\alpha \to \infty} \frac{|\{C(n) \bmod 2^\alpha : n \geq 0\}|}{2^\alpha}?$$

2-adic numbers

We'd like to work modulo 2^α for all α simultaneously.

Modulo 2:

$$0 + O(2^1)$$
$$1 + O(2^1)$$

Modulo 2^2:

$$0 + 0 \cdot 2^1 + O(2^2)$$
$$1 + 0 \cdot 2^1 + O(2^2)$$
$$0 + 1 \cdot 2^1 + O(2^2)$$
$$1 + 1 \cdot 2^1 + O(2^2)$$

Letting $\alpha \to \infty$ gives expressions of the form

$$d_0 + d_1 2^1 + d_2 2^2 + d_3 2^3 + \cdots$$

where each $d_i \in \{0, 1\}$. The set of 2-adic integers is denoted $\mathbb{Z}_2$.

The 2-adic absolute value $|\cdot|_2$ is defined by $|0|_2 := 0$ and $|\frac{a}{b}2^n|_2 := \frac{1}{2^n}$ for odd a, b and $n \in \mathbb{Z}$.

p-adic asymptotics

Suppose $s(n)_{n \geq 0}$ is the diagonal of a rational function.
Then $(s(n) \bmod p^\alpha)_{n \geq 0}$ is p-automatic.

Open question

What is the limiting density $\displaystyle\lim_{\alpha \to \infty} \frac{|\{s(n) \bmod p^\alpha : n \geq 0\}|}{p^\alpha}$*?*

In $\mathbb{Z}_p$, this limit is $\mu(\overline{\{s(n) : n \geq 0\}})$,
where μ is the Haar measure on $\mathbb{Z}_p$ defined by $\mu(p^\alpha \mathbb{Z}_p) = \frac{1}{p^\alpha}$.

Open questions

For which subsequences does $\displaystyle\lim_{i \to \infty} s(n_i)$ *exist?*
What is the limit?
How fast is the convergence, etc.?

$F(3^n)$ in $\mathbb{Z}_3$

Let $F(n)_{n\geq 0} = 0, 1, 1, 2, 3, 5, 8, 13, \ldots$ be the Fibonacci sequence.

$$\begin{aligned}
F(3^0) &= 1 = 1_3 \\
F(3^1) &= 2 = 2_3 \\
F(3^2) &= 34 = 1021_3 \\
F(3^3) &= 196418 = 100222102202_3 \\
F(3^4) &= 37889062373143906 = 202\cdots 222001000102120000 21_3
\end{aligned}$$

$F(3^n)_{n\geq 0}$ appears to have two limit points in $\mathbb{Z}_3$.
They are $\pm\sqrt{\frac{2}{5}} \in \mathbb{Z}_3$.

Two convergent subsequences

Values of $F(3^{2n})$:

Values of $F(3^{2n+1})$:

Subtract the limits

Values of $F(3^{2n}) - \lim_{m\to\infty} F(3^{2m})$:

Values of $F(3^{2n+1}) - \lim_{m\to\infty} F(3^{2m+1})$:

Divide by 3^n

Values of $\frac{F(3^{2n}) - \lim_{m\to\infty} F(3^{2m})}{3^{2n}}$:

Values of $\frac{F(3^{2n+1}) - \lim_{m\to\infty} F(3^{2m+1})}{3^{2n+1}}$:

These pictures suggest two 3-adic power series:
If $x = 3^{2n}$, then

$$F(x) = c_0 + c_1 x + c_2 x^2 + \cdots .$$

If $x = 3^{2n+1}$, then

$$F(x) = d_0 + d_1 x + d_2 x^2 + \cdots .$$

Binet formula in $\mathbb{Z}_3$

Let $\phi = \frac{1+\sqrt{5}}{2}$ and $\bar{\phi} = \frac{1-\sqrt{5}}{2}$ in $\mathbb{Q}_3(\sqrt{5})$.
Let $\omega(\phi), \omega(\bar{\phi}) \in \mathbb{Q}_3(\sqrt{5})$ be 8th roots of unity congruent to $\phi, \bar{\phi}$ mod 3.

Theorem (Rowland–Yassawi 2016)

For each $0 \le i \le 7$, *define* $F_i : \mathbb{Z}_3 \to \mathbb{Z}_3$ *by*

$$F_i(x) := \frac{\omega(\phi)^i \exp_3\left(x \log_3 \frac{\phi}{\omega(\phi)}\right) - \omega(\bar{\phi})^i \exp_3\left(x \log_3 \frac{\bar{\phi}}{\omega(\bar{\phi})}\right)}{\sqrt{5}}.$$

Then $F(n) = F_i(n)$ *for all* $n \equiv i \mod 8$.

Since $3^{2n} \equiv 1 \mod 8$,

$$\lim_{n\to\infty} F(3^{2n}) = \lim_{n\to\infty} F_1(3^{2n}) = F_1(0) = \frac{\omega(\phi) - \omega(\bar{\phi})}{\sqrt{5}} = \left(\frac{2}{5}\right)^{1/2}.$$

Limiting density

What is the limiting density

$$\lim_{\alpha\to\infty} \frac{|\{F(n) \bmod p^\alpha : n \geq 0\}|}{p^\alpha}?$$

Burr 1971: $(F(n) \bmod m)_{n\geq 0}$ contains all residue classes modulo m if and only if m is 5^k times

$$2, \quad 4, \quad 6, \quad 7, \quad 14, \quad \text{or} \quad 3^j$$

for some $k \geq 0$ and $j \geq 0$.

In particular, for $p = 3$ and $p = 5$ the limiting density is 1.

Limiting density for $p = 11$

$F(n)$ is interpolated to $\mathbb{Z}_{11}$ by 10 functions $F_0(x), \dots, F_9(x)$.

Theorem (Rowland–Yassawi 2016)

The limiting density of residues attained by the Fibonacci sequence modulo 11^α is

$$\lim_{\alpha \to \infty} \frac{|\{F(n) \bmod 11^\alpha : n \geq 0\}|}{11^\alpha} = \mu\left(\bigcup_{i=0}^{9} F_i(\mathbb{Z}_{11})\right) = \frac{145}{264}.$$

Why 11? Because $\mathbb{Z}_{11}$ contains a root of $x^2 - 5 = 0$.

Constant-recursive sequences

Let $s(n)_{n\geq 0}$ be a sequence of p-adic integers satisfying a recurrence

$$s(n+\ell) + c_{\ell-1}s(n+\ell-1) + \cdots + c_1 s(n+1) + c_0 s(n) = 0$$

with constant coefficients $c_i \in \mathbb{Z}_p$.

Theorem (Rowland–Yassawi 2016)

$s(n)_{n\geq 0}$ has an approximate twisted interpolation to $\mathbb{Z}_p$, i.e. there exists

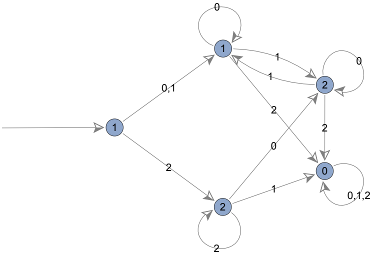
- *q a power of p,*
- *a finite partition $\mathbb{N} = \bigcup_{j\in J} A_j$ with each A_j dense in $r + q\mathbb{Z}_p$ for some $0 \leq r \leq q-1$,*
- *finitely many analytic functions $s_j : \mathbb{Z}_p \to \mathbb{C}_p$, and*
- *non-negative constants C, D with $D < 1$*

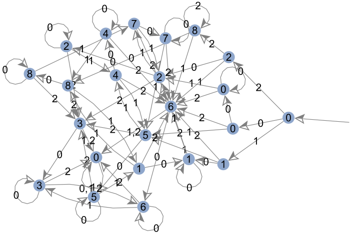
such that $|s(n) - s_j(n)|_p \leq C \cdot D^n$ for all $n \in A_j$ and $j \in J$.

Catalan numbers modulo 3^α

Recall:
Only $\approx 35\%$ of residues modulo 2^9 are attained by some $C(n)$.

$C(n)$ mod 3 and $C(n)$ mod 9:





There are no known forbidden residues modulo 3^α.

Open question

Is $\overline{\{C(n) : n \geq 0\}}$ *all of* $\mathbb{Z}_3$*?*

$C(2^n)$ in $\mathbb{Z}_2$

Theorem (Michel–Miller–Rennie 2014)

Let $a \in \mathbb{N}$. The p-adic limit $\lim_{n\to\infty} C(a\,p^n)$ exists.

In particular, in $\mathbb{Z}_2$

$$\lim_{n\to\infty} C(2^n) = 2 \cdot 3 \cdot (5 \cdot 7)^2 \cdot (9 \cdot 11 \cdot 13 \cdot 15)^3 \cdots .$$

What is the nature of this 2-adic integer? Is it algebraic over $\mathbb{Q}$?

Other sequences

Motzkin numbers $M(2^n)$:

Apéry numbers $A(2^n)$:

The rate of convergence reflects the "supercongruence"

$$A(p^n) \equiv A(p^{n-1}) \mod p^{3n}$$

for $p = 2$.