Arithmetic properties of some combinatorial sequences

Eric Rowland   Reem Yassawi

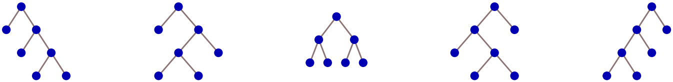
Université de Liège

2016 February 11

Catalan numbers modulo 2

What do combinatorial sequences look like modulo p^α?

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



$C(3) = 5$

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

Theorem (folklore)

For all $n \geq 0$, $C(n)$ 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*

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

Catalan numbers modulo 16

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*

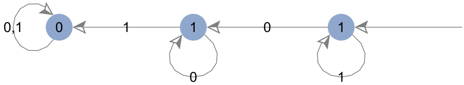
$$c_n \equiv_{16} \begin{cases} \left.\begin{matrix} 1 \\ 5 \\ 13 \end{matrix}\right\} & \text{if} \quad d(\alpha) = 0 \ \text{and} \quad \begin{cases} \beta \le 1, \\ \beta = 2, \\ \beta \ge 3, \end{cases} \\ \left.\begin{matrix} 2 \\ 10 \end{matrix}\right\} & \text{if} \quad d(\alpha) = 1,\ \alpha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

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.

Automatic sequences

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



This automaton outputs $C(n)$ mod 2 when fed the base-2 digits of n, starting with the least significant digit.

$(C(n) \bmod 2)_{n \geq 0}$ is 2-automatic.

Let $\mathcal{D}f$ denote the diagonal of a multivariate formal power series f.

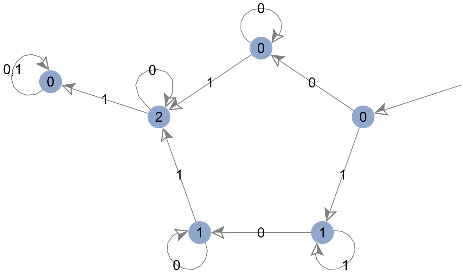
Theorem (Denef–Lipshitz 1987)

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

Catalan numbers modulo 4

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

$$\frac{y(2xy^2 + 2xy - 1)}{xy^2 + 2xy + x - 1}.$$



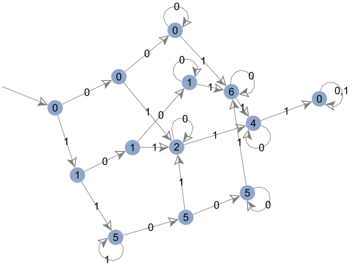
By computing an automaton for a sequence $\bmod p^\alpha$, we can answer...

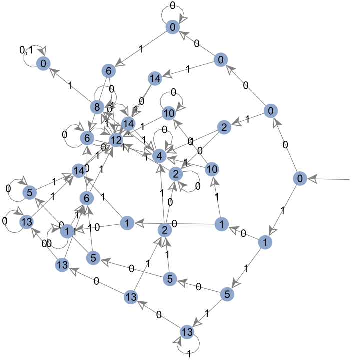
- Are there forbidden residues?
- What is the limiting distribution of residues (if it exists)?
- Is the sequence eventually periodic?
- Many other questions known to be decidable.

Catalan numbers modulo 8 and 16

Theorem (Liu–Yeh)

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





Catalan numbers modulo 2^α

Theorem

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

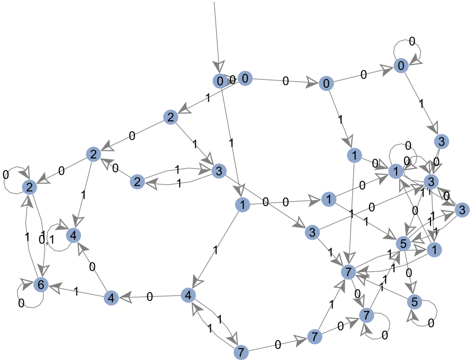
Does the density of residues modulo 2^α that are attained by some Catalan number tend to 0 as α gets large?

Motzkin numbers modulo 8

Theorem (Eu–Liu–Yeh)

For all $n \geq 0$, $M(n) \not\equiv 0 \mod 8$.

Proof:



Other combinatorial sequences

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

Theorem

For all $n \geq 0$, $R(n) \not\equiv 16 \mod 32$.

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

Theorem

For all $n \geq 0$, $P(n) \not\equiv 16 \mod 32$.

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

Theorem

For all $n \geq 0$, $H(n) \not\equiv 0 \mod 8$.

Scope

Christol (1990) conjectured that if an integer sequence

- is holonomic and
- grows at most exponentially,

then it is the diagonal of a rational function.

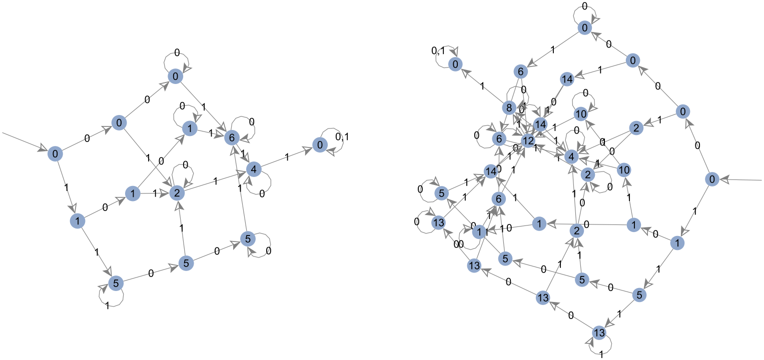
$(n!)_{n\geq 0}$ grows too quickly to be the diagonal of a rational function.

If the conjecture is true, then many sequences that occur in combinatorics are p-automatic when reduced modulo p^α.

Limiting properties

Open question

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



Can we get information about a sequence in the limit as $\alpha \to \infty$?

Values of $C(2^n)$

$$\begin{aligned}
C(1) &= 1 & &= \\
C(2) &= 2 &= {} & 10_2 \\
C(4) &= 14 &= {} & 1110_2 \\
C(8) &= 1430 &= {} & 10110010110_2 \\
C(16) &= 35357670 &= {} & 10000110111000001111100110_2
\end{aligned}$$

Michel, Miller, and Rennie (2014) showed that $\lim_{n\to\infty} C(2^n)$ exists.
This limit is a 2-adic integer.

p-adic numbers

Let p be a prime.

Every p-adic integer has a representation $d_0 + d_1 p + d_2 p^2 + \cdots$, where $d_i \in \{0, 1, \ldots, p-1\}$.

We define the p-adic absolute value $|\cdot|_p$ on $\mathbb{Q}$:
Let a, b be nonzero integers not divisible by p. Let $k \in \mathbb{Z}$.
Define $|\frac{a}{b}p^k|_p := \frac{1}{p^k}$ and $|0|_p := 0$.

$\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$.

$\mathbb{Z}_p := \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$.

In $\mathbb{Z}_2$, $\lim\limits_{n\to\infty} 2^n = 0$.

Interpolation to $\mathbb{Z}_2$?

$\lim_{n\to\infty} C(2^n)$ exists in $\mathbb{Z}_2$.

But we cannot interpolate $C(n)$ to a continuous function $C(x)$ on $\mathbb{Z}_2$ because

$$\lim_{n\to\infty} C(2^n) \neq 1 = C(0).$$

Values of $F(3^n)$

The Fibonacci sequence $F(n)_{n \geq 0} = 0, 1, 1, 2, 3, 5, 8, 13, \ldots$ satisfies

$$F(n+2) = F(n+1) + F(n).$$

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

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

Interpolation to $\mathbb{R}$

Let $\phi = \frac{1+\sqrt{5}}{2}$ and $\bar{\phi} = \frac{1-\sqrt{5}}{2}$. Then

$$F(n) = \frac{\phi^n - \bar{\phi}^n}{\sqrt{5}}.$$

Since ϕ is positive,

$$\phi^n = (\exp \log \phi)^n = \exp(n \log \phi).$$

But $\bar{\phi}$ is negative:

$$\bar{\phi}^n = (-1)^n(-\bar{\phi})^n = (-1)^n(\exp \log(-\bar{\phi}))^n = \cos(\pi n) \exp(n \log(-\bar{\phi})).$$

$F(n)$ is interpolated to $\mathbb{R}$ by the analytic function

$$F(x) = \frac{\exp(x \log \phi) - \cos(\pi x) \exp(x \log(-\bar{\phi}))}{\sqrt{5}}.$$

Extensions of $\mathbb{Q}_p$

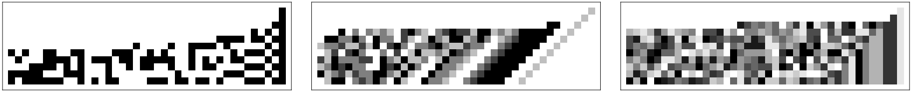
It can happen that $x^2 - x - 1$ has no roots in $\mathbb{Q}_p$.

Lemma

Let d and e be the degree and ramification index of $\mathbb{Q}_p(\sqrt{5})/\mathbb{Q}_p$.

- *If $p \equiv 2, 3 \mod 5$, then $\sqrt{5} \notin \mathbb{Q}_p$ and $d = 2$ and $e = 1$.*
- *If $p = 5$, then $\sqrt{5} \notin \mathbb{Q}_5$ and $d = e = 2$.*
- *If $p \equiv 1, 4 \mod 5$, then $\sqrt{5} \in \mathbb{Q}_p$, so $d = e = 1$.*

For $p = 2$, $p = 5$, and $p = 11$:



$f := d/e$ will turn out to be the number of limit points.

p-adic logarithm and exponential

The p-adic logarithm

$$\log_p x := \sum_{m \geq 1} (-1)^{m+1} \frac{(x-1)^m}{m}$$

converges for $x \in \mathbb{Z}_p$ such that $|x-1|_p < 1$.

The p-adic exponential function

$$\exp_p x := \sum_{m \geq 0} \frac{x^m}{m!}$$

converges for $x \in \mathbb{Z}_p$ such that $|x|_p < p^{-1/(p-1)}$.

If $|x-1|_p < p^{-1/(p-1)}$, then

$$x = \exp_p \log_p x.$$

Roots of unity

We may need to divide by a root of unity in $\mathbb{Z}_p$. Let $f = d/e$.

Proposition

Let $p \neq 2$. For each $\beta \in \mathbb{Q}_p(\sqrt{5})$ such that $|\beta|_p \leq 1$, there exists a $(p^f - 1)$-st root of unity $\omega(\beta)$ such that $|\frac{\beta}{\omega(\beta)} - 1|_p < p^{-1/(p-1)}$.

Let ϕ be a root of $x^2 - x - 1$; then $|\phi|_p = 1$, and we have

$$\begin{aligned}\phi^n = \omega(\phi)^n \left(\tfrac{\phi}{\omega(\phi)}\right)^n &= \omega(\phi)^n \left(\exp_p \log_p \left(\tfrac{\phi}{\omega(\phi)}\right)^n\right) \\ &= \omega(\phi)^n \exp_p \left(n \log_p \left(\tfrac{\phi}{\omega(\phi)}\right)\right).\end{aligned}$$

For n in a fixed residue class modulo $p^f - 1$, $\omega(\phi)^n$ is constant.

Twisted interpolation for the Fibonacci sequence

Let $\phi = \frac{1+\sqrt{5}}{2}$ and $\bar{\phi} = \frac{1-\sqrt{5}}{2}$ in $\mathbb{Q}_p(\sqrt{5})$.

Theorem

Let $p \neq 2$ be a prime, and let $0 \leq i \leq p^f - 2$.
Define the function $F_i : \mathbb{Z}_p \to \mathbb{Z}_p$ by

$$F_i(x) = \frac{\omega(\phi)^i \exp_p\left(x \log_p \frac{\phi}{\omega(\phi)}\right) - \omega(\bar{\phi})^i \exp_p\left(x \log_p \frac{\bar{\phi}}{\omega(\bar{\phi})}\right)}{\sqrt{5}}$$

$$= \sum_{m \geq 0} \frac{\left(\omega(\phi)^i - (-1)^m \omega(\bar{\phi})^i\right)\left(\log_p \frac{\phi}{\omega(\phi)}\right)^m}{m! \sqrt{5}} x^m.$$

Then $F(n) = F_i(n)$ for all $n \equiv i \mod p^f - 1$ and $0 \leq i \leq p^f - 2$.

Since $A_i := \{n \geq 0 : n \equiv i \mod p^f - 1\}$ is dense in $\mathbb{Z}_p$,
$F_i(x)$ is the unique continuous function that agrees with $F(n)$ on A_i.

$p = 5$

$\omega(\phi) = \omega(\bar{\phi}) = \omega(3)$, so all the $F_i(n)$ are equal up to a factor of $\omega(3)^n$.

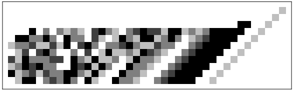
Corollary

$F(n)/\omega(3)^n$ can be extended to an analytic function on $\mathbb{Z}_5$, namely

$$\frac{2}{\sqrt{5}} \sinh_5\left(x \log_5 \frac{\phi}{\omega(3)}\right).$$

$$\sinh_p(x) := \frac{\exp_p(x) - \exp_p(-x)}{2} = \sum_{m \geq 0} \frac{1}{(2m+1)!} x^{2m+1}$$

In particular, $\lim_{n \to \infty} F(5^n) = 0$.



Limits of $F(p^n)$

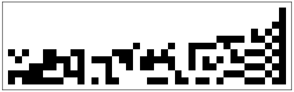
For $a, b \in \mathbb{Z}$, we have

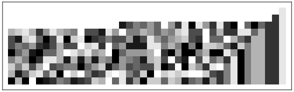
$$\lim_{n\to\infty} F(ap^{fn} + b) = \frac{\omega(\phi)^a \phi^b - \omega(\bar{\phi})^a \bar{\phi}^b}{\sqrt{5}}.$$

In $\mathbb{Z}_3$, $\lim_{n\to\infty} F(3^{2n})$ and $\lim_{n\to\infty} F(3^{2n+1})$ are equal to $\pm\sqrt{\frac{2}{5}}$.

In $\mathbb{Z}_2$, $\lim_{n\to\infty} F(2^{2n})$ and $\lim_{n\to\infty} F(2^{2n+1})$ are equal to $\pm\sqrt{-\frac{3}{5}}$.

In $\mathbb{Z}_{11}$, $\lim_{n\to\infty} F(11^n)$ is a root of $5x^2 + 5x + 1$.





Limiting density of attained residues

Burr (1971) characterized the integers m such that $(F(n) \bmod m)_{n \geq 0}$ contains all residue classes modulo m.

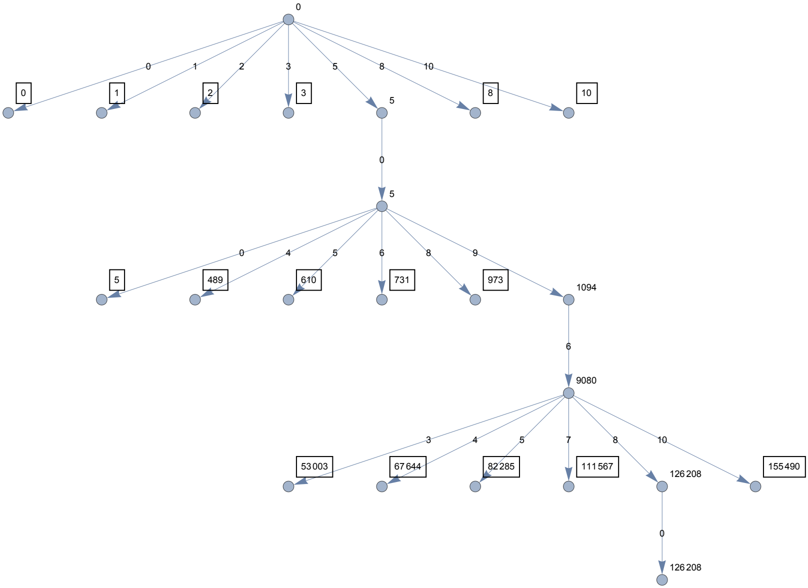
In particular, $F(n)_{n \geq 0}$ attains all residues modulo 3^α and 5^α.

Does the limit

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

exist for other primes?

Fibonacci residues modulo 11^α



Fibonacci residues modulo 11^α

Let μ be the Haar measure on $\mathbb{Z}_p$ defined by $\mu(m + p^\alpha \mathbb{Z}_p) = p^{-\alpha}$.

Theorem

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

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

The twisted interpolation of $F(n)$ to $\mathbb{Z}_{11}$ consists of 10 functions $F_0, \dots, F_9$.

General constant-recursive sequence

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

$$s(n+\ell) + a_{\ell-1} s(n+\ell-1) + \cdots + a_1 s(n+1) + a_0 s(n) = 0$$

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

We can write

$$s(n) = \sum_{\beta} c_\beta(n) \beta^n$$

for some polynomials $c_\beta(x) \in K[x]$, where β runs over the roots of the characteristic polynomial $x^\ell + \cdots + a_1 x + a_0$.

General constant-recursive sequence

Theorem

Let p be a prime, and let $s(n)_{n \geq 0}$ be a constant-recursive sequence of p-adic integers with monic characteristic polynomial $\in \mathbb{Z}_p[x]$. Then $s(n)_{n \geq 0}$ has an approximate twisted interpolation to $\mathbb{Z}_p$. That is, 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 continuous functions $s_j : \mathbb{Z}_p \to K$, 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 $j \in J$.

Example

Let $s(n+2) = 2s(n)$ and $s(0) = s(1) = 1$. The roots of the characteristic polynomial are $\pm\sqrt{2}$. For $p = 2$, the constants C, D are nonzero, since $\sqrt{2}$ is a uniformizer of $\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2$.

Applications

Theorem

Let $a, b \in \mathbb{Z}$ with $a \geq 1$. Then

$$\lim_{n\to\infty} s(ap^{fn} + b) = \sum_{|\beta|_p=1} c_\beta(b)\omega(\beta)^a \beta^b$$

In particular, the value of this limit is algebraic over $\mathbb{Q}_p$.

Theorem

Let $s(n)_{n\geq 0}$ be a sequence of p-adic integers with an approximate twisted interpolation $\{(s_{i,r}, A_{i,r}) : 0 \leq i \leq p^f - 2 \text{ and } 0 \leq r \leq q-1\}$. Then

$$\lim_{\alpha\to\infty} \frac{|\{s(n) \bmod p^\alpha : n \geq 0\}|}{p^\alpha} = \mu\left(\mathbb{Z}_p \cap \bigcup_{i,r} s_{i,r}(r + q\mathbb{Z}_p)\right).$$