p-adic valuations of polynomials

Eric Rowland

University of Liège

2015 January 8

p-adic valuation

For us, p is a prime.

Definition

Let $\nu_p(n)$ be the exponent of the largest power of p dividing n.

$\nu_5(75) = 2$ since $75 = 3^1 \cdot 5^2$.

By convention, $\nu_p(0) = \infty$.

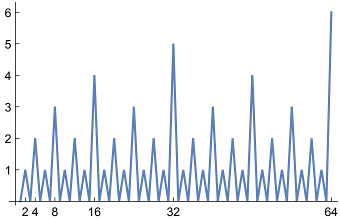
Question

Let $f(x)$ be an integer-valued polynomial.
What does the sequence $\nu_p(f(n))_{n \geq 0}$ look like?

The ruler sequence

The sequence $\nu_2(n)_{n\geq 0}$:

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\nu_2(n)$	∞	0	1	0	2	0	1	0	3	0	1	0	2	0	1	0	4



It satisfies a recurrence:

$$\nu_2(2n+0) = 1 + \nu_2(n)$$
$$\nu_2(2n+1) = 0$$

$\nu_2(an+b)_{n\geq 0}$ is an arithmetic subsequence of the ruler sequence.

A quadratic polynomial

The sequence $\nu_2(n^2 + 1)_{n \geq 0}$ is

$$0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1 \cdots.$$

This sequence is periodic:

- If n is even, then $n^2 + 1$ is odd.
- If n is odd, then $n^2 + 1 \equiv 2 \mod 4$.

More quadratic polynomials

$$\nu_2(n^2+2)_{n\geq 0} = 1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0 \cdots$$

$$\nu_2(n^2+3)_{n\geq 0} = 0\,2\,0\,2\,0\,2\,0\,2\,0\,2\,0\,2\,0\,2\,0\,2 \cdots$$

$$\nu_2(n^2+4)_{n\geq 0} = 2\,0\,3\,0\,2\,0\,3\,0\,2\,0\,3\,0\,2\,0\,3\,0 \cdots$$

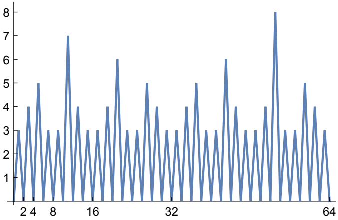
$$\nu_2(n^2+5)_{n\geq 0} = 0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1 \cdots$$

$$\nu_2(n^2+6)_{n\geq 0} = 1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0 \cdots$$

Boundedness

But $\nu_2(n^2+7)_{n\geq 0}$ is

$$0\,3\,0\,4\,0\,5\,0\,3\,0\,3\,0\,7\,0\,4\,0\,3\,0\,3\,0\,4\,0\,6\,0\,3\,0\,3\,0\,5\,0\,4\,0\,3\,\cdots.$$



Is it unbounded?

$\nu_2(n^2+7) = 3$ if and only if $n \equiv 1_2, 111_2 \mod 8$.

$\nu_2(n^2+7) = 4$ if and only if $n \equiv 1101_2, 11_2 \mod 16$.

$\nu_2(n^2+7) = 5$ if and only if $n \equiv 101_2, 11011_2 \mod 32$.

$\nu_2(n^2+7) = 6$ if and only if $n \equiv 10101_2, 101011_2 \mod 64$.

Convergence

It seems $\nu_2(n^2 + 7) = \alpha$ if and only if $n \equiv r, s \mod 2^\alpha$.

α	r	s
3	1_2	111_2
4	1101_2	11_2
5	101_2	11011_2
6	10101_2	101011_2
7	1110101_2	1011_2
8	110101_2	11001011_2
9	110110101_2	1001011_2
10	1010110101_2	101001011_2
11	10010110101_2	1101001011_2
12	100010110101_2	11101001011_2
13	1000010110101_2	111101001011_2
14	10000010110101_2	1111101001011_2

These two sequences are converging to 2-adic integers.

p-adic numbers

For a prime p, define the p-adic absolute value of a rational number by

$$\left|\frac{a}{b}\right|_p = \frac{1}{p^{\nu_p(a)-\nu_p(b)}}$$

and $|0|_p = 0$.

$|2^m|_2 = \frac{1}{2^m}$. $\lim_{m\to\infty} 2^m = 0$.
In the p-adic absolute value, n is small if it is highly divisible by p.

Definition

The set $\mathbb{Q}_p$ of p-adic numbers is the completion of $\mathbb{Q}$ w.r.t. $|\cdot|_p$.

A p-adic number can be written $\sum_{i\geq i_0} d_i p^i$, where $d_i \in \{0, 1, \dots, p-1\}$.

The set of $\mathbb{Z}_p$ of p-adic integers consists of elements $\sum_{i\geq 0} d_i p^i$.

Convergence

It seems $\nu_2(n^2 + 7) = \alpha$ if and only if $n \equiv r, s \mod 2^\alpha$.

α	r	s
3	1_2	111_2
4	1101_2	11_2
5	101_2	11011_2
6	10101_2	101011_2
7	1110101_2	1011_2
8	110101_2	11001011_2
9	110110101_2	1001011_2
10	1010110101_2	101001011_2
11	10010110101_2	1101001011_2
12	100010110101_2	11101001011_2
13	1000010110101_2	111101001011_2
14	10000010110101_2	1111101001011_2

What 2-adic integers are r, s converging to?

What are r, s converging to?

r, s make $n^2 + 7$ highly divisible by 2.
That is, $n^2 + 7 \approx 0$.

Maybe r, s are approximations to solutions of $x^2 + 7 = 0$.

In fact $x^2 + 7 = 0$ has two solutions in $\mathbb{Z}_2$ (by Hensel's lemma).
Call them $\pm\sqrt{-7} \in \mathbb{Z}_2$.

Then $\nu_2(n^2 + 7)$ is large for integer $n \approx \pm\sqrt{-7}$,
just as $\nu_2(n)$ is large for $n \approx 0$ (n highly divisible by 2).

Characterization of boundedness

General principle:
The p-adic roots of $f(x)$ determine the behavior of $\nu_p(f(n))$.

Proposition

Let $f(x)$ be an integer-valued polynomial. The sequence $\nu_p(f(n))_{n\geq 0}$ is bounded if and only if $f(x)$ has no roots in $\mathbb{Z}_p$.

x^2+1 has no roots in $\mathbb{Z}_2$ (since it has no roots modulo 4).
$\nu_2(n^2+1)$ is bounded.

x^2+7 does have roots in $\mathbb{Z}_2$.
$\nu_2(n^2+7)$ is unbounded.

Regular sequences

What is the structure of $\nu_p(f(n))_{n\geq 0}$?

For $f(x) = x$, recall

$$\begin{aligned}\nu_2(2n+0) &= 1 + \nu_2(n)\\ \nu_2(2n+1) &= 0.\end{aligned}$$

This is an example of a 2-regular sequence.

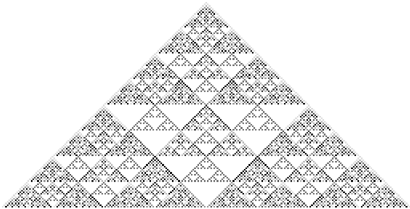
Definition (Allouche–Shallit 1992)

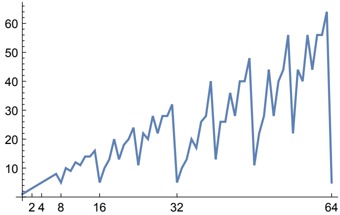
An integer sequence $s(n)_{n\geq 0}$ is k-regular if the $\mathbb{Z}$-module generated by

$$\{s(k^e n + r)_{n\geq 0} \mid e \geq 0,\ 0 \leq r \leq k^e - 1\}.$$

is finitely generated.

Counting nonzero binomial coefficients modulo 8





Let $s(n) = |\{0 \leq m \leq n : \binom{n}{m} \not\equiv 0 \mod 8\}|$.

1 2 3 4 5 6 7 8 5 10 9 12 11 14 14 16 5 10 13 20 13 18 20 24 $\cdots$

$$\begin{aligned}
s(2n+1) &= 2s(n) \\
s(4n+0) &= s(2n) \\
s(8n+2) &= -2s(n) + 2s(2n) + s(4n+2) \\
s(8n+6) &= 2s(4n+2)
\end{aligned}$$

p-regularity of valuation sequences

k-regular sequences are closed under addition and periodic indexing.

Since $\nu_2(n+1)_{n\geq 0}$ is 2-regular, the following is 2-regular.

$$\nu_2\left(74(n+1)^9(6n+5)^2(9n-7)^4\right)_{n\geq 0}$$

Each periodic sequence is k-regular for every k.
So $\nu_2(n^2+1)_{n\geq 0} = 0\,1\,0\,1\,0\,1\,\cdots$ is 2-regular.

Is $\nu_2(n^2+7)_{n\geq 0}$ a 2-regular sequence? (Does it satisfy a recurrence?)

$$0\,3\,0\,4\,0\,5\,0\,3\,0\,3\,0\,7\,0\,4\,0\,3\,0\,3\,0\,4\,0\,6\,0\,3\,0\,3\,0\,5\,0\,4\,0\,3\,\cdots$$

Theorem (Bell 2007)

If $f(x)$ is a polynomial, $\nu_p(f(n))$ is p-regular if and only if $f(x)$ factors as

$$(\textit{product of linear polynomials over } \mathbb{Q}) \cdot (\textit{polynomial with no roots in } \mathbb{Z}_p).$$

Period lengths

When $\nu_p(f(n))_{n\geq 0}$ is periodic, what is its (minimal) period length?

sequence	period length
$\nu_2(n^2+1)_{n\geq 0} = 0\,1\,0\,1\,0\,1\,0\,1\,\cdots$	2
$\nu_2(n^2+2)_{n\geq 0} = 1\,0\,1\,0\,1\,0\,1\,0\,\cdots$	2
$\nu_2(n^2+3)_{n\geq 0} = 0\,2\,0\,2\,0\,2\,0\,2\,\cdots$	2
$\nu_2(n^2+4)_{n\geq 0} = 2\,0\,3\,0\,2\,0\,3\,0\,\cdots$	4
$\nu_2(n^2+5)_{n\geq 0} = 0\,1\,0\,1\,0\,1\,0\,1\,\cdots$	2
$\nu_2(n^2+6)_{n\geq 0} = 1\,0\,1\,0\,1\,0\,1\,0\,\cdots$	2

A sequence with period length 8:

$$\nu_2(n^2+16)_{n\geq 0} = 4\,0\,2\,0\,5\,0\,2\,0\,4\,0\,2\,0\,5\,0\,2\,0\,\cdots$$

The period length

Again the roots of $f(x)$ determine the behavior of $\nu_p(f(n))$.
$f(x)$ has no roots in $\mathbb{Z}_p$ (otherwise $\nu_p(f(n))$ would be unbounded).

Theorem (Medina–Moll–Rowland 2015)

Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial that is irreducible over $\mathbb{Z}_p$.
Let $\alpha \geq 1$ be minimal such that $f(x) \equiv 0 \mod p^\alpha$ has no solutions.
Then $\nu_p(f(n))_{n \geq 0}$ is periodic with period length $p^{\lceil \frac{\alpha-1}{\deg f} \rceil}$.

For example, let $p = 2$ and $f(x) = x^3 + 8x^2 + 256x + 128$.

$f(x) \equiv 0 \mod 2^8$ has no solutions; $f(x) \equiv 0 \mod 2^7$ does, so $\alpha = 8$.
Therefore the period length is $p^{\lceil \frac{\alpha-1}{\deg f} \rceil} = 2^3$:

$$\nu_2(f(n))_{n \geq 0} = 7\,0\,3\,0\,6\,0\,3\,0\,7\,0\,3\,0\,6\,0\,3\,0 \cdots$$