An introduction to the p-adics

Siddharth Bhat

IIIT Theory group
Seminar Saturday

October 10th, 2019

Why p-adics?

Analogy between:

- $\mathbb{Z}$,

Why p-adics?

Analogy between:

- $\mathbb{Z}$, where $3, 5, 7, \ldots$ are the "primes"

Why p-adics?

Analogy between:

- $\mathbb{Z}$, where $3, 5, 7, \ldots$ are the "primes"
- $\mathbb{C}[X]$,

Why p-adics?

Analogy between:

- $\mathbb{Z}$, where $3, 5, 7, \ldots$ are the "primes"
- $\mathbb{C}[X]$, where $(x - a)$ are the "primes"

What is evaluation?

Remainder when dividing $p(x) = x^3 + x^2 + x + 1$ by $q(x) = x - 1$?

What is evaluation?

Remainder when dividing $p(x) = x^3 + x^2 + x + 1$ by $q(x) = x - 1$?

$$
\begin{array}{r|l}
\multicolumn{2}{r}{X^2 + 2X + 3} \\
\cline{2-2}
X - 1 & X^3 + X^2 + X + 1 \\
 & -X^3 + X^2 \\
\cline{2-2}
 & \qquad 2X^2 + X \\
 & \quad -2X^2 + 2X \\
\cline{2-2}
 & \qquad\qquad 3X + 1 \\
 & \qquad\quad -3X + 3 \\
\cline{2-2}
 & \qquad\qquad\qquad 4
\end{array}
$$

What is evaluation?

Remainder when dividing $p(x) = x^3 + x^2 + x + 1$ by $q(x) = x - 1$?

$$
\begin{array}{rrrrr}
 & & X^2 & +2X & +3 \\
\cline{2-5}
X-1) & X^3 & +X^2 & +X & +1 \\
 & -X^3 & +X^2 & & \\
\cline{2-3}
 & & 2X^2 & +X & \\
 & & -2X^2 & +2X & \\
\cline{3-4}
 & & & 3X & +1 \\
 & & & -3X & +3 \\
\cline{4-5}
 & & & & 4
\end{array}
$$

$$(x^3 + x^2 + x + 1) = (x - 1)(x^2 + 2x + 3) + 4$$

What is evaluation?

Remainder when dividing $p(x) = x^3 + x^2 + x + 1$ by $q(x) = x - 1$?

$$
\begin{array}{rrrrr}
 & & X^2 & +2X & +3 \\
\cline{2-5}
X-1 \big) & X^3 & +X^2 & +X & +1 \\
 & -X^3 & +X^2 & & \\
\cline{2-3}
 & & 2X^2 & +X & \\
 & & -2X^2 & +2X & \\
\cline{3-4}
 & & & 3X & +1 \\
 & & & -3X & +3 \\
\cline{4-5}
 & & & & 4
\end{array}
$$

$$(x^3 + x^2 + x + 1) = (x - 1)(x^2 + 2x + 3) + 4$$

- $p(1) = 1^3 + 1^2 + 1 + 1 = 4$. Coincidence?

What is evaluation?

Remainder when dividing $p(x) = x^3 + x^2 + x + 1$ by $q(x) = x - 1$?

$$
\begin{array}{r|l}
 & X^2 + 2X + 3 \\ \hline
X - 1 & X^3 + X^2 + X + 1 \\
 & -X^3 + X^2 \\ \cline{2-2}
 & 2X^2 + X \\
 & -2X^2 + 2X \\ \cline{2-2}
 & 3X + 1 \\
 & -3X + 3 \\ \cline{2-2}
 & 4
\end{array}
$$

$$(x^3 + x^2 + x + 1) = (x - 1)(x^2 + 2x + 3) + 4$$

- $p(1) = 1^3 + 1^2 + 1 + 1 = 4$. Coincidence?
- Factoring out $q(x) = (x - 1)$

What is evaluation?

Remainder when dividing $p(x) = x^3 + x^2 + x + 1$ by $q(x) = x - 1$?

$$
\begin{array}{r|llll}
\multicolumn{5}{r}{X^2 + 2X + 3} \\
\cline{2-5}
X - 1) & X^3 & + X^2 & + X & + 1 \\
 & - X^3 & + X^2 & & \\
\cline{2-3}
 & & 2X^2 & + X & \\
 & & - 2X^2 & + 2X & \\
\cline{3-4}
 & & & 3X & + 1 \\
 & & & - 3X & + 3 \\
\cline{4-5}
 & & & & 4
\end{array}
$$

$$(x^3 + x^2 + x + 1) = (x - 1)(x^2 + 2x + 3) + 4$$

- $p(1) = 1^3 + 1^2 + 1 + 1 = 4$. Coincidence?
- Factoring out $q(x) = (x - 1) \simeq$ setting $q(x) = 0$

What is evaluation?

Remainder when dividing $p(x) = x^3 + x^2 + x + 1$ by $q(x) = x - 1$?

$$
\begin{array}{r|l}
 & X^2 + 2X + 3 \\
\hline
X - 1) & X^3 \; + X^2 \; + X + 1 \\
 & -X^3 \; + X^2 \\
\hline
 & 2X^2 \; + X \\
 & -2X^2 + 2X \\
\hline
 & 3X + 1 \\
 & -3X + 3 \\
\hline
 & 4
\end{array}
$$

$$(x^3 + x^2 + x + 1) = (x - 1)(x^2 + 2x + 3) + 4$$

- $p(1) = 1^3 + 1^2 + 1 + 1 = 4.$ Coincidence?
- Factoring out $q(x) = (x - 1) \simeq$ setting $q(x) = 0$: remove $q(x)$.

What is evaluation?

Remainder when dividing $p(x) = x^3 + x^2 + x + 1$ by $q(x) = x - 1$?

$$
\begin{array}{r}
X^2 + 2X + 3 \\
X - 1 \overline{\big)\; X^3 + X^2 + X + 1} \\
\underline{-X^3 + X^2} \qquad \\
2X^2 + X \qquad \\
\underline{-2X^2 + 2X} \quad \\
3X + 1 \\
\underline{-3X + 3} \\
4
\end{array}
$$

$$(x^3 + x^2 + x + 1) = (x - 1)(x^2 + 2x + 3) + 4$$

- $p(1) = 1^3 + 1^2 + 1 + 1 = 4$. Coincidence?
- Factoring out $q(x) = (x - 1) \simeq$ setting $q(x) = 0$: remove $q(x)$.
- setting $x - 1 = 0$, or setting $x = 1$

What is evaluation?

Remainder when dividing $p(x) = x^3 + x^2 + x + 1$ by $q(x) = x - 1$?

$$
\begin{array}{r|l}
 & X^2 + 2X + 3 \\
\hline
X - 1 & X^3 + X^2 + X + 1 \\
 & -X^3 + X^2 \\
\hline
 & 2X^2 + X \\
 & -2X^2 + 2X \\
\hline
 & 3X + 1 \\
 & -3X + 3 \\
\hline
 & 4
\end{array}
$$

$$(x^3 + x^2 + x + 1) = (x - 1)(x^2 + 2x + 3) + 4$$

- $p(1) = 1^3 + 1^2 + 1 + 1 = 4$. Coincidence?
- Factoring out $q(x) = (x - 1) \simeq$ setting $q(x) = 0$: remove $q(x)$.
- setting $x - 1 = 0$, or setting $x = 1$
- Substituting $x = 1$: $p(1) = 1^3 + 1^2 + 1 + 1 = 4$

What is evaluation?

Remainder when dividing $p(x) = x^3 + x^2 + x + 1$ by $q(x) = x - 1$?

$$
\begin{array}{rrrrr}
 & & X^2 & +2X & +3 \\ \cline{2-5}
X-1) & X^3 & +X^2 & +X & +1 \\
 & -X^3 & +X^2 & & \\ \cline{2-3}
 & & 2X^2 & +X & \\
 & & -2X^2 & +2X & \\ \cline{3-4}
 & & & 3X & +1 \\
 & & & -3X & +3 \\ \cline{4-5}
 & & & & 4
\end{array}
$$

$$(x^3 + x^2 + x + 1) = (x - 1)(x^2 + 2x + 3) + 4$$

- $p(1) = 1^3 + 1^2 + 1 + 1 = 4$. Coincidence?
- Factoring out $q(x) = (x - 1) \simeq$ setting $q(x) = 0$: remove $q(x)$.
- setting $x - 1 = 0$, or setting $x = 1$
- Substituting $x = 1$: $p(1) = 1^3 + 1^2 + 1 + 1 = 4$

remainder of $p(x)$ on factoring $(x - a) \simeq$ evaluation of $p(x_0)$ at $x_0 = a$

What is evaluation in $\mathbb{Z}$?

remainder of $p(x)$ on factoring $(x - a) \simeq$ evaluation of $p(x_0)$ at $x_0 = a$

What is evaluation in $\mathbb{Z}$?

remainder of $p(x)$ on factoring $(x - a) \simeq$ evaluation of $p(x_0)$ at $x_0 = a$

evaluation of $p(x_0)$ at $x_0 = a \simeq$ remainder of $p(x)$ on factoring $(x - a)$

What is evaluation in $\mathbb{Z}$?

remainder of $p(x)$ on factoring $(x - a) \simeq$ evaluation of $p(x_0)$ at $x_0 = a$

evaluation of $p(x_0)$ at $x_0 = a \simeq$ remainder of $p(x)$ on factoring $(x - a)$

- $10(2)$

What is evaluation in $\mathbb{Z}$?

remainder of $p(x)$ on factoring $(x-a) \simeq$ evaluation of $p(x_0)$ at $x_0 = a$

evaluation of $p(x_0)$ at $x_0 = a \simeq$ remainder of $p(x)$ on factoring $(x-a)$

- $10(2) =$ remainder of 10 when factored by 2;

What is evaluation in $\mathbb{Z}$?

$$\text{remainder of } p(x) \text{ on factoring } (x-a) \simeq \text{evaluation of } p(x_0) \text{ at } x_0 = a$$

$$\text{evaluation of } p(x_0) \text{ at } x_0 = a \simeq \text{remainder of } p(x) \text{ on factoring } (x-a)$$

- $10(2)$ = remainder of 10 when factored by 2; $10 = 2 \cdot 5 + 0$

What is evaluation in $\mathbb{Z}$?

remainder of $p(x)$ on factoring $(x-a) \simeq$ evaluation of $p(x_0)$ at $x_0 = a$

evaluation of $p(x_0)$ at $x_0 = a \simeq$ remainder of $p(x)$ on factoring $(x-a)$

- $10(2)$ = remainder of 10 when factored by 2; $10 = 2 \cdot 5 + 0$; $10(2) = 0$

What is evaluation in $\mathbb{Z}$?

remainder of $p(x)$ on factoring $(x - a) \simeq$ evaluation of $p(x_0)$ at $x_0 = a$

evaluation of $p(x_0)$ at $x_0 = a \simeq$ remainder of $p(x)$ on factoring $(x - a)$

- $10(2)$ = remainder of 10 when factored by 2; $10 = 2 \cdot 5 + 0$; $10(2) = 0$
- $10(3)$

What is evaluation in $\mathbb{Z}$?

remainder of $p(x)$ on factoring $(x - a) \simeq$ evaluation of $p(x_0)$ at $x_0 = a$

evaluation of $p(x_0)$ at $x_0 = a \simeq$ remainder of $p(x)$ on factoring $(x - a)$

- $10(2)$ $=$ remainder of 10 when factored by 2; $10 = 2 \cdot 5 + 0$; $10(2) = 0$
- $10(3)$ $=$ remainder of 10 when factored by 3;

What is evaluation in $\mathbb{Z}$?

remainder of $p(x)$ on factoring $(x - a) \simeq$ evaluation of $p(x_0)$ at $x_0 = a$

evaluation of $p(x_0)$ at $x_0 = a \simeq$ remainder of $p(x)$ on factoring $(x - a)$

- $10(2)$ = remainder of 10 when factored by 2; $10 = 2 \cdot 5 + 0$; $10(2) = 0$
- $10(3)$ = remainder of 10 when factored by 3; $10 = 3 \cdot 3 + 1$

What is evaluation in $\mathbb{Z}$?

remainder of $p(x)$ on factoring $(x-a) \simeq$ evaluation of $p(x_0)$ at $x_0 = a$

evaluation of $p(x_0)$ at $x_0 = a \simeq$ remainder of $p(x)$ on factoring $(x-a)$

- $10(2) =$ remainder of 10 when factored by 2; $10 = 2 \cdot 5 + 0$; $10(2) = 0$
- $10(3) =$ remainder of 10 when factored by 3; $10 = 3 \cdot 3 + 1$; $10(3) = 1$

What is evaluation in $\mathbb{Z}$?

remainder of $p(x)$ on factoring $(x - a) \simeq$ evaluation of $p(x_0)$ at $x_0 = a$

evaluation of $p(x_0)$ at $x_0 = a \simeq$ remainder of $p(x)$ on factoring $(x - a)$

- $10(2) =$ remainder of 10 when factored by 2; $10 = 2 \cdot 5 + 0$; $10(2) = 0$
- $10(3) =$ remainder of 10 when factored by 3; $10 = 3 \cdot 3 + 1$; $10(3) = 1$
- $10(5)$

What is evaluation in $\mathbb{Z}$?

remainder of $p(x)$ on factoring $(x-a) \simeq$ evaluation of $p(x_0)$ at $x_0 = a$

evaluation of $p(x_0)$ at $x_0 = a \simeq$ remainder of $p(x)$ on factoring $(x-a)$

- $10(2) =$ remainder of 10 when factored by 2; $10 = 2 \cdot 5 + 0$; $10(2) = 0$
- $10(3) =$ remainder of 10 when factored by 3; $10 = 3 \cdot 3 + 1$; $10(3) = 1$
- $10(5) =$ remainder of 10 when factored by 5;

What is evaluation in $\mathbb{Z}$?

remainder of $p(x)$ on factoring $(x-a) \simeq$ evaluation of $p(x_0)$ at $x_0 = a$

evaluation of $p(x_0)$ at $x_0 = a \simeq$ remainder of $p(x)$ on factoring $(x-a)$

- $10(2)$ = remainder of 10 when factored by 2; $10 = 2 \cdot 5 + 0$; $10(2) = 0$
- $10(3)$ = remainder of 10 when factored by 3; $10 = 3 \cdot 3 + 1$; $10(3) = 1$
- $10(5)$ = remainder of 10 when factored by 5; $10 = 5 \cdot 2 + 0$

What is evaluation in $\mathbb{Z}$?

remainder of $p(x)$ on factoring $(x-a) \simeq$ evaluation of $p(x_0)$ at $x_0 = a$

evaluation of $p(x_0)$ at $x_0 = a \simeq$ remainder of $p(x)$ on factoring $(x-a)$

- $10(2) =$ remainder of 10 when factored by 2; $10 = 2 \cdot 5 + 0$; $10(2) = 0$
- $10(3) =$ remainder of 10 when factored by 3; $10 = 3 \cdot 3 + 1$; $10(3) = 1$
- $10(5) =$ remainder of 10 when factored by 5; $10 = 5 \cdot 2 + 0$; $10(5) = 0$

What is evaluation in $\mathbb{Z}$?

remainder of $p(x)$ on factoring $(x-a) \simeq$ evaluation of $p(x_0)$ at $x_0 = a$

evaluation of $p(x_0)$ at $x_0 = a \simeq$ remainder of $p(x)$ on factoring $(x-a)$

- $10(2)$ = remainder of 10 when factored by 2; $10 = 2 \cdot 5 + 0$; $10(2) = 0$
- $10(3)$ = remainder of 10 when factored by 3; $10 = 3 \cdot 3 + 1$; $10(3) = 1$
- $10(5)$ = remainder of 10 when factored by 5; $10 = 5 \cdot 2 + 0$; $10(5) = 0$
- $10(7)$

What is evaluation in $\mathbb{Z}$?

$$\text{remainder of } p(x) \text{ on factoring } (x-a) \simeq \text{evaluation of } p(x_0) \text{ at } x_0 = a$$

$$\text{evaluation of } p(x_0) \text{ at } x_0 = a \simeq \text{remainder of } p(x) \text{ on factoring } (x-a)$$

- $10(2) =$ remainder of 10 when factored by 2; $10 = 2 \cdot 5 + 0$; $10(2) = 0$
- $10(3) =$ remainder of 10 when factored by 3; $10 = 3 \cdot 3 + 1$; $10(3) = 1$
- $10(5) =$ remainder of 10 when factored by 5; $10 = 5 \cdot 2 + 0$; $10(5) = 0$
- $10(7) =$ remainder of 10 when factored by 7;

What is evaluation in $\mathbb{Z}$?

remainder of $p(x)$ on factoring $(x - a) \simeq$ evaluation of $p(x_0)$ at $x_0 = a$

evaluation of $p(x_0)$ at $x_0 = a \simeq$ remainder of $p(x)$ on factoring $(x - a)$

- $10(2)$ $=$ remainder of 10 when factored by 2; $10 = 2 \cdot 5 + 0$; $10(2) = 0$
- $10(3)$ $=$ remainder of 10 when factored by 3; $10 = 3 \cdot 3 + 1$; $10(3) = 1$
- $10(5)$ $=$ remainder of 10 when factored by 5; $10 = 5 \cdot 2 + 0$; $10(5) = 0$
- $10(7)$ $=$ remainder of 10 when factored by 7; $10 = 7 \cdot 1 + 3$

What is evaluation in $\mathbb{Z}$?

remainder of $p(x)$ on factoring $(x-a) \simeq$ evaluation of $p(x_0)$ at $x_0 = a$

evaluation of $p(x_0)$ at $x_0 = a \simeq$ remainder of $p(x)$ on factoring $(x-a)$

- $10(2)$ = remainder of 10 when factored by 2; $10 = 2 \cdot 5 + 0$; $10(2) = 0$
- $10(3)$ = remainder of 10 when factored by 3; $10 = 3 \cdot 3 + 1$; $10(3) = 1$
- $10(5)$ = remainder of 10 when factored by 5; $10 = 5 \cdot 2 + 0$; $10(5) = 0$
- $10(7)$ = remainder of 10 when factored by 7; $10 = 7 \cdot 1 + 3$; $10(7) = 3$

What is evaluation in $\mathbb{Z}$?

remainder of $p(x)$ on factoring $(x - a) \simeq$ evaluation of $p(x_0)$ at $x_0 = a$

evaluation of $p(x_0)$ at $x_0 = a \simeq$ remainder of $p(x)$ on factoring $(x - a)$

- $10(2)$ = remainder of 10 when factored by 2; $10 = 2 \cdot 5 + 0$; $10(2) = 0$
- $10(3)$ = remainder of 10 when factored by 3; $10 = 3 \cdot 3 + 1$; $10(3) = 1$
- $10(5)$ = remainder of 10 when factored by 5; $10 = 5 \cdot 2 + 0$; $10(5) = 0$
- $10(7)$ = remainder of 10 when factored by 7; $10 = 7 \cdot 1 + 3$; $10(7) = 3$

Why $n(p)$: only primes?

- $10(5) =$ remainder of 10 when factored by 5; $10 = 5 \cdot 2 + 0$; $10(5) = 0$
- $10(7) =$ remainder of 10 when factored by 7; $10 = 7 \cdot 1 + 3$; $10(7) = 3$
- $p(x) = (x^2 - 15x + 50)$.

Why $n(p)$: only primes?

- $10(5) =$ remainder of 10 when factored by 5; $10 = 5 \cdot 2 + 0$; $10(5) = 0$
- $10(7) =$ remainder of 10 when factored by 7; $10 = 7 \cdot 1 + 3$; $10(7) = 3$
- $p(x) = (x^2 - 15x + 50)$.
- $p(5) =$

Why $n(p)$: only primes?

- $10(5) =$ remainder of 10 when factored by 5; $10 = 5 \cdot 2 + 0$; $10(5) = 0$
- $10(7) =$ remainder of 10 when factored by 7; $10 = 7 \cdot 1 + 3$; $10(7) = 3$
- $p(x) = (x^2 - 15x + 50)$.
- $p(5) =$ remainder of $p(x)$ when factored by $(x - 5)$;

Why $n(p)$: only primes?

- $10(5)$ = remainder of 10 when factored by 5; $10 = 5 \cdot 2 + 0$; $10(5) = 0$
- $10(7)$ = remainder of 10 when factored by 7; $10 = 7 \cdot 1 + 3$; $10(7) = 3$
- $p(x) = (x^2 - 15x + 50)$.
- $p(5)$ = remainder of $p(x)$ when factored by $(x - 5)$;
- $p(x) = (x - 5)(x - 10) + 0$;

Why $n(p)$: only primes?

- $10(5)$ = remainder of 10 when factored by 5; $10 = 5 \cdot 2 + 0$; $10(5) = 0$
- $10(7)$ = remainder of 10 when factored by 7; $10 = 7 \cdot 1 + 3$; $10(7) = 3$
- $p(x) = (x^2 - 15x + 50)$.
- $p(5)$ = remainder of $p(x)$ when factored by $(x - 5)$;
- $p(x) = (x - 5)(x - 10) + 0$; $p(5) = 0$

Why $n(p)$: only primes?

- $10(5) =$ remainder of 10 when factored by 5; $10 = 5 \cdot 2 + 0$; $10(5) = 0$
- $10(7) =$ remainder of 10 when factored by 7; $10 = 7 \cdot 1 + 3$; $10(7) = 3$
- $p(x) = (x^2 - 15x + 50)$.
- $p(5) =$ remainder of $p(x)$ when factored by $(x - 5)$;
- $p(x) = (x - 5)(x - 10) + 0$; $p(5) = 0$
- $p(1) =$

Why $n(p)$: only primes?

- $10(5) =$ remainder of 10 when factored by 5; $10 = 5 \cdot 2 + 0$; $10(5) = 0$
- $10(7) =$ remainder of 10 when factored by 7; $10 = 7 \cdot 1 + 3$; $10(7) = 3$
- $p(x) = (x^2 - 15x + 50)$.
- $p(5) =$ remainder of $p(x)$ when factored by $(x - 5)$;
- $p(x) = (x - 5)(x - 10) + 0$; $p(5) = 0$
- $p(1) =$ remainder of $p(x)$ when factored by $(x - 1)$;

Why $n(p)$: only primes?

- $10(5)$ = remainder of 10 when factored by 5; $10 = 5 \cdot 2 + 0$; $10(5) = 0$
- $10(7)$ = remainder of 10 when factored by 7; $10 = 7 \cdot 1 + 3$; $10(7) = 3$
- $p(x) = (x^2 - 15x + 50)$.
- $p(5)$ = remainder of $p(x)$ when factored by $(x - 5)$;
- $p(x) = (x - 5)(x - 10) + 0$; $p(5) = 0$
- $p(1)$ = remainder of $p(x)$ when factored by $(x - 1)$;
- $p(x) = (x - 1)(x - 14) + 36$;

Why $n(p)$: only primes?

- $10(5)$ = remainder of 10 when factored by 5; $10 = 5 \cdot 2 + 0$; $10(5) = 0$
- $10(7)$ = remainder of 10 when factored by 7; $10 = 7 \cdot 1 + 3$; $10(7) = 3$
- $p(x) = (x^2 - 15x + 50)$.
- $p(5)$ = remainder of $p(x)$ when factored by $(x - 5)$;
- $p(x) = (x - 5)(x - 10) + 0$; $p(5) = 0$
- $p(1)$ = remainder of $p(x)$ when factored by $(x - 1)$;
- $p(x) = (x - 1)(x - 14) + 36$; $p(1) = 36$

Why $n(p)$: only primes?

- $10(5)$ = remainder of 10 when factored by 5; $10 = 5 \cdot 2 + 0$; $10(5) = 0$
- $10(7)$ = remainder of 10 when factored by 7; $10 = 7 \cdot 1 + 3$; $10(7) = 3$
- $p(x) = (x^2 - 15x + 50)$.
- $p(5)$ = remainder of $p(x)$ when factored by $(x - 5)$;
- $p(x) = (x - 5)(x - 10) + 0$; $p(5) = 0$
- $p(1)$ = remainder of $p(x)$ when factored by $(x - 1)$;
- $p(x) = (x - 1)(x - 14) + 36$; $p(1) = 36$

Why $n(p)$: only primes?

- $10(5)$ = remainder of 10 when factored by 5; $10 = 5 \cdot 2 + 0$; $10(5) = 0$
- $10(7)$ = remainder of 10 when factored by 7; $10 = 7 \cdot 1 + 3$; $10(7) = 3$
- $p(x) = (x^2 - 15x + 50)$.
- $p(5)$ = remainder of $p(x)$ when factored by $(x - 5)$;
- $p(x) = (x - 5)(x - 10) + 0$; $p(5) = 0$
- $p(1)$ = remainder of $p(x)$ when factored by $(x - 1)$;
- $p(x) = (x - 1)(x - 14) + 36$; $p(1) = 36$

Theorem (Fundamental theorem of algebra)

Every nonconstant polynomial $p(x) \in \mathbb{C}[X]$ can be written uniquely (upto reordering) as a product of monic irreducibles of the form $(x - z_i)$ for $z_i \in C[X]$.

$$p(x) = \pm 1 \prod_i (x - z_i)$$

Why $n(p)$: only primes?

- $10(5) =$ remainder of 10 when factored by 5; $10 = 5 \cdot 2 + 0$; $10(5) = 0$
- $10(7) =$ remainder of 10 when factored by 7; $10 = 7 \cdot 1 + 3$; $10(7) = 3$
- $p(x) = (x^2 - 15x + 50)$.
- $p(5) =$ remainder of $p(x)$ when factored by $(x - 5)$;
- $p(x) = (x - 5)(x - 10) + 0$; $p(5) = 0$
- $p(1) =$ remainder of $p(x)$ when factored by $(x - 1)$;
- $p(x) = (x - 1)(x - 14) + 36$; $p(1) = 36$

Theorem (Fundamental theorem of algebra)

Every nonconstant polynomial $p(x) \in \mathbb{C}[X]$ can be written uniquely (upto reordering) as a product of monic irreducibles of the form $(x - z_i)$ for $z_i \in C[X]$.

$$p(x) = \pm 1 \prod_i (x - z_i)$$

Theorem (Fundamental theorem of arithmetic)

Every non-zero integer can be written uniquely (upto reordering) as a product of primes

$$n = \pm 1 \prod_i p_i$$

Cheap trick?

- What are the complex numbers?

Cheap trick?

- What are the complex numbers?
- $\mathbb{R}$ with i: $i^2 = -1$.

Cheap trick?

- What are the complex numbers?
- $\mathbb{R}$ with i: $i^2 = -1$. That is, $i^2 + 1 = 0$.

Cheap trick?

- What are the complex numbers?
- $\mathbb{R}$ with i: $i^2 = -1$. That is, $i^2 + 1 = 0$.
- Equivalently: $\mathbb{R}[X]$

Cheap trick?

- What are the complex numbers?
- $\mathbb{R}$ with i: $i^2 = -1$. That is, $i^2 + 1 = 0$.
- Equivalently: $\mathbb{R}[X]$ divided by $q(x) = x^2 + 1$.

Cheap trick?

- What are the complex numbers?
- $\mathbb{R}$ with i: $i^2 = -1$. That is, $i^2 + 1 = 0$.
- Equivalently: $\mathbb{R}[X]$ divided by $q(x) = x^2 + 1$.
- Left with only linear polynomials.

Cheap trick?

- What are the complex numbers?
- $\mathbb{R}$ with i: $i^2 = -1$. That is, $i^2 + 1 = 0$.
- Equivalently: $\mathbb{R}[X]$ divided by $q(x) = x^2 + 1$.
- Left with only linear polynomials.
- All higher power polynomials $h(x)$ are $h(x) = p(x) \cdot q(x) + r(x)$

Cheap trick?

- What are the complex numbers?
- $\mathbb{R}$ with i: $i^2 = -1$. That is, $i^2 + 1 = 0$.
- Equivalently: $\mathbb{R}[X]$ divided by $q(x) = x^2 + 1$.
- Left with only linear polynomials.
- All higher power polynomials $h(x)$ are $h(x) = p(x) \cdot q(x) + r(x)$ $\texttt{degree}(r) \leqslant 1$.
- Sum of linear polynomials: $(a + xb) + (c + xd) = (a + c) + x(b + d)$

Cheap trick?

- What are the complex numbers?
- $\mathbb{R}$ with i: $i^2 = -1$. That is, $i^2 + 1 = 0$.
- Equivalently: $\mathbb{R}[X]$ divided by $q(x) = x^2 + 1$.
- Left with only linear polynomials.
- All higher power polynomials $h(x)$ are $h(x) = p(x) \cdot q(x) + r(x)$ $\texttt{degree}(r) \leqslant 1$.
- Sum of linear polynomials: $(a + xb) + (c + xd) = (a + c) + x(b + d)$
- Product of linear polynomials: $(a + xb) \cdot (c + xd) = ac + x(ad + bc) + bdx^2$

Cheap trick?

- What are the complex numbers?
- $\mathbb{R}$ with i: $i^2 = -1$. That is, $i^2 + 1 = 0$.
- Equivalently: $\mathbb{R}[X]$ divided by $q(x) = x^2 + 1$.
- Left with only linear polynomials.
- All higher power polynomials $h(x)$ are $h(x) = p(x) \cdot q(x) + r(x)$ $\mathtt{degree}(r) \leqslant 1$.
- Sum of linear polynomials: $(a + xb) + (c + xd) = (a + c) + x(b + d)$
- Product of linear polynomials: $(a + xb) \cdot (c + xd) = ac + x(ad + bc) + bdx^2$
- dividing product by $q(x) = x^2 + 1$:

$$
\begin{array}{r|lr}
 & & bd \\
\hline
x^2+1) & bdx^2 + (1ad + 1bc)\,x & +\,ac \\
 & -\,bdx^2 & -\,bd \\
\hline
 & \multicolumn{2}{r}{(1ad + 1bc)\,x + (-1bd + 1ac)}
\end{array}
$$

This is what we expect: Complex multiplication

$(a + bi)(c + di) = (ad + bc)i + (ac - bd)$

Natural numbers at primes

- $(x-1)(x-3)^2$

Natural numbers at primes

- $(x-1)(x-3)^2 = x^3 - 7x^2 + 15x - 9$

Natural numbers at primes

- $(x-1)(x-3)^2 = x^3 - 7x^2 + 15x - 9$
- $x^3 - 7x^2 + 15x - 9 = 2(x-3)^2 + (x-3)^3$

Natural numbers at primes

- $(x-1)(x-3)^2 = x^3 - 7x^2 + 15x - 9$
- $x^3 - 7x^2 + 15x - 9 = 2(x-3)^2 + (x-3)^3$
- $x^3 - 7x^2 + 15x - 9$ has a root at 3 of order 2

Natural numbers at primes

- $(x-1)(x-3)^2 = x^3 - 7x^2 + 15x - 9$
- $x^3 - 7x^2 + 15x - 9 = 2(x-3)^2 + (x-3)^3$
- $x^3 - 7x^2 + 15x - 9$ has a root at 3 of order 2
- $72 = 0 \cdot 1 + 0 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^3$

Natural numbers at primes

- $(x-1)(x-3)^2 = x^3 - 7x^2 + 15x - 9$
- $x^3 - 7x^2 + 15x - 9 = 2(x-3)^2 + (x-3)^3$
- $x^3 - 7x^2 + 15x - 9$ has a root at 3 of order 2
- $72 = 0 \cdot 1 + 0 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^3$
- $72 = 3^2 * 2^3$

Natural numbers at primes

- $(x-1)(x-3)^2 = x^3 - 7x^2 + 15x - 9$
- $x^3 - 7x^2 + 15x - 9 = 2(x-3)^2 + (x-3)^3$
- $x^3 - 7x^2 + 15x - 9$ has a root at 3 of order 2
- $72 = 0 \cdot 1 + 0 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^3$
- $72 = 3^2 * 2^3$
- 72 has a root at 3 of order 2

Natural numbers at primes

- $(x-1)(x-3)^2 = x^3 - 7x^2 + 15x - 9$
- $x^3 - 7x^2 + 15x - 9 = 2(x-3)^2 + (x-3)^3$
- $x^3 - 7x^2 + 15x - 9$ has a root at 3 of order 2
- $72 = 0 \cdot 1 + 0 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^3$
- $72 = 3^2 * 2^3$
- 72 has a root at 3 of order 2
- **Definition:** The p-adic expansion of a natural number n is the unique decomposition $n = \sum_i a_i p^i$ for $0 \leqslant a_i < p$.

Extending to the negatives

- Consider -1.

Extending to the negatives

- Consider -1.
- Goal: write $-1 = a_0 3^0 + a_1 3^1 + a_2 3^2 + a_3 3^3 + \cdots$.
- $-1 \equiv -1 + 3 - 3$.

Extending to the negatives

- Consider -1.
- Goal: write $-1 = a_0 3^0 + a_1 3^1 + a_2 3^2 + a_3 3^3 + \cdots$.
- $-1 \equiv -1 + 3 - 3$.
- $-1 \equiv 2 - 3$

Extending to the negatives

- Consider -1.
- Goal: write $-1 = a_0 3^0 + a_1 3^1 + a_2 3^2 + a_3 3^3 + \cdots$.
- $-1 \equiv -1 + 3 - 3$.
- $-1 \equiv 2 - 3$
- $-1 \equiv 2 - 3 + 9 - 9$

Extending to the negatives

- Consider -1.
- Goal: write $-1 = a_0 3^0 + a_1 3^1 + a_2 3^2 + a_3 3^3 + \cdots$.
- $-1 \equiv -1 + 3 - 3$.
- $-1 \equiv 2 - 3$
- $-1 \equiv 2 - 3 + 9 - 9$
- $-1 \equiv 2 + (9 - 3) - 9$

Extending to the negatives

- Consider -1.
- Goal: write $-1 = a_0 3^0 + a_1 3^1 + a_2 3^2 + a_3 3^3 + \cdots$.
- $-1 \equiv -1 + 3 - 3$.
- $-1 \equiv 2 - 3$
- $-1 \equiv 2 - 3 + 9 - 9$
- $-1 \equiv 2 + (9 - 3) - 9$
- $-1 \equiv 2 + 6 - 9$

Extending to the negatives

- Consider -1.
- Goal: write $-1 = a_0 3^0 + a_1 3^1 + a_2 3^2 + a_3 3^3 + \cdots$.
- $-1 \equiv -1 + 3 - 3$.
- $-1 \equiv 2 - 3$
- $-1 \equiv 2 - 3 + 9 - 9$
- $-1 \equiv 2 + (9 - 3) - 9$
- $-1 \equiv 2 + 6 - 9$
- $-1 \equiv 2 + 6 - 9 + 27 - 27$

Extending to the negatives

- Consider -1.
- Goal: write $-1 = a_0 3^0 + a_1 3^1 + a_2 3^2 + a_3 3^3 + \cdots$.
- $-1 \equiv -1 + 3 - 3$.
- $-1 \equiv 2 - 3$
- $-1 \equiv 2 - 3 + 9 - 9$
- $-1 \equiv 2 + (9 - 3) - 9$
- $-1 \equiv 2 + 6 - 9$
- $-1 \equiv 2 + 6 - 9 + 27 - 27$
- $-1 \equiv 2 + 6 + (27 - 9) - 125$

Extending to the negatives

- Consider -1.
- Goal: write $-1 = a_0 3^0 + a_1 3^1 + a_2 3^2 + a_3 3^3 + \cdots$.
- $-1 \equiv -1 + 3 - 3$.
- $-1 \equiv 2 - 3$
- $-1 \equiv 2 - 3 + 9 - 9$
- $-1 \equiv 2 + (9 - 3) - 9$
- $-1 \equiv 2 + 6 - 9$
- $-1 \equiv 2 + 6 - 9 + 27 - 27$
- $-1 \equiv 2 + 6 + (27 - 9) - 125$
- $-1 \equiv 2 + 6 + 100 - 125$

Extending to the negatives

- Consider -1.
- Goal: write $-1 = a_0 3^0 + a_1 3^1 + a_2 3^2 + a_3 3^3 + \cdots$.
- $-1 \equiv -1 + 3 - 3$.
- $-1 \equiv 2 - 3$
- $-1 \equiv 2 - 3 + 9 - 9$
- $-1 \equiv 2 + (9 - 3) - 9$
- $-1 \equiv 2 + 6 - 9$
- $-1 \equiv 2 + 6 - 9 + 27 - 27$
- $-1 \equiv 2 + 6 + (27 - 9) - 125$
- $-1 \equiv 2 + 6 + 100 - 125$
- $-1 \equiv 4 \cdot 5^0 + 4 \cdot 5^1 + 4 \cdot 5^2 + \cdots$.

Extending to the negatives

- Consider -1.
- Goal: write $-1 = a_0 3^0 + a_1 3^1 + a_2 3^2 + a_3 3^3 + \cdots$.
- $-1 \equiv -1 + 3 - 3$.
- $-1 \equiv 2 - 3$
- $-1 \equiv 2 - 3 + 9 - 9$
- $-1 \equiv 2 + (9 - 3) - 9$
- $-1 \equiv 2 + 6 - 9$
- $-1 \equiv 2 + 6 - 9 + 27 - 27$
- $-1 \equiv 2 + 6 + (27 - 9) - 125$
- $-1 \equiv 2 + 6 + 100 - 125$
- $-1 \equiv 4 \cdot 5^0 + 4 \cdot 5^1 + 4 \cdot 5^2 + \cdots$.
- Curiously, this matches the 2's complement definition of -1.

Extending to the negatives

- Consider -1.
- Goal: write $-1 = a_0 3^0 + a_1 3^1 + a_2 3^2 + a_3 3^3 + \cdots$.
- $-1 \equiv -1 + 3 - 3$.
- $-1 \equiv 2 - 3$
- $-1 \equiv 2 - 3 + 9 - 9$
- $-1 \equiv 2 + (9 - 3) - 9$
- $-1 \equiv 2 + 6 - 9$
- $-1 \equiv 2 + 6 - 9 + 27 - 27$
- $-1 \equiv 2 + 6 + (27 - 9) - 125$
- $-1 \equiv 2 + 6 + 100 - 125$
- $-1 \equiv 4 \cdot 5^0 + 4 \cdot 5^1 + 4 \cdot 5^2 + \cdots$.
- Curiously, this matches the 2's complement definition of -1.
- $-a \equiv -1 \times a$. For example, let's compute $-18 \pmod 5$.

Rationals

- Evaluate $1/4$ in the 3-adic system.

Rationals

- Evaluate $1/4$ in the 3-adic system.
- $1/4$

Rationals

- Evaluate $1/4$ in the 3-adic system.
- $1/4 = 1/(1+3)$

Rationals

- Evaluate $1/4$ in the 3-adic system.
- $1/4 = 1/(1+3) = 1 - 3 + 3^2 - 3^3 + 3^4 + \ldots$

Rationals

- Evaluate $1/4$ in the 3-adic system.
- $1/4 = 1/(1+3) = 1 - 3 + 3^2 - 3^3 + 3^4 + \ldots$
- What is -3? that's not allowed!

Rationals

- Evaluate $1/4$ in the 3-adic system.
- $1/4 = 1/(1+3) = 1 - 3 + 3^2 - 3^3 + 3^4 + \dots$
- What is -3? that's not allowed!
- $3^2 = 3 \cdot 3$

Rationals

- Evaluate 1/4 in the 3-adic system.
- $1/4 = 1/(1+3) = 1 - 3 + 3^2 - 3^3 + 3^4 + \ldots$
- What is -3? that's not allowed!
- $3^2 = 3 \cdot 3$
- $1/4 = 1 - 3 + 3 \cdot 3 - 3^3 + 3^4 + \cdots$

Rationals

- Evaluate 1/4 in the 3-adic system.
- $1/4 = 1/(1+3) = 1 - 3 + 3^2 - 3^3 + 3^4 + \dots$
- What is -3? that's not allowed!
- $3^2 = 3 \cdot 3$
- $1/4 = 1 - 3 + 3 \cdot 3 - 3^3 + 3^4 + \cdots$
- $1/4 = 1 + 2 \cdot 3 - 3^3 + 3^4 + \cdots$

Rationals

- Evaluate $1/4$ in the 3-adic system.
- $1/4 = 1/(1+3) = 1 - 3 + 3^2 - 3^3 + 3^4 + \ldots$
- What is -3? that's not allowed!
- $3^2 = 3 \cdot 3$
- $1/4 = 1 - 3 + 3 \cdot 3 - 3^3 + 3^4 + \cdots$
- $1/4 = 1 + 2 \cdot 3 - 3^3 + 3^4 + \cdots$
- $1/4 = 1 + 2 \cdot 3 - 3^3 + 3 \cdot 3^3 + \cdots$

Rationals

- Evaluate $1/4$ in the 3-adic system.
- $1/4 = 1/(1+3) = 1 - 3 + 3^2 - 3^3 + 3^4 + \ldots$
- What is -3? that's not allowed!
- $3^2 = 3 \cdot 3$
- $1/4 = 1 - 3 + 3 \cdot 3 - 3^3 + 3^4 + \cdots$
- $1/4 = 1 + 2 \cdot 3 - 3^3 + 3^4 + \cdots$
- $1/4 = 1 + 2 \cdot 3 - 3^3 + 3 \cdot 3^3 + \cdots$
- $1/4 = 1 + 2 \cdot 3 + 2 \cdot 3^3 + \cdots$

Rationals

- Evaluate $1/4$ in the 3-adic system.
- $1/4 = 1/(1+3) = 1 - 3 + 3^2 - 3^3 + 3^4 + \dots$
- What is -3? that's not allowed!
- $3^2 = 3 \cdot 3$
- $1/4 = 1 - 3 + 3 \cdot 3 - 3^3 + 3^4 + \cdots$
- $1/4 = 1 + 2 \cdot 3 - 3^3 + 3^4 + \cdots$
- $1/4 = 1 + 2 \cdot 3 - 3^3 + 3 \cdot 3^3 + \cdots$
- $1/4 = 1 + 2 \cdot 3 + 2 \cdot 3^3 + \cdots$
- $1/4$ is $4^{-1} \pmod 3$

Rationals

- Evaluate $1/4$ in the 3-adic system.
- $1/4 = 1/(1+3) = 1 - 3 + 3^2 - 3^3 + 3^4 + \ldots$
- What is -3? that's not allowed!
- $3^2 = 3 \cdot 3$
- $1/4 = 1 - 3 + 3 \cdot 3 - 3^3 + 3^4 + \cdots$
- $1/4 = 1 + 2 \cdot 3 - 3^3 + 3^4 + \cdots$
- $1/4 = 1 + 2 \cdot 3 - 3^3 + 3 \cdot 3^3 + \cdots$
- $1/4 = 1 + 2 \cdot 3 + 2 \cdot 3^3 + \cdots$
- $1/4$ is $4^{-1} \pmod 3$
- $4 * 4 = 16 \equiv 1 \pmod 3$

Rationals

- Evaluate $1/4$ in the 3-adic system.
- $1/4 = 1/(1+3) = 1 - 3 + 3^2 - 3^3 + 3^4 + \ldots$
- What is -3? that's not allowed!
- $3^2 = 3 \cdot 3$
- $1/4 = 1 - 3 + 3 \cdot 3 - 3^3 + 3^4 + \cdots$
- $1/4 = 1 + 2 \cdot 3 - 3^3 + 3^4 + \cdots$
- $1/4 = 1 + 2 \cdot 3 - 3^3 + 3 \cdot 3^3 + \cdots$
- $1/4 = 1 + 2 \cdot 3 + 2 \cdot 3^3 + \cdots$
- $1/4$ is $4^{-1} \pmod 3$
- $4 * 4 = 16 \equiv 1 \pmod 3$
- $4^{-1} \equiv 4 \pmod 3$

Rationals

- Evaluate $1/4$ in the 3-adic system.
- $1/4 = 1/(1+3) = 1 - 3 + 3^2 - 3^3 + 3^4 + \ldots$
- What is -3? that's not allowed!
- $3^2 = 3 \cdot 3$
- $1/4 = 1 - 3 + 3 \cdot 3 - 3^3 + 3^4 + \cdots$
- $1/4 = 1 + 2 \cdot 3 - 3^3 + 3^4 + \cdots$
- $1/4 = 1 + 2 \cdot 3 - 3^3 + 3 \cdot 3^3 + \cdots$
- $1/4 = 1 + 2 \cdot 3 + 2 \cdot 3^3 + \cdots$
- $1/4$ is $4^{-1} \pmod 3$
- $4 * 4 = 16 \equiv 1 \pmod 3$
- $4^{-1} \equiv 4 \pmod 3$

Irrationals?

Convergence

A lemma of Hensel

On $(x - a)$

- Dividing $p(x)$ by $(x - a_0) \simeq$ evaluating $p(x)$ at $x = a_0$

On $(x - a)$

- Dividing $p(x)$ by $(x - a_0) \simeq$ evaluating $p(x)$ at $x = a_0$
- Dividing $z \in \mathbb{Z}$ by $a_0 \in \mathbb{Z} \simeq$ evaluating z at a_0?

On $(x-a)$

- Dividing $p(x)$ by $(x-a_0) \simeq$ evaluating $p(x)$ at $x=a_0$
- Dividing $z \in \mathbb{Z}$ by $a_0 \in \mathbb{Z} \simeq$ evaluating z at a_0?
- $f(x)$: continuous, emphnon-zero at $x=a_0$.

On $(x-a)$

- Dividing $p(x)$ by $(x-a_0) \simeq$ evaluating $p(x)$ at $x = a_0$
- Dividing $z \in \mathbb{Z}$ by $a_0 \in \mathbb{Z} \simeq$ evaluating z at a_0?
- $f(x)$: continuous, emphnon-zero at $x = a_0$.
- $f(x)$: *invertible* around $x = a_0$.

On $(x - a)$

- Dividing $p(x)$ by $(x - a_0) \simeq$ evaluating $p(x)$ at $x = a_0$
- Dividing $z \in \mathbb{Z}$ by $a_0 \in \mathbb{Z} \simeq$ evaluating z at a_0?
- $f(x)$: continuous, emphnon-zero at $x = a_0$.
- $f(x)$: *invertible* around $x = a_0$.
- consider 6.

On $(x-a)$

- Dividing $p(x)$ by $(x-a_0) \simeq$ evaluating $p(x)$ at $x=a_0$
- Dividing $z \in \mathbb{Z}$ by $a_0 \in \mathbb{Z} \simeq$ evaluating z at a_0?
- $f(x)$: continuous, emphnon-zero at $x=a_0$.
- $f(x)$: *invertible* around $x=a_0$.
- consider 6.
- nonzero at $a_0=4$: $6 \simeq 2 \pmod 4$

On $(x - a)$

- Dividing $p(x)$ by $(x - a_0) \simeq$ evaluating $p(x)$ at $x = a_0$
- Dividing $z \in \mathbb{Z}$ by $a_0 \in \mathbb{Z} \simeq$ evaluating z at a_0?
- $f(x)$: continuous, emphnon-zero at $x = a_0$.
- $f(x)$: *invertible* around $x = a_0$.
- consider 6.
- nonzero at $a_0 = 4$: $6 \simeq 2 \pmod 4$
- *not invertible* in $(\mathbb{Z}/4\mathbb{Z})^\times$

On $(x - a)$

- Dividing $p(x)$ by $(x - a_0) \simeq$ evaluating $p(x)$ at $x = a_0$
- Dividing $z \in \mathbb{Z}$ by $a_0 \in \mathbb{Z} \simeq$ evaluating z at a_0?
- $f(x)$: continuous, emphnon-zero at $x = a_0$.
- $f(x)$: *invertible* around $x = a_0$.
- consider 6.
- nonzero at $a_0 = 4$: $6 \simeq 2 \pmod 4$
- *not invertible* in $(\mathbb{Z}/4\mathbb{Z})^{\times}$
- $(\mathbb{Z}/n\mathbb{Z})^{\times}$:group iff n prime