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 $q(x) = x - 1$?

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

What is evaluation?

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

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

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

What is evaluation?

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

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

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

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

What is evaluation?

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

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

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

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

What is evaluation?

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

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

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

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

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 $q(x) = x - 1$?

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

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

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

$$
\begin{array}{r}
X^2 + 2X + 3 \\
X - 1 \overline{\smash{)}\, X^3 + X^2 + X + 1} \\
\underline{-X^3 + X^2 } \\
2X^2 + X \\
\underline{-2X^2 + 2X } \\
3X + 1 \\
\underline{-3X + 3} \\
4
\end{array}
$$

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

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

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

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

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

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; $10 = 2 \cdot 5 + 0$

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 $\mathbb{Z}$?

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

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

- $10(2)$ = 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;

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 $\mathbb{Z}$?

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;

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 $(x-a)$

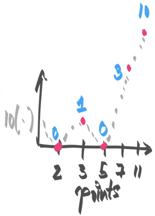
- $10(2) =$ remainder of 10 when factored by 2; $10 = 2 \cdot 5 + 0$; $10(2) = 0$
- $10(3) =$ remainder of 10 when factored by 3; $10 = 3 \cdot 3 + 1$; $10(3) = 1$
- $10(5) =$ remainder of 10 when factored by 5; $10 = 5 \cdot 2 + 0$; $10(5) = 0$
- $10(7) =$ remainder of 10 when factored by 7; $10 = 7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

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 $h(x) = p(x) \cdot q(x) + r(x)$ $\texttt{degree}(r) \leqslant 1$.

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 $h(x) = p(x) \cdot q(x) + r(x)$ $\texttt{degree}(r) \leqslant 1$.
- Example: $7x^2 + 5 = 7(x^2 + 1) - 2$

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 $h(x) = p(x) \cdot q(x) + r(x)$ $\texttt{degree}(r) \leqslant 1$.
- Example: $7x^2 + 5 = 7(x^2 + 1) - 2$
- 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 $h(x) = p(x) \cdot q(x) + r(x)$ $\texttt{degree}(r) \leqslant 1$.
- Example: $7x^2 + 5 = 7(x^2 + 1) - 2$
- 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 $h(x) = p(x) \cdot q(x) + r(x)$ $\mathtt{degree}(r) \leqslant 1$.
- Example: $7x^2 + 5 = 7(x^2 + 1) - 2$
- 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 $q(x) = x^2 + 1$:

$$
\begin{array}{r@{}l}
 & bd \\
\cline{2-2}
x^2 + 1 \big) & \; bdx^2 + (1ad + 1bc)\,x \quad + ac \\
 & -bdx^2 - bd \\
\cline{2-2}
 & (1ad + 1bc)\,x + (-1bd + 1ac)
\end{array}
$$

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 $h(x) = p(x) \cdot q(x) + r(x)$ $\mathtt{degree}(r) \leqslant 1$.
- Example: $7x^2 + 5 = 7(x^2 + 1) - 2$
- 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 $q(x) = x^2 + 1$:

$$
\begin{array}{r|lr}
 & & bd \\
\cline{2-3}
x^2+1) & bdx^2 + (1ad + 1bc)\,x & + ac \\
 & -\,bdx^2 & -\,bd \\
\cline{2-3}
 & \multicolumn{2}{r}{(1ad + 1bc)\,x + (-1bd + 1ac)}
\end{array}
$$

This is what we expect: Complex multiplication

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

Taylor series

- Taylor series of $q(x) \in \mathbb{C}[X]$ at $x = x_0$: $q(x) = \sum_i a_i (x - x_0)^i$

Taylor series

- Taylor series of $q(x) \in \mathbb{C}[X]$ at $x = x_0$: $q(x) = \sum_i a_i (x - x_0)^i$
- Taylor series of $n \in \mathbb{Z}$ at p prime: $n = \sum_i b_i p^i$.

Taylor series

- Taylor series of $q(x) \in \mathbb{C}[X]$ at $x = x_0$: $q(x) = \sum_i a_i (x - x_0)^i$
- Taylor series of $n \in \mathbb{Z}$ at p prime: $n = \sum_i b_i p^i$.

Definition

The p-adic expansion of a natural number n is the unique decomposition $n = \sum_i b_i p^i$ for $0 \leqslant b_i < p$.

- Taylor series of $q(x) = x^3 - 7x^2 + 15x - 9$

Taylor series

- Taylor series of $q(x) \in \mathbb{C}[X]$ at $x = x_0$: $q(x) = \sum_i a_i(x - x_0)^i$
- Taylor series of $n \in \mathbb{Z}$ at p prime: $n = \sum_i b_i p^i$.

Definition

The p-adic expansion of a natural number n is the unique decomposition $n = \sum_i b_i p^i$ for $0 \leqslant b_i < p$.

- Taylor series of $q(x) = x^3 - 7x^2 + 15x - 9$ at $x = 3$:

Taylor series

- Taylor series of $q(x) \in \mathbb{C}[X]$ at $x = x_0$: $q(x) = \sum_i a_i (x - x_0)^i$
- Taylor series of $n \in \mathbb{Z}$ at p prime: $n = \sum_i b_i p^i$.

Definition

The p-adic expansion of a natural number n is the unique decomposition $n = \sum_i b_i p^i$ for $0 \leqslant b_i < p$.

- Taylor series of $q(x) = x^3 - 7x^2 + 15x - 9$ at $x = 3$: $q(x) = 2(x-3)^2 + (x-3)^3$

Taylor series

- Taylor series of $q(x) \in \mathbb{C}[X]$ at $x = x_0$: $q(x) = \sum_i a_i (x - x_0)^i$
- Taylor series of $n \in \mathbb{Z}$ at p prime: $n = \sum_i b_i p^i$.

Definition

The p-adic expansion of a natural number n is the unique decomposition $n = \sum_i b_i p^i$ for $0 \leqslant b_i < p$.

- Taylor series of $q(x) = x^3 - 7x^2 + 15x - 9$ at $x = 3$: $q(x) = 2(x-3)^2 + (x-3)^3$
- $q(x) = (x-3)^2(2 + (x-3))$

Taylor series

- Taylor series of $q(x) \in \mathbb{C}[X]$ at $x = x_0$: $q(x) = \sum_i a_i(x - x_0)^i$
- Taylor series of $n \in \mathbb{Z}$ at p prime: $n = \sum_i b_i p^i$.

Definition

The p-adic expansion of a natural number n is the unique decomposition $n = \sum_i b_i p^i$ for $0 \leqslant b_i < p$.

- Taylor series of $q(x) = x^3 - 7x^2 + 15x - 9$ at $x = 3$: $q(x) = 2(x-3)^2 + (x-3)^3$
- $q(x) = (x-3)^2(2 + (x-3)) = (x-3)^2(x-1)$

Taylor series

- Taylor series of $q(x) \in \mathbb{C}[X]$ at $x = x_0$: $q(x) = \sum_i a_i (x - x_0)^i$
- Taylor series of $n \in \mathbb{Z}$ at p prime: $n = \sum_i b_i p^i$.

Definition

The p-adic expansion of a natural number n is the unique decomposition $n = \sum_i b_i p^i$ for $0 \leqslant b_i < p$.

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

Taylor series

- Taylor series of $q(x) \in \mathbb{C}[X]$ at $x = x_0$: $q(x) = \sum_i a_i (x - x_0)^i$
- Taylor series of $n \in \mathbb{Z}$ at p prime: $n = \sum_i b_i p^i$.

Definition

The p-adic expansion of a natural number n is the unique decomposition $n = \sum_i b_i p^i$ for $0 \leqslant b_i < p$.

- Taylor series of $q(x) = x^3 - 7x^2 + 15x - 9$ at $x = 3$: $q(x) = 2(x-3)^2 + (x-3)^3$
- $q(x) = (x-3)^2(2 + (x-3)) = (x-3)^2(x-1)$
- $x^3 - 7x^2 + 15x - 9$ has a root at 3 of order 2
- Taylor series/p-adic expansion of 72 at $p = 3$:

Taylor series

- Taylor series of $q(x) \in \mathbb{C}[X]$ at $x = x_0$: $q(x) = \sum_i a_i (x - x_0)^i$
- Taylor series of $n \in \mathbb{Z}$ at p prime: $n = \sum_i b_i p^i$.

Definition

The p-adic expansion of a natural number n is the unique decomposition $n = \sum_i b_i p^i$ for $0 \leqslant b_i < p$.

- Taylor series of $q(x) = x^3 - 7x^2 + 15x - 9$ at $x = 3$: $q(x) = 2(x-3)^2 + (x-3)^3$
- $q(x) = (x-3)^2(2 + (x-3)) = (x-3)^2(x-1)$
- $x^3 - 7x^2 + 15x - 9$ has a root at 3 of order 2
- Taylor series/p-adic expansion of 72 at $p = 3$: $72 = 0 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^3$

Taylor series

- Taylor series of $q(x) \in \mathbb{C}[X]$ at $x = x_0$: $q(x) = \sum_i a_i (x - x_0)^i$
- Taylor series of $n \in \mathbb{Z}$ at p prime: $n = \sum_i b_i p^i$.

Definition

The p-adic expansion of a natural number n is the unique decomposition $n = \sum_i b_i p^i$ for $0 \leqslant b_i < p$.

- Taylor series of $q(x) = x^3 - 7x^2 + 15x - 9$ at $x = 3$: $q(x) = 2(x-3)^2 + (x-3)^3$
- $q(x) = (x-3)^2(2 + (x-3)) = (x-3)^2(x-1)$
- $x^3 - 7x^2 + 15x - 9$ has a root at 3 of order 2
- Taylor series/p-adic expansion of 72 at $p = 3$: $72 = 0 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^3$
- $72 = 3^2 * (2 + 2 \cdot 3) = 3^2 * 2^3$

Taylor series

- Taylor series of $q(x) \in \mathbb{C}[X]$ at $x = x_0$: $q(x) = \sum_i a_i (x - x_0)^i$
- Taylor series of $n \in \mathbb{Z}$ at p prime: $n = \sum_i b_i p^i$.

Definition

The p-adic expansion of a natural number n is the unique decomposition $n = \sum_i b_i p^i$ for $0 \leqslant b_i < p$.

- Taylor series of $q(x) = x^3 - 7x^2 + 15x - 9$ at $x = 3$: $q(x) = 2(x-3)^2 + (x-3)^3$
- $q(x) = (x-3)^2(2 + (x-3)) = (x-3)^2(x-1)$
- $x^3 - 7x^2 + 15x - 9$ has a root at 3 of order 2
- Taylor series/p-adic expansion of 72 at $p = 3$: $72 = 0 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^3$
- $72 = 3^2 * (2 + 2 \cdot 3) = 3^2 * 2^3$
- 72 has a root at $p = 3$ of order 2

Taylor series

- Taylor series of $q(x) \in \mathbb{C}[X]$ at $x = x_0$: $q(x) = \sum_i a_i (x - x_0)^i$
- Taylor series of $n \in \mathbb{Z}$ at p prime: $n = \sum_i b_i p^i$.

Definition

The p-adic expansion of a natural number n is the unique decomposition $n = \sum_i b_i p^i$ for $0 \leqslant b_i < p$.

- Taylor series of $q(x) = x^3 - 7x^2 + 15x - 9$ at $x = 3$: $q(x) = 2(x-3)^2 + (x-3)^3$
- $q(x) = (x-3)^2(2 + (x-3)) = (x-3)^2(x-1)$
- $x^3 - 7x^2 + 15x - 9$ has a root at 3 of order 2
- Taylor series/p-adic expansion of 72 at $p = 3$: $72 = 0 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^3$
- $72 = 3^2 * (2 + 2 \cdot 3) = 3^2 * 2^3$
- 72 has a root at $p = 3$ of order 2

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

Extending to the negatives

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

Checking our math: $-1+1$

- $-1 \equiv 2 \cdot 3^0 + 2 \cdot 3^1 + 2 \cdot 3^2 + 2 \cdot 3^3 + \cdots$.

Checking our math: $-1+1$

- $-1 \equiv 2 \cdot 3^0 + 2 \cdot 3^1 + 2 \cdot 3^2 + 2 \cdot 3^3 + \cdots.$
- $-1 + 1 = \mathbf{1} + \mathbf{2} \cdot \mathbf{3^0} + +2 \cdot 3^1 + 2 \cdot 3^2 + 2 \cdot 3^3 + \cdots.$

Checking our math: $-1+1$

- $-1 \equiv 2\cdot 3^0 + 2\cdot 3^1 + 2\cdot 3^2 + 2\cdot 3^3 + \cdots.$
- $-1+1 = \mathbf{1} + \mathbf{2}\cdot\mathbf{3^0} + +2\cdot 3^1 + 2\cdot 3^2 + 2\cdot 3^3 + \cdots.$
- $-1+1 = \mathbf{1}\cdot\mathbf{3^1} + \mathbf{2}\cdot\mathbf{3^1} + 2\cdot 3^2 + 2\cdot 3^3 + \cdots.$

Checking our math: $-1+1$

- $-1 \equiv 2\cdot 3^0 + 2\cdot 3^1 + 2\cdot 3^2 + 2\cdot 3^3 + \cdots$.
- $-1+1 = \mathbf{1} + \mathbf{2}\cdot\mathbf{3^0} + +2\cdot 3^1 + 2\cdot 3^2 + 2\cdot 3^3 + \cdots$.
- $-1+1 = \mathbf{1}\cdot\mathbf{3^1} + \mathbf{2}\cdot\mathbf{3^1} + 2\cdot 3^2 + 2\cdot 3^3 + \cdots$.
- $-1+1 = \mathbf{1}\cdot\mathbf{3^2} + \mathbf{2}\cdot\mathbf{3^2} + 2\cdot 3^3 + \cdots$.

Checking our math: $-1+1$

- $-1 \equiv 2 \cdot 3^0 + 2 \cdot 3^1 + 2 \cdot 3^2 + 2 \cdot 3^3 + \cdots$.
- $-1+1 = \mathbf{1} + \mathbf{2} \cdot \mathbf{3^0} + +2 \cdot 3^1 + 2 \cdot 3^2 + 2 \cdot 3^3 + \cdots$.
- $-1+1 = \mathbf{1} \cdot \mathbf{3^1} + \mathbf{2} \cdot \mathbf{3^1} + 2 \cdot 3^2 + 2 \cdot 3^3 + \cdots$.
- $-1+1 = \mathbf{1} \cdot \mathbf{3^2} + \mathbf{2} \cdot \mathbf{3^2} + 2 \cdot 3^3 + \cdots$.
- $-1+1 = \mathbf{1} \cdot \mathbf{3^3} + \mathbf{2} \cdot \mathbf{3^3} + \cdots$.

Checking our math: $-1+1$

- $-1 \equiv 2 \cdot 3^0 + 2 \cdot 3^1 + 2 \cdot 3^2 + 2 \cdot 3^3 + \cdots$.
- $-1+1 = \mathbf{1} + \mathbf{2} \cdot \mathbf{3^0} + +2 \cdot 3^1 + 2 \cdot 3^2 + 2 \cdot 3^3 + \cdots$.
- $-1+1 = \mathbf{1} \cdot \mathbf{3^1} + \mathbf{2} \cdot \mathbf{3^1} + 2 \cdot 3^2 + 2 \cdot 3^3 + \cdots$.
- $-1+1 = \mathbf{1} \cdot \mathbf{3^2} + \mathbf{2} \cdot \mathbf{3^2} + 2 \cdot 3^3 + \cdots$.
- $-1+1 = \mathbf{1} \cdot \mathbf{3^3} + \mathbf{2} \cdot \mathbf{3^3} + \cdots$.
- $-1+1 = \cdots$

Checking our math: $-1+1$

- $-1 \equiv 2 \cdot 3^0 + 2 \cdot 3^1 + 2 \cdot 3^2 + 2 \cdot 3^3 + \cdots.$
- $-1+1 = \mathbf{1} + \mathbf{2} \cdot \mathbf{3^0} + +2 \cdot 3^1 + 2 \cdot 3^2 + 2 \cdot 3^3 + \cdots.$
- $-1+1 = \mathbf{1} \cdot \mathbf{3^1} + \mathbf{2} \cdot \mathbf{3^1} + 2 \cdot 3^2 + 2 \cdot 3^3 + \cdots.$
- $-1+1 = \mathbf{1} \cdot \mathbf{3^2} + \mathbf{2} \cdot \mathbf{3^2} + 2 \cdot 3^3 + \cdots.$
- $-1+1 = \mathbf{1} \cdot \mathbf{3^3} + \mathbf{2} \cdot \mathbf{3^3} + \cdots.$
- $-1+1 = \cdots$
- $-1+1 = 0.$

Positional notation

```
...22222
...00001 +
----------
...?????
----------
```

Positional notation

```
...22222
...00001 +
----------
...?????
----------
```

```
      1
...22222
...00001 +
----------
       0
----------
```

Positional notation

```
...22222
...00001 +
----------
...?????
----------
```

```
      1
...22222
...00001 +
----------
       0
----------
```

```
      1
...22222
...00001 +
----------
      00
----------
```

Positional notation

```
...22222
...00001 +
----------
...?????
----------
```

```
      1
...22222
...00001 +
----------
       0
----------
```

```
      1
...22222
...00001 +
----------
      00
----------
```

```
...22222
...00001 +
----------
...00000
----------
```

Positional notation

```
...22222
...00001 +
----------
...?????
----------
```

```
      1
...22222
...00001 +
----------
       0
----------
```

```
      1
...22222
...00001 +
----------
      00
----------
```

```
...22222
...00001 +
----------
...00000
----------
```

- What is -1 is 2 - adically?

Positional notation

```
...22222
...00001 +
----------
...?????
----------
```

```
       1
...22222
...00001 +
----------
       0
----------
```

```
       1
...22222
...00001 +
----------
      00
----------
```

```
...22222
...00001 +
----------
...00000
----------
```

- What is -1 is 2 - adically?
- $-1 = \ldots 11111.$

Positional notation

```
...22222
...00001 +
----------
...?????
----------
```

```
       1
...22222
...00001 +
----------
       0
----------
```

```
      1
...22222
...00001 +
----------
      00
----------
```

```
...22222
...00001 +
----------
...00000
----------
```

- What is -1 is 2 - adically?
- $-1 = \ldots 11111$.
- Same as 2's complement!

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.
- $1/4 = 1/(1+3) = 1 - 3 + 3^2 - 3^3 + 3^4 + \dots$

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!
- $3^2 = 3 \cdot 3$
- $1/4 = 1 - \mathbf{3} + \mathbf{3} \cdot \mathbf{3} - 3^3 + 3^4 + \cdots$

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!
- $3^2 = 3 \cdot 3$
- $1/4 = 1 - \mathbf{3} + \mathbf{3} \cdot \mathbf{3} - 3^3 + 3^4 + \cdots$
- $1/4 = 1 + \mathbf{2} \cdot \mathbf{3} - 3^3 + 3^4 + \cdots$

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!
- $3^2 = 3 \cdot 3$
- $1/4 = 1 \mathbf{-3} + \mathbf{3} \cdot \mathbf{3} - 3^3 + 3^4 + \cdots$
- $1/4 = 1 + \mathbf{2} \cdot \mathbf{3} - 3^3 + 3^4 + \cdots$
- $1/4 = 1 + 2 \cdot 3 \mathbf{-3^3} + \mathbf{3^4} + \cdots$

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!
- $3^2 = 3 \cdot 3$
- $1/4 = 1 \mathbf{-3} + \mathbf{3} \cdot \mathbf{3} - 3^3 + 3^4 + \cdots$
- $1/4 = 1 + \mathbf{2} \cdot \mathbf{3} - 3^3 + 3^4 + \cdots$
- $1/4 = 1 + 2 \cdot 3 \mathbf{-3^3} + \mathbf{3^4} + \cdots$
- $1/4 = 1 + 2 \cdot 3 \mathbf{-3^3} + \mathbf{3} \cdot \mathbf{3^3} + \cdots$

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!
- $3^2 = 3 \cdot 3$
- $1/4 = 1 \mathbf{-3} + \mathbf{3} \cdot \mathbf{3} - 3^3 + 3^4 + \cdots$
- $1/4 = 1 + \mathbf{2} \cdot \mathbf{3} - 3^3 + 3^4 + \cdots$
- $1/4 = 1 + 2 \cdot 3 \mathbf{-3^3} + \mathbf{3^4} + \cdots$
- $1/4 = 1 + 2 \cdot 3 \mathbf{-3^3} + \mathbf{3} \cdot \mathbf{3^3} + \cdots$
- $1/4 = 1 + 2 \cdot 3 + 2 \cdot 3^3 + \cdots$

Rationals

- Evaluate $1/4$ in the 3-adic system.
- $1/4 = 1/(1+3) = 1 - 3 + 3^2 - 3^3 + 3^4 + \ldots$
- What is -3? that's not allowed!
- $3^2 = 3 \cdot 3$
- $1/4 = 1 - \mathbf{3} + \mathbf{3} \cdot \mathbf{3} - 3^3 + 3^4 + \cdots$
- $1/4 = 1 + \mathbf{2} \cdot \mathbf{3} - 3^3 + 3^4 + \cdots$
- $1/4 = 1 + 2 \cdot 3 - \mathbf{3^3} + \mathbf{3^4} + \cdots$
- $1/4 = 1 + 2 \cdot 3 - \mathbf{3^3} + \mathbf{3} \cdot \mathbf{3^3} + \cdots$
- $1/4 = 1 + 2 \cdot 3 + 2 \cdot 3^3 + \cdots$
- $1/4 = 1 + 2 \cdot 3 + 2 \cdot 3^3 + 2 \cdot 3^5 + 2 \cdot 3^7 + \cdots$

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!
- $3^2 = 3 \cdot 3$
- $1/4 = 1 - \mathbf{3} + \mathbf{3} \cdot \mathbf{3} - 3^3 + 3^4 + \cdots$
- $1/4 = 1 + \mathbf{2} \cdot \mathbf{3} - 3^3 + 3^4 + \cdots$
- $1/4 = 1 + 2 \cdot 3 - \mathbf{3^3} + \mathbf{3^4} + \cdots$
- $1/4 = 1 + 2 \cdot 3 - \mathbf{3^3} + \mathbf{3} \cdot \mathbf{3^3} + \cdots$
- $1/4 = 1 + 2 \cdot 3 + 2 \cdot 3^3 + \cdots$
- $1/4 = 1 + 2 \cdot 3 + 2 \cdot 3^3 + 2 \cdot 3^5 + 2 \cdot 3^7 + \cdots$
- Similar cleverness produces $1/p$ for any rational.

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!
- $3^2 = 3 \cdot 3$
- $1/4 = 1 \mathbf{-3} + \mathbf{3} \cdot \mathbf{3} - 3^3 + 3^4 + \cdots$
- $1/4 = 1 + \mathbf{2} \cdot \mathbf{3} - 3^3 + 3^4 + \cdots$
- $1/4 = 1 + 2 \cdot 3 \mathbf{-3^3} + \mathbf{3^4} + \cdots$
- $1/4 = 1 + 2 \cdot 3 \mathbf{-3^3} + \mathbf{3} \cdot \mathbf{3^3} + \cdots$
- $1/4 = 1 + 2 \cdot 3 + 2 \cdot 3^3 + \cdots$
- $1/4 = 1 + 2 \cdot 3 + 2 \cdot 3^3 + 2 \cdot 3^5 + 2 \cdot 3^7 + \cdots$
- Similar cleverness produces $1/p$ for any rational.

A step back

- Let $x = a_0 + a_1 p + a_2 p^2 + \dots$

A step back

- Let $x = a_0 + a_1 p + a_2 p^2 + \dots$
- $x \equiv a_0 \pmod{p}$

A step back

- Let $x = a_0 + a_1 p + a_2 p^2 + \dots$
- $x \equiv a_0 \pmod{p}$
- $x \equiv a_0 + a_1 p \pmod{p^2}$

A step back

- Let $x = a_0 + a_1 p + a_2 p^2 + \dots$
- $x \equiv a_0 \pmod{p}$
- $x \equiv a_0 + a_1 p \pmod{p^2}$
- $x - a_0 \equiv a_1 p \pmod{p^2}$

A step back

- Let $x = a_0 + a_1 p + a_2 p^2 + \dots$
- $x \equiv a_0 \pmod{p}$
- $x \equiv a_0 + a_1 p \pmod{p^2}$
- $x - a_0 \equiv a_1 p \pmod{p^2}$
- $x \equiv a_0 + a_1 p + a_2 p^2 \pmod{p^3}$

A step back

- Let $x = a_0 + a_1 p + a_2 p^2 + \dots$
- $x \equiv a_0 \pmod{p}$
- $x \equiv a_0 + a_1 p \pmod{p^2}$
- $x - a_0 \equiv a_1 p \pmod{p^2}$
- $x \equiv a_0 + a_1 p + a_2 p^2 \pmod{p^3}$
- $x - a_0 - a_1 p \equiv a_2 p^2 \pmod{p^3}$

A step back

- Let $-1 = \sum_i a_i 3^i$

- Let $x = a_0 + a_1 p + a_2 p^2 + \dots$
- $x \equiv a_0 \pmod{p}$
- $x \equiv a_0 + a_1 p \pmod{p^2}$
- $x - a_0 \equiv a_1 p \pmod{p^2}$
- $x \equiv a_0 + a_1 p + a_2 p^2 \pmod{p^3}$
- $x - a_0 - a_1 p \equiv a_2 p^2 \pmod{p^3}$

A step back

- **Let** $-1 = \sum_i a_i 3^i$
- **Let** $-1 = a_0 \pmod 3$

- Let $x = a_0 + a_1 p + a_2 p^2 + \dots$
- $x \equiv a_0 \pmod p$
- $x \equiv a_0 + a_1 p \pmod {p^2}$
- $x - a_0 \equiv a_1 p \pmod {p^2}$
- $x \equiv a_0 + a_1 p + a_2 p^2 \pmod {p^3}$
- $x - a_0 - a_1 p \equiv a_2 p^2 \pmod {p^3}$

A step back

- Let $-1 = \sum_i a_i 3^i$
- Let $-1 = a_0 \pmod 3$; $a_0 = 2 \pmod 3$

- Let $x = a_0 + a_1 p + a_2 p^2 + \dots$
- $x \equiv a_0 \pmod p$
- $x \equiv a_0 + a_1 p \pmod {p^2}$
- $x - a_0 \equiv a_1 p \pmod {p^2}$
- $x \equiv a_0 + a_1 p + a_2 p^2 \pmod {p^3}$
- $x - a_0 - a_1 p \equiv a_2 p^2 \pmod {p^3}$

A step back

- Let $-1 = \sum_i a_i 3^i$
- Let $-1 = a_0 \pmod 3$; $a_0 = 2 \pmod 3$
- Let $-1 = 2 + a_1 \cdot 3 \pmod 9$;

- Let $x = a_0 + a_1 p + a_2 p^2 + \dots$
- $x \equiv a_0 \pmod p$
- $x \equiv a_0 + a_1 p \pmod{p^2}$
- $x - a_0 \equiv a_1 p \pmod{p^2}$
- $x \equiv a_0 + a_1 p + a_2 p^2 \pmod{p^3}$
- $x - a_0 - a_1 p \equiv a_2 p^2 \pmod{p^3}$

A step back

- Let $-1 = \sum_i a_i 3^i$
- Let $-1 = a_0 \pmod 3$; $a_0 = 2 \pmod 3$
- Let $-1 = 2 + a_1 \cdot 3 \pmod 9$;
  $-3 = a_1 \cdot 3 \pmod 9$;

- Let $x = a_0 + a_1 p + a_2 p^2 + \dots$
- $x \equiv a_0 \pmod p$
- $x \equiv a_0 + a_1 p \pmod{p^2}$
- $x - a_0 \equiv a_1 p \pmod{p^2}$
- $x \equiv a_0 + a_1 p + a_2 p^2 \pmod{p^3}$
- $x - a_0 - a_1 p \equiv a_2 p^2 \pmod{p^3}$

A step back

- Let $x = a_0 + a_1 p + a_2 p^2 + \dots$
- $x \equiv a_0 \pmod{p}$
- $x \equiv a_0 + a_1 p \pmod{p^2}$
- $x - a_0 \equiv a_1 p \pmod{p^2}$
- $x \equiv a_0 + a_1 p + a_2 p^2 \pmod{p^3}$
- $x - a_0 - a_1 p \equiv a_2 p^2 \pmod{p^3}$

- Let $-1 = \sum_i a_i 3^i$
- Let $-1 = a_0 \pmod{3}$; $a_0 = 2 \pmod{3}$
- Let $-1 = 2 + a_1 \cdot 3 \pmod{9}$; $-3 = a_1 \cdot 3 \pmod{9}$; $6 = a_1 \cdot 3 \pmod{9}$;

A step back

- Let $x = a_0 + a_1 p + a_2 p^2 + \dots$
- $x \equiv a_0 \pmod{p}$
- $x \equiv a_0 + a_1 p \pmod{p^2}$
- $x - a_0 \equiv a_1 p \pmod{p^2}$
- $x \equiv a_0 + a_1 p + a_2 p^2 \pmod{p^3}$
- $x - a_0 - a_1 p \equiv a_2 p^2 \pmod{p^3}$

- Let $-1 = \sum_i a_i 3^i$
- Let $-1 = a_0 \pmod{3}$; $a_0 = 2 \pmod{3}$
- Let $-1 = 2 + a_1 \cdot 3 \pmod{9}$; $-3 = a_1 \cdot 3 \pmod{9}$; $6 = a_1 \cdot 3 \pmod{9}$; $a_1 = 2$
- Let $-1 = 2 + 2 \cdot 3 + 2 \cdot 3^2 + \dots$

- Let $1/4 = \sum_i a_i 3^i$

A step back

- Let $x = a_0 + a_1 p + a_2 p^2 + \dots$
- $x \equiv a_0 \pmod{p}$
- $x \equiv a_0 + a_1 p \pmod{p^2}$
- $x - a_0 \equiv a_1 p \pmod{p^2}$
- $x \equiv a_0 + a_1 p + a_2 p^2 \pmod{p^3}$
- $x - a_0 - a_1 p \equiv a_2 p^2 \pmod{p^3}$

- Let $-1 = \sum_i a_i 3^i$
- Let $-1 = a_0 \pmod{3}$; $a_0 = 2 \pmod{3}$
- Let $-1 = 2 + a_1 \cdot 3 \pmod{9}$;
  $-3 = a_1 \cdot 3 \pmod{9}$; $6 = a_1 \cdot 3 \pmod{9}$;
  $a_1 = 2$
- Let $-1 = 2 + 2 \cdot 3 + 2 \cdot 3^2 + \dots$

- Let $1/4 = \sum_i a_i 3^i$
- What defines $1/4$?

A step back

- Let $x = a_0 + a_1 p + a_2 p^2 + \dots$
- $x \equiv a_0 \pmod{p}$
- $x \equiv a_0 + a_1 p \pmod{p^2}$
- $x - a_0 \equiv a_1 p \pmod{p^2}$
- $x \equiv a_0 + a_1 p + a_2 p^2 \pmod{p^3}$
- $x - a_0 - a_1 p \equiv a_2 p^2 \pmod{p^3}$

- Let $-1 = \sum_i a_i 3^i$
- Let $-1 = a_0 \pmod{3}$; $a_0 = 2 \pmod{3}$
- Let $-1 = 2 + a_1 \cdot 3 \pmod{9}$; $-3 = a_1 \cdot 3 \pmod{9}$; $6 = a_1 \cdot 3 \pmod{9}$; $a_1 = 2$
- Let $-1 = 2 + 2 \cdot 3 + 2 \cdot 3^2 + \dots$

- Let $1/4 = \sum_i a_i 3^i$
- What defines $1/4$? The equation $1/4 \cdot 4 = 1$.

A step back

- Let $x = a_0 + a_1 p + a_2 p^2 + \dots$
- $x \equiv a_0 \pmod{p}$
- $x \equiv a_0 + a_1 p \pmod{p^2}$
- $x - a_0 \equiv a_1 p \pmod{p^2}$
- $x \equiv a_0 + a_1 p + a_2 p^2 \pmod{p^3}$
- $x - a_0 - a_1 p \equiv a_2 p^2 \pmod{p^3}$

- Let $-1 = \sum_i a_i 3^i$
- Let $-1 = a_0 \pmod 3$; $a_0 = 2 \pmod 3$
- Let $-1 = 2 + a_1 \cdot 3 \pmod 9$;
  $-3 = a_1 \cdot 3 \pmod 9$; $6 = a_1 \cdot 3 \pmod 9$;
  $a_1 = 2$
- Let $-1 = 2 + 2 \cdot 3 + 2 \cdot 3^2 + \dots$

- Let $1/4 = \sum_i a_i 3^i$
- What defines $1/4$? The equation $1/4 \cdot 4 = 1$.
- $(a_0 + 3a_1 + 9a_2 + \dots)(1 + 3 + 0 \cdot 9 + \cdots) = 1$

A step back

- Let $x = a_0 + a_1 p + a_2 p^2 + \dots$
- $x \equiv a_0 \pmod{p}$
- $x \equiv a_0 + a_1 p \pmod{p^2}$
- $x - a_0 \equiv a_1 p \pmod{p^2}$
- $x \equiv a_0 + a_1 p + a_2 p^2 \pmod{p^3}$
- $x - a_0 - a_1 p \equiv a_2 p^2 \pmod{p^3}$

- Let $-1 = \sum_i a_i 3^i$
- Let $-1 = a_0 \pmod{3}$; $a_0 = 2 \pmod{3}$
- Let $-1 = 2 + a_1 \cdot 3 \pmod{9}$; $-3 = a_1 \cdot 3 \pmod{9}$; $6 = a_1 \cdot 3 \pmod{9}$; $a_1 = 2$
- Let $-1 = 2 + 2 \cdot 3 + 2 \cdot 3^2 + \dots$

- Let $1/4 = \sum_i a_i 3^i$
- What defines $1/4$? The equation $1/4 \cdot 4 = 1$.
- $(a_0 + 3a_1 + 9a_2 + \dots)(1 + 3 + 0 \cdot 9 + \cdots) = 1$
- $a_0 \cdot 1 \equiv 1 \pmod{3}$

A step back

- Let $x = a_0 + a_1 p + a_2 p^2 + \dots$
- $x \equiv a_0 \pmod{p}$
- $x \equiv a_0 + a_1 p \pmod{p^2}$
- $x - a_0 \equiv a_1 p \pmod{p^2}$
- $x \equiv a_0 + a_1 p + a_2 p^2 \pmod{p^3}$
- $x - a_0 - a_1 p \equiv a_2 p^2 \pmod{p^3}$

- Let $-1 = \sum_i a_i 3^i$
- Let $-1 = a_0 \pmod{3}$; $a_0 = 2 \pmod{3}$
- Let $-1 = 2 + a_1 \cdot 3 \pmod{9}$;
  $-3 = a_1 \cdot 3 \pmod{9}$; $6 = a_1 \cdot 3 \pmod{9}$;
  $a_1 = 2$
- Let $-1 = 2 + 2 \cdot 3 + 2 \cdot 3^2 + \dots$

- Let $1/4 = \sum_i a_i 3^i$
- What defines $1/4$? The equation $1/4 \cdot 4 = 1$.
- $(a_0 + 3a_1 + 9a_2 + \dots)(1 + 3 + 0 \cdot 9 + \cdots) = 1$
- $a_0 \cdot 1 \equiv 1 \pmod{3} a_0 = 1$.

A step back

- Let $x = a_0 + a_1 p + a_2 p^2 + \dots$
- $x \equiv a_0 \pmod{p}$
- $x \equiv a_0 + a_1 p \pmod{p^2}$
- $x - a_0 \equiv a_1 p \pmod{p^2}$
- $x \equiv a_0 + a_1 p + a_2 p^2 \pmod{p^3}$
- $x - a_0 - a_1 p \equiv a_2 p^2 \pmod{p^3}$

- Let $-1 = \sum_i a_i 3^i$
- Let $-1 = a_0 \pmod{3}$; $a_0 = 2 \pmod{3}$
- Let $-1 = 2 + a_1 \cdot 3 \pmod{9}$;
  $-3 = a_1 \cdot 3 \pmod{9}$; $6 = a_1 \cdot 3 \pmod{9}$;
  $a_1 = 2$
- Let $-1 = 2 + 2 \cdot 3 + 2 \cdot 3^2 + \dots$

- Let $1/4 = \sum_i a_i 3^i$
- What defines $1/4$? The equation $1/4 \cdot 4 = 1$.
- $(a_0 + 3a_1 + 9a_2 + \dots)(1 + 3 + 0 \cdot 9 + \cdots) = 1$
- $a_0 \cdot 1 \equiv 1 \pmod{3} a_0 = 1$.
- $(1 + 3a_1)(1 + 3) \equiv 1 \pmod{9}$

A step back

- Let $x = a_0 + a_1 p + a_2 p^2 + \dots$
- $x \equiv a_0 \pmod{p}$
- $x \equiv a_0 + a_1 p \pmod{p^2}$
- $x - a_0 \equiv a_1 p \pmod{p^2}$
- $x \equiv a_0 + a_1 p + a_2 p^2 \pmod{p^3}$
- $x - a_0 - a_1 p \equiv a_2 p^2 \pmod{p^3}$

- Let $-1 = \sum_i a_i 3^i$
- Let $-1 = a_0 \pmod{3}$; $a_0 = 2 \pmod{3}$
- Let $-1 = 2 + a_1 \cdot 3 \pmod{9}$; $-3 = a_1 \cdot 3 \pmod{9}$; $6 = a_1 \cdot 3 \pmod{9}$; $a_1 = 2$
- Let $-1 = 2 + 2 \cdot 3 + 2 \cdot 3^2 + \dots$

- Let $1/4 = \sum_i a_i 3^i$
- What defines $1/4$? The equation $1/4 \cdot 4 = 1$.
- $(a_0 + 3a_1 + 9a_2 + \dots)(1 + 3 + 0 \cdot 9 + \cdots) = 1$
- $a_0 \cdot 1 \equiv 1 \pmod{3} a_0 = 1$.
- $(1 + 3a_1)(1 + 3) \equiv 1 \pmod{9} 4 + 12a_1 \equiv 1 \pmod{9}$

A step back

- Let $x = a_0 + a_1 p + a_2 p^2 + \dots$
- $x \equiv a_0 \pmod{p}$
- $x \equiv a_0 + a_1 p \pmod{p^2}$
- $x - a_0 \equiv a_1 p \pmod{p^2}$
- $x \equiv a_0 + a_1 p + a_2 p^2 \pmod{p^3}$
- $x - a_0 - a_1 p \equiv a_2 p^2 \pmod{p^3}$

- Let $-1 = \sum_i a_i 3^i$
- Let $-1 = a_0 \pmod{3}$; $a_0 = 2 \pmod{3}$
- Let $-1 = 2 + a_1 \cdot 3 \pmod{9}$; $-3 = a_1 \cdot 3 \pmod{9}$; $6 = a_1 \cdot 3 \pmod{9}$; $a_1 = 2$
- Let $-1 = 2 + 2 \cdot 3 + 2 \cdot 3^2 + \dots$

- Let $1/4 = \sum_i a_i 3^i$
- What defines $1/4$? The equation $1/4 \cdot 4 = 1$.
- $(a_0 + 3a_1 + 9a_2 + \dots)(1 + 3 + 0 \cdot 9 + \cdots) = 1$
- $a_0 \cdot 1 \equiv 1 \pmod{3} a_0 = 1$.
- $(1 + 3a_1)(1 + 3) \equiv 1 \pmod{9} 4 + 12a_1 \equiv 1 \pmod{9}$
- $3a_1 \equiv -3 \equiv 6 \pmod{9}$

A step back

- Let $x = a_0 + a_1 p + a_2 p^2 + \dots$
- $x \equiv a_0 \pmod{p}$
- $x \equiv a_0 + a_1 p \pmod{p^2}$
- $x - a_0 \equiv a_1 p \pmod{p^2}$
- $x \equiv a_0 + a_1 p + a_2 p^2 \pmod{p^3}$
- $x - a_0 - a_1 p \equiv a_2 p^2 \pmod{p^3}$

- Let $-1 = \sum_i a_i 3^i$
- Let $-1 = a_0 \pmod{3}$; $a_0 = 2 \pmod{3}$
- Let $-1 = 2 + a_1 \cdot 3 \pmod{9}$; $-3 = a_1 \cdot 3 \pmod{9}$; $6 = a_1 \cdot 3 \pmod{9}$; $a_1 = 2$
- Let $-1 = 2 + 2 \cdot 3 + 2 \cdot 3^2 + \dots$

- Let $1/4 = \sum_i a_i 3^i$
- What defines $1/4$? The equation $1/4 \cdot 4 = 1$.
- $(a_0 + 3a_1 + 9a_2 + \dots)(1 + 3 + 0 \cdot 9 + \cdots) = 1$
- $a_0 \cdot 1 \equiv 1 \pmod{3} a_0 = 1.$
- $(1 + 3a_1)(1 + 3) \equiv 1 \pmod{9} 4 + 12a_1 \equiv 1 \pmod{9}$
- $3a_1 \equiv -3 \equiv 6 \pmod{9}$
- $a_1 \equiv 2 \pmod{9}$

A step back

- Let $x = a_0 + a_1 p + a_2 p^2 + \dots$
- $x \equiv a_0 \pmod{p}$
- $x \equiv a_0 + a_1 p \pmod{p^2}$
- $x - a_0 \equiv a_1 p \pmod{p^2}$
- $x \equiv a_0 + a_1 p + a_2 p^2 \pmod{p^3}$
- $x - a_0 - a_1 p \equiv a_2 p^2 \pmod{p^3}$

- Let $-1 = \sum_i a_i 3^i$
- Let $-1 = a_0 \pmod{3}$; $a_0 = 2 \pmod{3}$
- Let $-1 = 2 + a_1 \cdot 3 \pmod{9}$; $-3 = a_1 \cdot 3 \pmod{9}$; $6 = a_1 \cdot 3 \pmod{9}$; $a_1 = 2$
- Let $-1 = 2 + 2 \cdot 3 + 2 \cdot 3^2 + \dots$

- Let $1/4 = \sum_i a_i 3^i$
- What defines $1/4$? The equation $1/4 \cdot 4 = 1$.
- $(a_0 + 3a_1 + 9a_2 + \dots)(1 + 3 + 0 \cdot 9 + \cdots) = 1$
- $a_0 \cdot 1 \equiv 1 \pmod{3} a_0 = 1$.
- $(1 + 3a_1)(1 + 3) \equiv 1 \pmod{9} 4 + 12a_1 \equiv 1 \pmod{9}$
- $3a_1 \equiv -3 \equiv 6 \pmod{9}$
- $a_1 \equiv 2 \pmod{9}$
- $1/4 = 1 + 2 \cdot 3 + 2 \cdot 3^3 + \dots$

Irrationals

- Let's solve $X^2 = 2$ in the $7-$adics.

Irrationals

- Let's solve $X^2 = 2$ in the $7-$adics.
- Such a solution does not "really exist" in the rationals or the integers.

Irrationals

- Let's solve $X^2 = 2$ in the $7-$adics.
- Such a solution does not "really exist" in the rationals or the integers.
- Start with $X \equiv 3 \pmod{} 7$, $X \equiv 4 \equiv -3 \pmod{7}$.

Convergence

- Intuition: higher powers of p should become “smaller” for convergence!

Convergence

- Intuition: higher powers of p should become "smaller" for convergence!
- $|a|_p = p^{-1 \cdot \text{highest power of } p \text{ which divides } a}$

Convergence

- Intuition: higher powers of p should become "smaller" for convergence!
- $|a|_p = p^{-1 \cdot \text{highest power of } p \text{ which divides } a}$
- $|10|_3 = 3^{-0} = 1$

Convergence

- Intuition: higher powers of p should become "smaller" for convergence!
- $|a|_p = p^{-1 \cdot \text{highest power of } p \text{ which divides } a}$
- $|10|_3 = 3^{-0} = 1$
- $|3|_3 = 3^{-1} = 1/3$

Convergence

- Intuition: higher powers of p should become "smaller" for convergence!
- $|a|_p = p^{-1 \cdot \text{highest power of } p \text{ which divides } a}$
- $|10|_3 = 3^{-0} = 1$
- $|3|_3 = 3^{-1} = 1/3$
- $|9|_3 = 3^{-2} = 1/9$

Convergence

- Intuition: higher powers of p should become "smaller" for convergence!
- $|a|_p = p^{-1 \cdot \text{highest power of } p \text{ which divides } a}$
- $|10|_3 = 3^{-0} = 1$
- $|3|_3 = 3^{-1} = 1/3$
- $|9|_3 = 3^{-2} = 1/9$
- $|90|_3 = 3^{-2} = 1/9$

Convergence

- Intuition: higher powers of p should become “smaller” for convergence!
- $|a|_p = p^{-1 \cdot \text{highest power of } p \text{ which divides } a}$
- $|10|_3 = 3^{-0} = 1$
- $|3|_3 = 3^{-1} = 1/3$
- $|9|_3 = 3^{-2} = 1/9$
- $|90|_3 = 3^{-2} = 1/9$
- $|27|_3 = 3^{-3} = 1/27$

Convergence

- Intuition: higher powers of p should become "smaller" for convergence!
- $|a|_p = p^{-1 \cdot \text{highest power of } p \text{ which divides } a}$
- $|10|_3 = 3^{-0} = 1$
- $|3|_3 = 3^{-1} = 1/3$
- $|9|_3 = 3^{-2} = 1/9$
- $|90|_3 = 3^{-2} = 1/9$
- $|27|_3 = 3^{-3} = 1/27$
- $|a + b|_p \leqslant |a|_p + |b|_p$?

Convergence

- Intuition: higher powers of p should become "smaller" for convergence!
- $|a|_p = p^{-1 \cdot \text{highest power of } p \text{ which divides } a}$
- $|10|_3 = 3^{-0} = 1$
- $|3|_3 = 3^{-1} = 1/3$
- $|9|_3 = 3^{-2} = 1/9$
- $|90|_3 = 3^{-2} = 1/9$
- $|27|_3 = 3^{-3} = 1/27$
- $|a + b|_p \leqslant |a|_p + |b|_p$?

Scam v/s non-scam

- Solve $x = 1 + 3x$

Scam v/s non-scam

- Solve $x = 1 + 3x$
- **Non scam**:$-2x = 1$

Scam v/s non-scam

- Solve $x = 1 + 3x$
- **Non scam**:$-2x = 1$; $x = -1/2$
- $x_0 = 1$

Scam v/s non-scam

- Solve $x = 1 + 3x$
- **Non scam**:$-2x = 1$; $x = -1/2$
- $x_0 = 1$
- $x_1 = 1 + 3$
- $x_2 = 1 + 3x_1 = 1 + 3(1 + 3) = 1 + 3 + 3^2$

Scam v/s non-scam

- Solve $x = 1 + 3x$
- **Non scam**:$-2x = 1$; $x = -1/2$
- $x_0 = 1$
- $x_1 = 1 + 3$
- $x_2 = 1 + 3x_1 = 1 + 3(1 + 3) = 1 + 3 + 3^2$
- $x_i = 1 + 3 + 3^2 + \cdots + 3^i$

Scam v/s non-scam

- Solve $x = 1 + 3x$
- **Non scam**:$-2x = 1$; $x = -1/2$
- $x_0 = 1$
- $x_1 = 1 + 3$
- $x_2 = 1 + 3x_1 = 1 + 3(1 + 3) = 1 + 3 + 3^2$
- $x_i = 1 + 3 + 3^2 + \cdots + 3^i$
- $x_\infty = 1/(1 - 3) = -1/2$
- Converges? We need $|3| < 1$

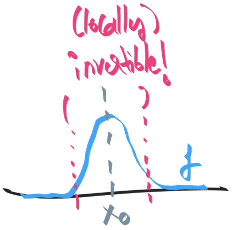
Scam v/s non-scam

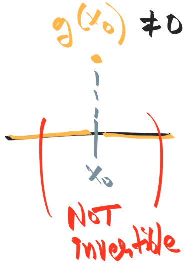
- Solve $x = 1 + 3x$
- **Non scam**:$-2x = 1$; $x = -1/2$
- $x_0 = 1$
- $x_1 = 1 + 3$
- $x_2 = 1 + 3x_1 = 1 + 3(1 + 3) = 1 + 3 + 3^2$
- $x_i = 1 + 3 + 3^2 + \cdots + 3^i$
- $x_\infty = 1/(1 - 3) = -1/2$
- Converges? We need $|3| < 1$
- But it is! $|3|_3 < 1$

Scam v/s non-scam

- Solve $x = 1 + 3x$
- **Non scam**:$-2x = 1$; $x = -1/2$
- $x_0 = 1$
- $x_1 = 1 + 3$
- $x_2 = 1 + 3x_1 = 1 + 3(1 + 3) = 1 + 3 + 3^2$
- $x_i = 1 + 3 + 3^2 + \cdots + 3^i$
- $x_\infty = 1/(1 - 3) = -1/2$
- Converges? We need $|3| < 1$
- But it is! $|3|_3 < 1$

Why only primes? Geometry of functions

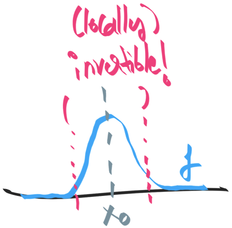




$f(x_0) \neq 0 \Rightarrow f$ invertible (locally)

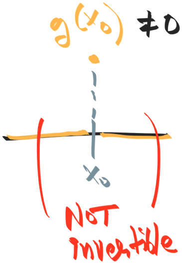
$f \,\%\, (x - x_0) \neq 0 \Rightarrow f$ invertible (locally)

Why only primes? Geometry of functions



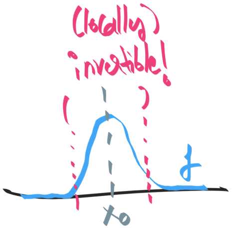
$f(x_0) \neq 0 \Rightarrow f$ invertible (locally)

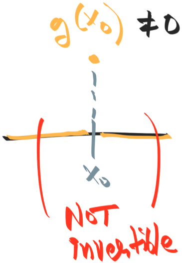
$f \,\%\, (x - x_0) \neq 0 \Rightarrow f$ invertible (locally)



- $f(x)$: continuous, *non-zero* at $x = x_0$.

Why only primes? Geometry of functions



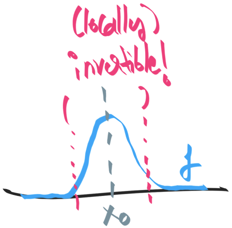


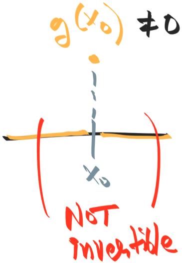
$f(x_0) \neq 0 \Rightarrow f$ invertible (locally)

$f \,\%\, (x - x_0) \neq 0 \Rightarrow f$ invertible (locally)

- $f(x)$: continuous, *non-zero* at $x = x_0$.
- $f(x)$: *locally invertible* at $x = x_0$.

Why only primes? Geometry of functions



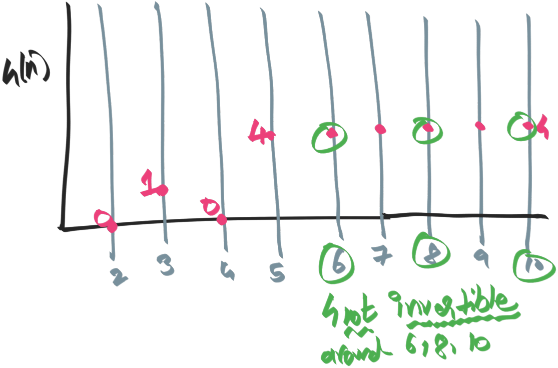


$f(x_0) \neq 0 \Rightarrow f$ invertible (locally)

$f \,\%\, (x - x_0) \neq 0 \Rightarrow f$ invertible (locally)

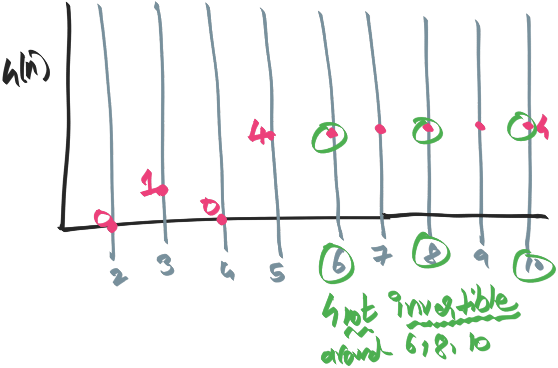
- $f(x)$: continuous, *non-zero* at $x = x_0$.
- $f(x)$: *locally invertible* at $x = x_0$.

Why only primes? Geometry of numbers



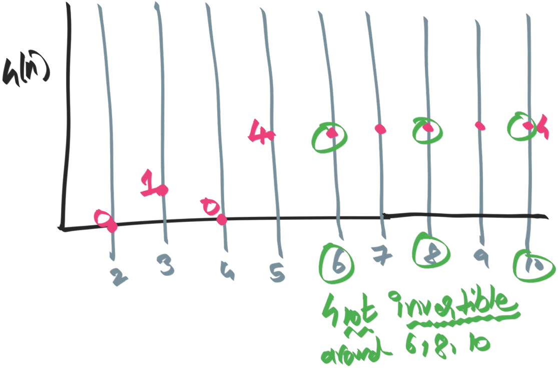
- consider 4.

Why only primes? Geometry of numbers



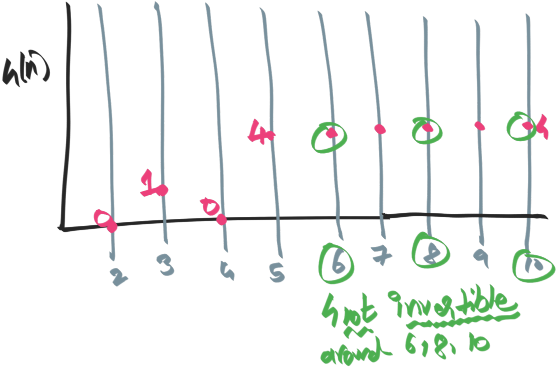
- consider 4.
- nonzero at $a_0 = 6$: $4 \simeq 4 \pmod 6$

Why only primes? Geometry of numbers



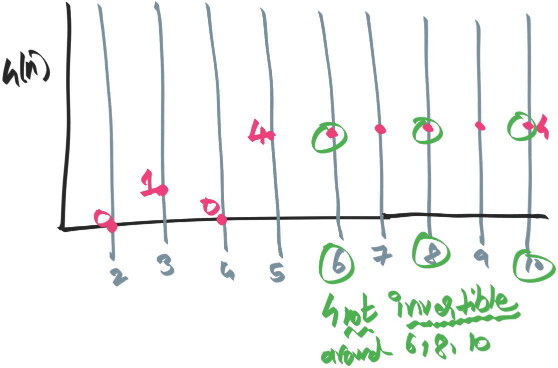
- consider 4.
- nonzero at $a_0 = 6$: $4 \simeq 4 \pmod 6$
- *not invertible* modulo 6:
  $[0, 1, 2, 3, 4, 5] \times 4 \equiv [0, 4, 8, 12, 16, 20] \equiv [0, 4, 2, 0, 4, 2] \pmod 6$

Why only primes? Geometry of numbers



- consider 4.
- nonzero at $a_0 = 6$: $4 \simeq 4 \pmod{6}$
- *not invertible* modulo 6: $[0,1,2,3,4,5] \times 4 \equiv [0,4,8,12,16,20] \equiv [0,4,2,0,4,2] \pmod{6}$
- If we want 4 to be a *continuous* function

Why only primes? Geometry of numbers



- consider 4.
- nonzero at $a_0 = 6$: $4 \simeq 4 \pmod 6$
- *not invertible* modulo 6:
  $[0, 1, 2, 3, 4, 5] \times 4 \equiv [0, 4, 8, 12, 16, 20] \equiv [0, 4, 2, 0, 4, 2] \pmod 6$
- If we want 4 to be a *continuous* function
- then 6 should not be a point!