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"

Why p-adics?

Analogy between:

- $\mathbb{Z}$, where $3, 5, 7, \ldots$ are the "primes"
- $\mathbb{C}[X]$, where $(x - a)$ are the "primes"
- $\mathbb{C}[X]$ has evaluation, taylor series. Can we access that in $\mathbb{Z}$?

What is factorization?

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

What is factorization?

Remainder when factoring $p(x) = x^3 + x^2 + x + 1$ 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 factorization?

Remainder when factoring $p(x) = x^3 + x^2 + x + 1$ 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 factorization?

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

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

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

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

What is factorization?

Remainder when factoring $p(x) = x^3 + x^2 + x + 1$ 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 $q(x) = (x - 1)$

What is factorization?

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

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

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

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

What is factorization?

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

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

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

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

What is factorization?

Remainder when factoring $p(x) = x^3 + x^2 + x + 1$ 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 $x = 1$

What is factorization?

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

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

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

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

What is factorization?

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

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

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

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

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 $\mathbb{Z}$?

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 $\mathbb{Z}$?

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 $(x - a)$

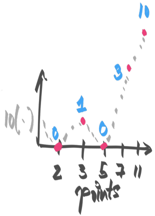
- $10(2) =$ remainder of 10 when factored by 2; $10 = 2 \cdot 5 + 0$; $10(2) = 0$
- $10(3) =$ remainder of 10 when factored by 3; $10 = 3 \cdot 3 + 1$; $10(3) = 1$
- $10(5) =$ remainder of 10 when factored by 5; $10 = 5 \cdot 2 + 0$; $10(5) = 0$
- $10(7) =$ remainder of 10 when factored by 7; $10 = 7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

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: $\mathbb{R}[X]$ factored by 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: $\mathbb{R}[X]$ factored by 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: $\mathbb{R}[X]$ factored by 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: $\mathbb{R}[X]$ factored by 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: $\mathbb{R}[X]$ factored by 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: $\mathbb{R}[X]$ factored by 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: $\mathbb{R}[X]$ factored by 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: $\mathbb{R}[X]$ factored by 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: $(a + xb) \cdot (c + xd) = ac + x(ad + bc) + bdx^2$
- factoring product by $q(x) = x^2 + 1$:

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

Cheap trick?

- What are the complex numbers?
- $\mathbb{R}$ with i: $i^2 = -1$. That is, $i^2 + 1 = 0$.
- Equivalently: $\mathbb{R}[X]$ factored by 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: $(a + xb) \cdot (c + xd) = ac + x(ad + bc) + bdx^2$
- factoring product by $q(x) = x^2 + 1$:

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

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: $-1+1$

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

Checking our math: $-1+1$

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

Checking our math: $-1+1$

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

Checking our math: $-1+1$

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

Checking our math: $-1+1$

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

Checking our math: $-1+1$

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

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

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

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

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

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

Rationals

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

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!
- $3^2 = 3 \cdot 3$
- $1/4 = 1 - 3 + 3 \cdot 3 - 3^3 + 3^4 + \cdots$
- $1/4 = 1 + 2 \cdot 3 - 3^3 + 3^4 + \cdots$
- $1/4 = 1 + 2 \cdot 3 - 3^3 + 3^4 + \cdots$
- $1/4 = 1 + 2 \cdot 3 - 3^3 + 3 \cdot 3^3 + \cdots$
- $1/4 = 1 + 2 \cdot 3 + 2 \cdot 3^3 + \cdots$
- $1/4 = 1 + 2 \cdot 3 + 2 \cdot 3^3 + 2 \cdot 3^5 + 2 \cdot 3^7 + \cdots$
- 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!
- $3^2 = 3 \cdot 3$
- $1/4 = 1 - 3 + 3 \cdot 3 - 3^3 + 3^4 + \cdots$
- $1/4 = 1 + 2 \cdot 3 - 3^3 + 3^4 + \cdots$
- $1/4 = 1 + 2 \cdot 3 - 3^3 + 3^4 + \cdots$
- $1/4 = 1 + 2 \cdot 3 - 3^3 + 3 \cdot 3^3 + \cdots$
- $1/4 = 1 + 2 \cdot 3 + 2 \cdot 3^3 + \cdots$
- $1/4 = 1 + 2 \cdot 3 + 2 \cdot 3^3 + 2 \cdot 3^5 + 2 \cdot 3^7 + \cdots$
- 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 $-1 = a_{\mathbf{0}} \pmod 3$; $a_{\mathbf{0}} = 2 \pmod 3$
- Let $-1 = 2 + a_{\mathbf{1}} \cdot 3 \pmod 9$;
  $-3 = a_{\mathbf{1}} \cdot 3 \pmod 9$;

- 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 $-1 = a_{\mathbf{0}} \pmod 3$; $a_{\mathbf{0}} = 2 \pmod 3$
- Let $-1 = 2 + a_{\mathbf{1}} \cdot 3 \pmod 9$;
  $-3 = a_{\mathbf{1}} \cdot 3 \pmod 9$; $6 = a_{\mathbf{1}} \cdot 3 \pmod 9$;

- 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 $-1 = \mathbf{a_0} \pmod{3}$; $\mathbf{a_0} = 2 \pmod{3}$
- Let $-1 = 2 + \mathbf{a_1} \cdot 3 \pmod{9}$; $-3 = \mathbf{a_1} \cdot 3 \pmod{9}$; $6 = \mathbf{a_1} \cdot 3 \pmod{9}$; $\mathbf{a_1} = 2$
- 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 $-1 = a_\mathbf{0} \pmod{3}$; $a_\mathbf{0} = 2 \pmod{3}$
- Let $-1 = 2 + a_\mathbf{1} \cdot 3 \pmod{9}$;
  $-3 = a_\mathbf{1} \cdot 3 \pmod{9}$; $6 = a_\mathbf{1} \cdot 3 \pmod{9}$;
  $a_\mathbf{1} = 2$
- Let $-1 = 2 + 2 \cdot 3 + 2 \cdot 3^\mathbf{2} + \dots$

- 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 $-1 = a_{\mathbf{0}} \pmod{3}$; $a_{\mathbf{0}} = 2 \pmod{3}$
- Let $-1 = 2 + a_{\mathbf{1}} \cdot 3 \pmod{9}$; $-3 = a_{\mathbf{1}} \cdot 3 \pmod{9}$; $6 = a_{\mathbf{1}} \cdot 3 \pmod{9}$; $a_{\mathbf{1}} = 2$
- Let $-1 = 2 + 2 \cdot 3 + 2 \cdot 3^{\mathbf{2}} + \dots$

- 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 $-1 = a_{\mathbf{0}} \pmod{3}$; $a_{\mathbf{0}} = 2 \pmod{3}$
- Let $-1 = 2 + a_{\mathbf{1}} \cdot 3 \pmod{9}$; $-3 = a_{\mathbf{1}} \cdot 3 \pmod{9}$; $6 = a_{\mathbf{1}} \cdot 3 \pmod{9}$; $a_{\mathbf{1}} = 2$
- Let $-1 = 2 + 2 \cdot 3 + 2 \cdot 3^{\mathbf{2}} + \dots$

- Let $1/4 = \sum_i a_i 3^i$
- What defines $1/4$? The equation $1/4 \cdot 4 = 1$.
- $(a_{\mathbf{0}} + 3a_{\mathbf{1}} + 9a_{\mathbf{2}} + \dots)(1 + 3 + 0 \cdot 9 + \cdots) = 1$

A step back

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

- Let $-1 = \sum_i a_i 3^i$
- Let $-1 = a_\mathbf{0} \pmod{3}$; $a_\mathbf{0} = 2 \pmod{3}$
- Let $-1 = 2 + a_\mathbf{1} \cdot 3 \pmod{9}$;
  $-3 = a_\mathbf{1} \cdot 3 \pmod{9}$; $6 = a_\mathbf{1} \cdot 3 \pmod{9}$;
  $a_\mathbf{1} = 2$
- Let $-1 = 2 + 2 \cdot 3 + 2 \cdot 3^\mathbf{2} + \ldots$

- Let $1/4 = \sum_i a_i 3^i$
- What defines $1/4$? The equation $1/4 \cdot 4 = 1$.
- $(a_\mathbf{0} + 3a_\mathbf{1} + 9a_\mathbf{2} + \ldots)(1 + 3 + 0 \cdot 9 + \cdots) = 1$
- $a_\mathbf{0} \cdot 1 \equiv 1 \pmod{3}$

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 $-1 = a_{\mathbf{0}} \pmod{3}$; $a_{\mathbf{0}} = 2 \pmod{3}$
- Let $-1 = 2 + a_{\mathbf{1}} \cdot 3 \pmod{9}$;
  $-3 = a_{\mathbf{1}} \cdot 3 \pmod{9}$; $6 = a_{\mathbf{1}} \cdot 3 \pmod{9}$;
  $a_{\mathbf{1}} = 2$
- 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 $1/4 \cdot 4 = 1$.
- $(a_{\mathbf{0}} + 3a_{\mathbf{1}} + 9a_{\mathbf{2}} + \dots)(1 + 3 + 0 \cdot 9 + \cdots) = 1$
- $a_{\mathbf{0}} \cdot 1 \equiv 1 \pmod{3} a_{\mathbf{0}} = 1$.

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 $-1 = a_{\mathbf{0}} \pmod{3}$; $a_{\mathbf{0}} = 2 \pmod{3}$
- Let $-1 = 2 + a_{\mathbf{1}} \cdot 3 \pmod{9}$; $-3 = a_{\mathbf{1}} \cdot 3 \pmod{9}$; $6 = a_{\mathbf{1}} \cdot 3 \pmod{9}$; $a_{\mathbf{1}} = 2$
- Let $-1 = 2 + 2 \cdot 3 + 2 \cdot 3^{\mathbf{2}} + \dots$

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

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 $-1 = a_\mathbf{0} \pmod{3}$; $a_\mathbf{0} = 2 \pmod{3}$
- Let $-1 = 2 + a_\mathbf{1} \cdot 3 \pmod{9}$;
  $-3 = a_\mathbf{1} \cdot 3 \pmod{9}$; $6 = a_\mathbf{1} \cdot 3 \pmod{9}$;
  $a_\mathbf{1} = 2$
- Let $-1 = 2 + 2 \cdot 3 + 2 \cdot 3^\mathbf{2} + \dots$

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

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

- 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 $-1 = 2 + 2 \cdot 3 + 2 \cdot 3^2 + \ldots$

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

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.
- Let $x = \sum_i a_0 + 7a_1 + 49a_2 + \ldots$

Irrationals

- Let's solve $X^2 = 2$ in the $7-$adics.
- Such a solution does not "really exist" in the rationals or the integers.
- Let $x = \sum_i a_0 + 7a_1 + 49a_2 + \dots$
- Start with $x^2 \equiv a_0^2 \equiv 2 \pmod{7}$

Irrationals

- Let's solve $X^2 = 2$ in the $7-$adics.
- Such a solution does not "really exist" in the rationals or the integers.
- Let $x = \sum_i a_0 + 7a_1 + 49a_2 + \dots$
- Start with $x^2 \equiv a_0^2 \equiv 2 \pmod 7$
- $a_0 = 3$
- $(3 + 7a_1)^2 \equiv 2 \pmod{49}$

Irrationals

- Let's solve $X^2 = 2$ in the $7-$adics.
- Such a solution does not "really exist" in the rationals or the integers.
- Let $x = \sum_i a_0 + 7a_1 + 49a_2 + \ldots$
- Start with $x^2 \equiv a_0^2 \equiv 2 \pmod 7$
- $a_0 = 3$
- $(3 + 7a_1)^2 \equiv 2 \pmod{49}$
- $9 + 42a_1 + 49a_1^2 \equiv 2 \pmod{49}$

Irrationals

- Let's solve $X^2 = 2$ in the $7-$adics.
- Such a solution does not "really exist" in the rationals or the integers.
- Let $x = \sum_i a_0 + 7a_1 + 49a_2 + \dots$
- Start with $x^2 \equiv a_0^2 \equiv 2 \pmod 7$
- $a_0 = 3$
- $(3 + 7a_1)^2 \equiv 2 \pmod{49}$
- $9 + 42a_1 + 49a_1^2 \equiv 2 \pmod{49}$
- $7 + 42a_1 \equiv 0 \pmod{49}$

Irrationals

- Let's solve $X^2 = 2$ in the $7-$adics.
- Such a solution does not "really exist" in the rationals or the integers.
- Let $x = \sum_i a_0 + 7a_1 + 49a_2 + \ldots$
- Start with $x^2 \equiv a_0^2 \equiv 2 \pmod 7$
- $a_0 = 3$
- $(3 + 7a_1)^2 \equiv 2 \pmod{49}$
- $9 + 42a_1 + 49a_1^2 \equiv 2 \pmod{49}$
- $7 + 42a_1 \equiv 0 \pmod{49}$
- $-42 + 42a_1 \equiv 0 \pmod{49}$

Irrationals

- Let's solve $X^2 = 2$ in the $7-$adics.
- Such a solution does not "really exist" in the rationals or the integers.
- Let $x = \sum_i a_0 + 7a_1 + 49a_2 + \dots$
- Start with $x^2 \equiv a_0^2 \equiv 2 \pmod 7$
- $a_0 = 3$
- $(3 + 7a_1)^2 \equiv 2 \pmod{49}$
- $9 + 42a_1 + 49a_1^2 \equiv 2 \pmod{49}$
- $7 + 42a_1 \equiv 0 \pmod{49}$
- $-42 + 42a_1 \equiv 0 \pmod{49}$
- $a_1 \equiv 1 \pmod{49}$

Irrationals

- Let's solve $X^2 = 2$ in the 7$-$adics.
- Such a solution does not "really exist" in the rationals or the integers.
- Let $x = \sum_i a_0 + 7a_1 + 49a_2 + \dots$
- Start with $x^2 \equiv a_0^2 \equiv 2 \pmod 7$
- $a_0 = 3$
- $(3 + 7a_1)^2 \equiv 2 \pmod{49}$
- $9 + 42a_1 + 49a_1^2 \equiv 2 \pmod{49}$
- $7 + 42a_1 \equiv 0 \pmod{49}$
- $-42 + 42a_1 \equiv 0 \pmod{49}$
- $a_1 \equiv 1 \pmod{49}$
- Keep going to extract $a_2, a_3, \dots$

Irrationals

- Let's solve $X^2 = 2$ in the $7-$adics.
- Such a solution does not "really exist" in the rationals or the integers.
- Let $x = \sum_i a_0 + 7a_1 + 49a_2 + \ldots$
- Start with $x^2 \equiv a_0^2 \equiv 2 \pmod 7$
- $a_0 = 3$
- $(3 + 7a_1)^2 \equiv 2 \pmod{49}$
- $9 + 42a_1 + 49a_1^2 \equiv 2 \pmod{49}$
- $7 + 42a_1 \equiv 0 \pmod{49}$
- $-42 + 42a_1 \equiv 0 \pmod{49}$
- $a_1 \equiv 1 \pmod{49}$
- Keep going to extract $a_2, a_3, \ldots$
- We solved an equation in $\mathbb{Q}_7$ for which we didn't have a solution in $\mathbb{Q}$!

Irrationals

- Let's solve $X^2 = 2$ in the $7-$adics.
- Such a solution does not "really exist" in the rationals or the integers.
- Let $x = \sum_i a_0 + 7a_1 + 49a_2 + \ldots$
- Start with $x^2 \equiv a_0^2 \equiv 2 \pmod 7$
- $a_0 = 3$
- $(3 + 7a_1)^2 \equiv 2 \pmod{49}$
- $9 + 42a_1 + 49a_1^2 \equiv 2 \pmod{49}$
- $7 + 42a_1 \equiv 0 \pmod{49}$
- $-42 + 42a_1 \equiv 0 \pmod{49}$
- $a_1 \equiv 1 \pmod{49}$
- Keep going to extract $a_2, a_3, \ldots$
- We solved an equation in $\mathbb{Q}_7$ for which we didn't have a solution in $\mathbb{Q}$!
- Can we always lift? **Hensel's lemma**

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!
- $|a|_p = p^{-1 \cdot \text{highest power of } p \text{ which divides } a}$
- $|10|_3 = 3^{-0} = 1$
- $|3|_3 = 3^{-1} = 1/3$
- $|9|_3 = 3^{-2} = 1/9$
- $|90|_3 = 3^{-2} = 1/9$
- $|27|_3 = 3^{-3} = 1/27$
- $|ab|_p = |a|_p \cdot |b|_p$. Plays well with multiplication

Convergence

- Intuition: higher powers of p should become "smaller" for convergence!
- $|a|_p = p^{-1 \cdot \text{highest power of } p \text{ which divides } a}$
- $|10|_3 = 3^{-0} = 1$
- $|3|_3 = 3^{-1} = 1/3$
- $|9|_3 = 3^{-2} = 1/9$
- $|90|_3 = 3^{-2} = 1/9$
- $|27|_3 = 3^{-3} = 1/27$
- $|ab|_p = |a|_p \cdot |b|_p$. Plays well with multiplication
- What about addition?

Convergence

- Intuition: higher powers of p should become "smaller" for convergence!
- $|a|_p = p^{-1 \cdot \text{highest power of } p \text{ which divides } a}$
- $|10|_3 = 3^{-0} = 1$
- $|3|_3 = 3^{-1} = 1/3$
- $|9|_3 = 3^{-2} = 1/9$
- $|90|_3 = 3^{-2} = 1/9$
- $|27|_3 = 3^{-3} = 1/27$
- $|ab|_p = |a|_p \cdot |b|_p$. Plays well with multiplication
- What about addition?
- $|a + b|_p \leqslant \max(|a|_p, |b|_p)$

Convergence

- Intuition: higher powers of p should become "smaller" for convergence!
- $|a|_p = p^{-1 \cdot \text{highest power of } p \text{ which divides } a}$
- $|10|_3 = 3^{-0} = 1$
- $|3|_3 = 3^{-1} = 1/3$
- $|9|_3 = 3^{-2} = 1/9$
- $|90|_3 = 3^{-2} = 1/9$
- $|27|_3 = 3^{-3} = 1/27$
- $|ab|_p = |a|_p \cdot |b|_p$. Plays well with multiplication
- What about addition?
- $|a + b|_p \leqslant \max(|a|_p, |b|_p)$
- Let $a = p^{\alpha} a'$, $b = p^{\beta} b'$, let $\alpha \leqslant \beta$ WLOG.

Convergence

- Intuition: higher powers of p should become "smaller" for convergence!
- $|a|_p = p^{-1 \cdot \text{highest power of } p \text{ which divides } a}$
- $|10|_3 = 3^{-0} = 1$
- $|3|_3 = 3^{-1} = 1/3$
- $|9|_3 = 3^{-2} = 1/9$
- $|90|_3 = 3^{-2} = 1/9$
- $|27|_3 = 3^{-3} = 1/27$
- $|ab|_p = |a|_p \cdot |b|_p$. Plays well with multiplication
- What about addition?
- $|a+b|_p \leqslant \max(|a|_p, |b|_p)$
- Let $a = p^{\alpha} a'$, $b = p^{\beta} b'$, let $\alpha \leqslant \beta$ WLOG.
- $(a+b) = p^{\alpha}(a' + p^{\beta-\alpha} b')$

Convergence

- Intuition: higher powers of p should become "smaller" for convergence!
- $|a|_p = p^{-1 \cdot \text{highest power of } p \text{ which divides } a}$
- $|10|_3 = 3^{-0} = 1$
- $|3|_3 = 3^{-1} = 1/3$
- $|9|_3 = 3^{-2} = 1/9$
- $|90|_3 = 3^{-2} = 1/9$
- $|27|_3 = 3^{-3} = 1/27$
- $|ab|_p = |a|_p \cdot |b|_p$. Plays well with multiplication
- What about addition?
- $|a + b|_p \leqslant \max(|a|_p, |b|_p)$
- Let $a = p^\alpha a'$, $b = p^\beta b'$, let $\alpha \leqslant \beta$ WLOG.
- $(a + b) = p^\alpha (a' + p^{\beta-\alpha} b')$
- If $(a' + p^{\beta-\alpha} b')$ is *not* divisible by p

Convergence

- Intuition: higher powers of p should become "smaller" for convergence!
- $|a|_p = p^{-1 \cdot \text{highest power of } p \text{ which divides } a}$
- $|10|_3 = 3^{-0} = 1$
- $|3|_3 = 3^{-1} = 1/3$
- $|9|_3 = 3^{-2} = 1/9$
- $|90|_3 = 3^{-2} = 1/9$
- $|27|_3 = 3^{-3} = 1/27$
- $|ab|_p = |a|_p \cdot |b|_p$. Plays well with multiplication
- What about addition?
- $|a+b|_p \leqslant \max(|a|_p, |b|_p)$
- Let $a = p^{\alpha} a'$, $b = p^{\beta} b'$, let $\alpha \leqslant \beta$ WLOG.
- $(a+b) = p^{\alpha}(a' + p^{\beta-\alpha} b')$
- If $(a' + p^{\beta-\alpha} b')$ is *not* divisible by p , then $|a+b|_p = p^{-\alpha} = |a|_p$

Convergence

- Intuition: higher powers of p should become "smaller" for convergence!
- $|a|_p = p^{-1 \cdot \text{highest power of } p \text{ which divides } a}$
- $|10|_3 = 3^{-0} = 1$
- $|3|_3 = 3^{-1} = 1/3$
- $|9|_3 = 3^{-2} = 1/9$
- $|90|_3 = 3^{-2} = 1/9$
- $|27|_3 = 3^{-3} = 1/27$
- $|ab|_p = |a|_p \cdot |b|_p$. Plays well with multiplication
- What about addition?
- $|a+b|_p \leqslant \max(|a|_p, |b|_p)$
- Let $a = p^\alpha a'$, $b = p^\beta b'$, let $\alpha \leqslant \beta$ WLOG.
- $(a+b) = p^\alpha (a' + p^{\beta-\alpha} b')$
- If $(a' + p^{\beta-\alpha} b')$ is *not* divisible by p , then $|a+b|_p = p^{-\alpha} = |a|_p$
- If $(a' + p^{\beta-\alpha} b')$ *is* divisible by p

Convergence

- Intuition: higher powers of p should become "smaller" for convergence!
- $|a|_p = p^{-1 \cdot \text{highest power of } p \text{ which divides } a}$
- $|10|_3 = 3^{-0} = 1$
- $|3|_3 = 3^{-1} = 1/3$
- $|9|_3 = 3^{-2} = 1/9$
- $|90|_3 = 3^{-2} = 1/9$
- $|27|_3 = 3^{-3} = 1/27$
- $|ab|_p = |a|_p \cdot |b|_p$. Plays well with multiplication
- What about addition?
- $|a+b|_p \leqslant \max(|a|_p, |b|_p)$
- Let $a = p^{\alpha} a'$, $b = p^{\beta} b'$, let $\alpha \leqslant \beta$ WLOG.
- $(a+b) = p^{\alpha}(a' + p^{\beta-\alpha} b')$
- If $(a' + p^{\beta-\alpha} b')$ is *not* divisible by p , then $|a+b|_p = p^{-\alpha} = |a|_p$
- If $(a' + p^{\beta-\alpha} b')$ *is* divisible by p , then $|a+b|_p = p^{-(\alpha + \texttt{more})} < p^{-\alpha}$

Convergence

- Intuition: higher powers of p should become "smaller" for convergence!
- $|a|_p = p^{-1 \cdot \text{highest power of } p \text{ which divides } a}$
- $|10|_3 = 3^{-0} = 1$
- $|3|_3 = 3^{-1} = 1/3$
- $|9|_3 = 3^{-2} = 1/9$
- $|90|_3 = 3^{-2} = 1/9$
- $|27|_3 = 3^{-3} = 1/27$
- $|ab|_p = |a|_p \cdot |b|_p$. Plays well with multiplication
- What about addition?
- $|a + b|_p \leqslant \max(|a|_p, |b|_p)$
- Let $a = p^{\alpha} a'$, $b = p^{\beta} b'$, let $\alpha \leqslant \beta$ WLOG.
- $(a + b) = p^{\alpha}(a' + p^{\beta-\alpha} b')$
- If $(a' + p^{\beta-\alpha} b')$ is *not* divisible by p , then $|a + b|_p = p^{-\alpha} = |a|_p$
- If $(a' + p^{\beta-\alpha} b')$ *is* divisible by p , then $|a + b|_p = p^{-(\alpha + \texttt{more})} < p^{-\alpha}$
- $|10|_2 = |2 * 5|_2 = 1/2$; $|40|_2 = |8 * 5|_2 = 1/8$

Convergence

- Intuition: higher powers of p should become "smaller" for convergence!
- $|a|_p = p^{-1 \cdot \text{highest power of } p \text{ which divides } a}$
- $|10|_3 = 3^{-0} = 1$
- $|3|_3 = 3^{-1} = 1/3$
- $|9|_3 = 3^{-2} = 1/9$
- $|90|_3 = 3^{-2} = 1/9$
- $|27|_3 = 3^{-3} = 1/27$
- $|ab|_p = |a|_p \cdot |b|_p$. Plays well with multiplication
- What about addition?
- $|a+b|_p \leqslant \max(|a|_p, |b|_p)$
- Let $a = p^\alpha a'$, $b = p^\beta b'$, let $\alpha \leqslant \beta$ WLOG.
- $(a+b) = p^\alpha(a' + p^{\beta-\alpha} b')$
- If $(a' + p^{\beta-\alpha} b')$ is *not* divisible by p , then $|a+b|_p = p^{-\alpha} = |a|_p$
- If $(a' + p^{\beta-\alpha} b')$ *is* divisible by p , then $|a+b|_p = p^{-(\alpha+\mathtt{more})} < p^{-\alpha}$
- $|10|_2 = |2 * 5|_2 = 1/2$; $|40|_2 = |8 * 5|_2 = 1/8$
- $|10 + 40|_2 = |50|_2 = |2 * 25|_2 = 1/2$

Convergence

- Intuition: higher powers of p should become "smaller" for convergence!
- $|a|_p = p^{-1 \cdot \text{highest power of } p \text{ which divides } a}$
- $|10|_3 = 3^{-0} = 1$
- $|3|_3 = 3^{-1} = 1/3$
- $|9|_3 = 3^{-2} = 1/9$
- $|90|_3 = 3^{-2} = 1/9$
- $|27|_3 = 3^{-3} = 1/27$
- $|ab|_p = |a|_p \cdot |b|_p$. Plays well with multiplication
- What about addition?
- $|a+b|_p \leqslant \max(|a|_p, |b|_p)$
- Let $a = p^\alpha a'$, $b = p^\beta b'$, let $\alpha \leqslant \beta$ WLOG.
- $(a+b) = p^\alpha (a' + p^{\beta-\alpha} b')$
- If $(a' + p^{\beta-\alpha} b')$ is *not* divisible by p , then $|a+b|_p = p^{-\alpha} = |a|_p$
- If $(a' + p^{\beta-\alpha} b')$ *is* divisible by p , then $|a+b|_p = p^{-(\alpha + \texttt{more})} < p^{-\alpha}$
- $|10|_2 = |2 * 5|_2 = 1/2$; $|40|_2 = |8 * 5|_2 = 1/8$
- $|10 + 40|_2 = |50|_2 = |2 * 25|_2 = 1/2$
- $|10 + 10|_2 = |20|_2 = |4 * 5|_2 = 1/4$

Convergence

- Intuition: higher powers of p should become "smaller" for convergence!
- $|a|_p = p^{-1 \cdot \text{highest power of } p \text{ which divides } a}$
- $|10|_3 = 3^{-0} = 1$
- $|3|_3 = 3^{-1} = 1/3$
- $|9|_3 = 3^{-2} = 1/9$
- $|90|_3 = 3^{-2} = 1/9$
- $|27|_3 = 3^{-3} = 1/27$
- $|ab|_p = |a|_p \cdot |b|_p$. Plays well with multiplication
- What about addition?
- $|a + b|_p \leqslant \max(|a|_p, |b|_p)$
- Let $a = p^{\alpha} a'$, $b = p^{\beta} b'$, let $\alpha \leqslant \beta$ WLOG.
- $(a + b) = p^{\alpha}(a' + p^{\beta-\alpha} b')$
- If $(a' + p^{\beta-\alpha} b')$ is *not* divisible by p , then $|a + b|_p = p^{-\alpha} = |a|_p$
- If $(a' + p^{\beta-\alpha} b')$ *is* divisible by p , then $|a + b|_p = p^{-(\alpha + \texttt{more})} < p^{-\alpha}$
- $|10|_2 = |2 * 5|_2 = 1/2$; $|40|_2 = |8 * 5|_2 = 1/8$
- $|10 + 40|_2 = |50|_2 = |2 * 25|_2 = 1/2$
- $|10 + 10|_2 = |20|_2 = |4 * 5|_2 = 1/4$

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**:$-2x = 1$; $x = -1/2$

Scam v/s non-scam

- Solve $x = 1 + 3x$
- **Non scam**:$-2x = 1$; $x = -1/2$
- Recurrence: $x[i+1] = 1 + 3x[i]$

Scam v/s non-scam

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

Scam v/s non-scam

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

Scam v/s non-scam

- Solve $x = 1 + 3x$
- **Non scam**:$-2x = 1$; $x = -1/2$
- Recurrence: $x[i+1] = 1 + 3x[i]$
- $x_0 = 1$
- $x_1 = 1 + 3$
- $x_2 = 1 + 3x_1 = 1 + 3(1 + 3) = 1 + 3 + 3^2$
- $x_3 = 1 + 3x_2 = 1 + 3(1 + 3 + 3^2) = 1 + 3 + 3^2 + 3^3$

Scam v/s non-scam

- Solve $x = 1 + 3x$
- **Non scam**:$-2x = 1$; $x = -1/2$
- Recurrence: $x[i + 1] = 1 + 3x[i]$
- $x_0 = 1$
- $x_1 = 1 + 3$
- $x_2 = 1 + 3x_1 = 1 + 3(1 + 3) = 1 + 3 + 3^2$
- $x_3 = 1 + 3x_2 = 1 + 3(1 + 3 + 3^2) = 1 + 3 + 3^2 + 3^3$
- $x_i = 1 + 3 + 3^2 + \cdots + 3^i$

Scam v/s non-scam

- Solve $x = 1 + 3x$
- **Non scam**:$-2x = 1$; $x = -1/2$
- Recurrence: $x[i+1] = 1 + 3x[i]$
- $x_0 = 1$
- $x_1 = 1 + 3$
- $x_2 = 1 + 3x_1 = 1 + 3(1+3) = 1 + 3 + 3^2$
- $x_3 = 1 + 3x_2 = 1 + 3(1 + 3 + 3^2) = 1 + 3 + 3^2 + 3^3$
- $x_i = 1 + 3 + 3^2 + \cdots + 3^i$
- $x_\infty = 1/(1-3) = -1/2$
- Converges? We need $|3| < 1$

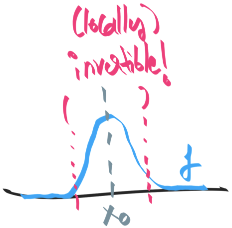
Scam v/s non-scam

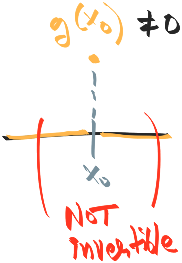
- Solve $x = 1 + 3x$
- **Non scam**:$-2x = 1$; $x = -1/2$
- Recurrence: $x[i+1] = 1 + 3x[i]$
- $x_0 = 1$
- $x_1 = 1 + 3$
- $x_2 = 1 + 3x_1 = 1 + 3(1 + 3) = 1 + 3 + 3^2$
- $x_3 = 1 + 3x_2 = 1 + 3(1 + 3 + 3^2) = 1 + 3 + 3^2 + 3^3$
- $x_i = 1 + 3 + 3^2 + \cdots + 3^i$
- $x_\infty = 1/(1 - 3) = -1/2$
- Converges? We need $|3| < 1$
- But it is! $|3|_3 < 1$

Scam v/s non-scam

- Solve $x = 1 + 3x$
- **Non scam**:$-2x = 1$; $x = -1/2$
- Recurrence: $x[i+1] = 1 + 3x[i]$
- $x_0 = 1$
- $x_1 = 1 + 3$
- $x_2 = 1 + 3x_1 = 1 + 3(1+3) = 1 + 3 + 3^2$
- $x_3 = 1 + 3x_2 = 1 + 3(1 + 3 + 3^2) = 1 + 3 + 3^2 + 3^3$
- $x_i = 1 + 3 + 3^2 + \cdots + 3^i$
- $x_\infty = 1/(1-3) = -1/2$
- Converges? We need $|3| < 1$
- But it is! $|3|_3 < 1$

Why only primes? Geometry of functions

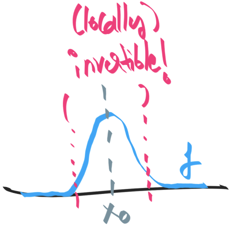


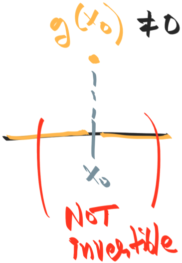


$f(x_0) \neq 0 \Rightarrow f$ invertible (locally)

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

Why only primes? Geometry of functions



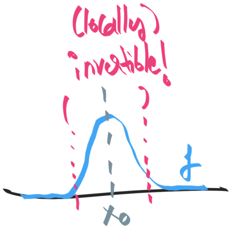


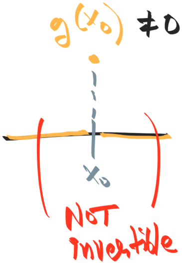
$f(x_0) \neq 0 \Rightarrow f$ invertible (locally)

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

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

Why only primes? Geometry of functions





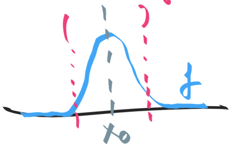
$f(x_0) \neq 0 \Rightarrow f$ invertible (locally)

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

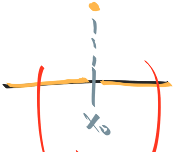
(locally) invertible!



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

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

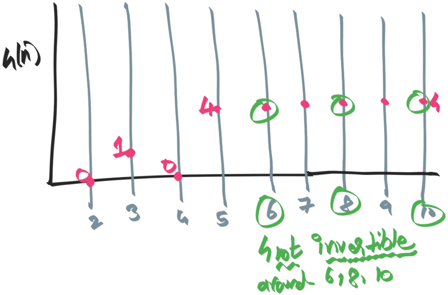
$g(x_0) \neq 0$



NOT invertible

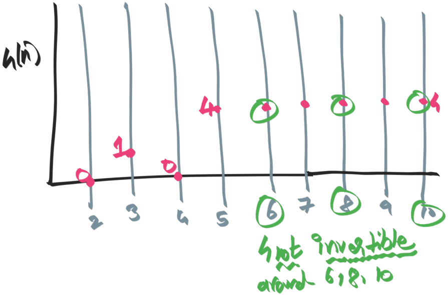
- $f(x)$: continuous, *non-zero* at $x = x_0$.
- $f(x)$: *locally invertible* at $x = x_0$.

Why only primes? Geometry of numbers



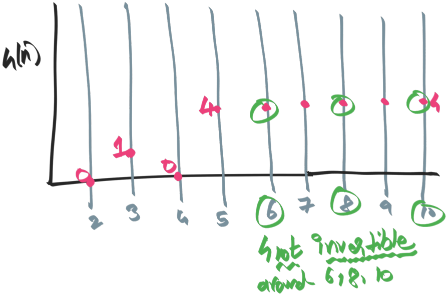
- consider $4(\cdot)$ as function $\mathbb{N} \to \mathbb{N}$.

Why only primes? Geometry of numbers



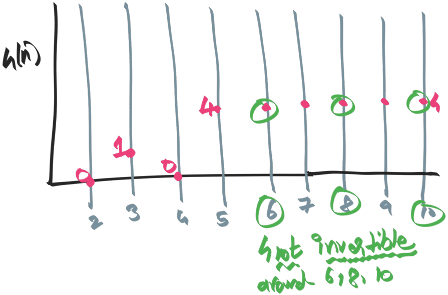
- consider $4(\cdot)$ as function $\mathbb{N} \to \mathbb{N}$.
- nonzero at $a_0 = 6$: $4 \simeq 4 \pmod 6$

Why only primes? Geometry of numbers



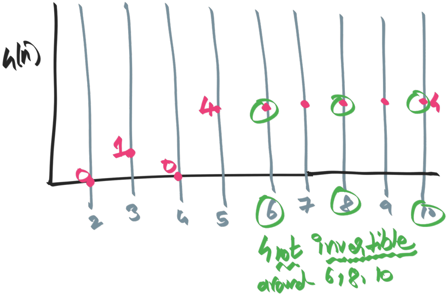
- consider $4(\cdot)$ as function $\mathbb{N} \to \mathbb{N}$.
- nonzero at $a_0 = 6$: $4 \simeq 4 \pmod{6}$
- *not invertible* modulo 6:
  $[0, 1, 2, 3, 4, 5] \times 4 \equiv [0, 4, 8, 12, 16, 20] \equiv [0, 4, 2, 0, 4, 2] \pmod{6}$

Why only primes? Geometry of numbers



- consider $4(\cdot)$ as function $\mathbb{N} \to \mathbb{N}$.
- 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 $4(\cdot)$ as function $\mathbb{N} \to \mathbb{N}$.
- 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!
- The only points in $\mathbb{N}$ which obey "any non zero function is locally invertible" are primes.
- Hence, we only consider evaluation at primes.

Why is this useful?

- Does $x^2 = 2$ have a solution in $\mathbb{Z}$?
- If it has a solution in $\mathbb{Z}$

Why is this useful?

- Does $x^2 = 2$ have a solution in $\mathbb{Z}$?
- If it has a solution in $\mathbb{Z}$
- It must continue to have solutions in $Z/n\mathbb{Z}$

Why is this useful?

- Does $x^2 = 2$ have a solution in $\mathbb{Z}$?
- If it has a solution in $\mathbb{Z}$
- It must continue to have solutions in $Z/n\mathbb{Z}$
- $a \cdot b = c \implies a \cdot_n b \equiv c \pmod{n}$, $a + b = c \implies a +_n b \equiv c \pmod{n}$

Why is this useful?

- Does $x^2 = 2$ have a solution in $\mathbb{Z}$?
- If it has a solution in $\mathbb{Z}$
- It must continue to have solutions in $Z/n\mathbb{Z}$
- $a \cdot b = c \implies a \cdot_n b \equiv c \pmod{n}$, $a + b = c \implies a +_n b \equiv c \pmod{n}$
- $x^2 = 2 \pmod{5}$: $[0, 1, 2, 3, 4]^2 = [0, 1, 4, 9, 16] = [0, 1, 4, 4, 1]$
- So $x^2 = 2$ has no solution in $\mathbb{Z}$
- We used a *finite number of candidates* in $\mathbb{Z}/5Z$

Why is this useful?

- Does $x^2 = 2$ have a solution in $\mathbb{Z}$?
- If it has a solution in $\mathbb{Z}$
- It must continue to have solutions in $Z/n\mathbb{Z}$
- $a \cdot b = c \implies a \cdot_n b \equiv c \pmod{n}$, $a + b = c \implies a +_n b \equiv c \pmod{n}$
- $x^2 = 2 \pmod{5}$: $[0, 1, 2, 3, 4]^2 = [0, 1, 4, 9, 16] = [0, 1, 4, 4, 1]$
- So $x^2 = 2$ has no solution in $\mathbb{Z}$
- We used a *finite number of candidates* in $\mathbb{Z}/5Z$, eliminated infinite number of candidates in $\mathbb{Z}$.
- Hasse Minkowski: A quadratic form $(ax^2 + bxy + cy^2)$ has a root in $\mathbb{Q}$ iff it has roots in all $\mathbb{Q}_p$.

Hensel's Lemma

Theorem

- *Let $f(x)$ be a polynomial with integer or p-adic coefficients.*
- *If $f(r) \equiv 0 \pmod{p^k}$ and $f'(r) \not\equiv 0 \pmod{p}$ [non-degenerate], then*
- *(1) there is an integer s such that $f(s) \equiv 0 \pmod{p^{k+1}}$ [lifting]*
- *(2) and $r \equiv s \pmod{p^k}$ [consistency]*

- **Since** $r \equiv s \left(\bmod p^k\right)$ **[consistency], we have** $s = r + tp^k$ **for some** $t \in \mathbb{Z}$.

Hensel's Lemma

Theorem

- *Let $f(x)$ be a polynomial with integer or p-adic coefficients.*
- *If $f(r) \equiv 0 \pmod{p^k}$ and $f'(r) \not\equiv 0 \pmod{p}$ [non-degenerate], then*
- *(1) there is an integer s such that $f(s) \equiv 0 \pmod{p^{k+1}}$ [lifting]*
- *(2) and $r \equiv s \pmod{p^k}$ [consistency]*

- Since $r \equiv s \left(\mathrm{mod}\ p^k\right)$ [consistency], we have $s = r + tp^k$ for some $t \in \mathbb{Z}$.
- If we find a t, then we are done, since that is the unknown to find s.

Hensel's Lemma

Theorem

- *Let $f(x)$ be a polynomial with integer or p-adic coefficients.*
- *If $f(r) \equiv 0 \pmod{p^k}$ and $f'(r) \not\equiv 0 \pmod{p}$ [non-degenerate], then*
- *(1) there is an integer s such that $f(s) \equiv 0 \pmod{p^{k+1}}$ [lifting]*
- *(2) and $r \equiv s \pmod{p^k}$ [consistency]*

- Since $r \equiv s \left(\mathrm{mod}\ p^k\right)$ [consistency], we have $s = r + tp^k$ for some $t \in \mathbb{Z}$.
- If we find a t, then we are done, since that is the unknown to find s.
- $f(s) = f(r + tp^k) = f(r) + f'(r)tp^k + (tp^k)^2(\ldots)$.

Hensel's Lemma

Theorem

- *Let $f(x)$ be a polynomial with integer or p-adic coefficients.*
- *If $f(r) \equiv 0 \pmod{p^k}$ and $f'(r) \not\equiv 0 \pmod{p}$ [non-degenerate], then*
- *(1) there is an integer s such that $f(s) \equiv 0 \pmod{p^{k+1}}$ [lifting]*
- *(2) and $r \equiv s \pmod{p^k}$ [consistency]*

- Since $r \equiv s \left(\mathrm{mod}\ p^k\right)$ [consistency], we have $s = r + tp^k$ for some $t \in \mathbb{Z}$.
- If we find a t, then we are done, since that is the unknown to find s.
- $f(s) = f(r + tp^k) = f(r) + f'(r)tp^k + (tp^k)^2(\dots)$.
- $f(s) = f(r + tp^k) = f(r) + f'(r)tp^k + p^{2k}t^2 g(t)$ for some $g(t) \in \mathbb{Z}[t]$.

Hensel's Lemma

Theorem

- *Let $f(x)$ be a polynomial with integer or p-adic coefficients.*
- *If $f(r) \equiv 0 \pmod{p^k}$ and $f'(r) \not\equiv 0 \pmod{p}$ [non-degenerate], then*
- *(1) there is an integer s such that $f(s) \equiv 0 \pmod{p^{k+1}}$ [lifting]*
- *(2) and $r \equiv s \pmod{p^k}$ [consistency]*

- Since $r \equiv s \pmod{p^k}$ [consistency], we have $s = r + tp^k$ for some $t \in \mathbb{Z}$.
- If we find a t, then we are done, since that is the unknown to find s.
- $f(s) = f(r + tp^k) = f(r) + f'(r)tp^k + (tp^k)^2(\dots)$.
- $f(s) = f(r + tp^k) = f(r) + f'(r)tp^k + p^{2k}t^2 g(t)$ for some $g(t) \in \mathbb{Z}[t]$.
- Since $f(r) \equiv 0 \pmod{p^k}$, we have $f(r) = zp^k$ for some $z \in \mathbb{Z}$.

Hensel's Lemma

Theorem

- *Let $f(x)$ be a polynomial with integer or p-adic coefficients.*
- *If $f(r) \equiv 0 \pmod{p^k}$ and $f'(r) \not\equiv 0 \pmod{p}$ [non-degenerate], then*
- *(1) there is an integer s such that $f(s) \equiv 0 \pmod{p^{k+1}}$ [lifting]*
- *(2) and $r \equiv s \pmod{p^k}$ [consistency]*

- Since $r \equiv s \pmod{p^k}$ [consistency], we have $s = r + tp^k$ for some $t \in \mathbb{Z}$.
- If we find a t, then we are done, since that is the unknown to find s.
- $f(s) = f(r + tp^k) = f(r) + f'(r)tp^k + (tp^k)^2(\dots)$.
- $f(s) = f(r + tp^k) = f(r) + f'(r)tp^k + p^{2k}t^2 g(t)$ for some $g(t) \in \mathbb{Z}[t]$.
- Since $f(r) \equiv 0 \pmod{p^k}$, we have $f(r) = zp^k$ for some $z \in \mathbb{Z}$.
- $f(s) = f(r + tp^k) = zp^k + f'(r)tp^k + p^{2k}t^2 g(t)$.

Hensel's Lemma

Theorem

- *Let $f(x)$ be a polynomial with integer or p-adic coefficients.*
- *If $f(r) \equiv 0 \pmod{p^k}$ and $f'(r) \not\equiv 0 \pmod{p}$ [non-degenerate], then*
- *(1) there is an integer s such that $f(s) \equiv 0 \pmod{p^{k+1}}$ [lifting]*
- *(2) and $r \equiv s \pmod{p^k}$ [consistency]*

- Since $r \equiv s \pmod{p^k}$ [consistency], we have $s = r + tp^k$ for some $t \in \mathbb{Z}$.
- If we find a t, then we are done, since that is the unknown to find s.
- $f(s) = f(r + tp^k) = f(r) + f'(r)tp^k + (tp^k)^2(\dots)$.
- $f(s) = f(r + tp^k) = f(r) + f'(r)tp^k + p^{2k}t^2 g(t)$ for some $g(t) \in \mathbb{Z}[t]$.
- Since $f(r) \equiv 0 \pmod{p^k}$, we have $f(r) = zp^k$ for some $z \in \mathbb{Z}$.
- $f(s) = f(r + tp^k) = zp^k + f'(r)tp^k + p^{2k}t^2 g(t)$.
- $f(s) = f(r + tp^k) = p^k(z + f'(r)t) + p^{2k}t^2 g(t)$.

Hensel's Lemma

Theorem

- *Let $f(x)$ be a polynomial with integer or p-adic coefficients.*
- *If $f(r) \equiv 0 \pmod{p^k}$ and $f'(r) \not\equiv 0 \pmod{p}$ [non-degenerate], then*
- *(1) there is an integer s such that $f(s) \equiv 0 \pmod{p^{k+1}}$ [lifting]*
- *(2) and $r \equiv s \pmod{p^k}$ [consistency]*

- Since $r \equiv s \pmod{p^k}$ [consistency], we have $s = r + tp^k$ for some $t \in \mathbb{Z}$.
- If we find a t, then we are done, since that is the unknown to find s.
- $f(s) = f(r + tp^k) = f(r) + f'(r)tp^k + (tp^k)^2(\dots)$.
- $f(s) = f(r + tp^k) = f(r) + f'(r)tp^k + p^{2k}t^2 g(t)$ for some $g(t) \in \mathbb{Z}[t]$.
- Since $f(r) \equiv 0 \pmod{p^k}$, we have $f(r) = zp^k$ for some $z \in \mathbb{Z}$.
- $f(s) = f(r + tp^k) = zp^k + f'(r)tp^k + p^{2k}t^2 g(t)$.
- $f(s) = f(r + tp^k) = p^k(z + f'(r)t) + p^{2k}t^2 g(t)$.
- We need $f(s) \equiv 0 \pmod{p^{k+1}}$ for [lifting].
- $f(s) \equiv 0 \pmod{p^{k+1}}$ iff $p^k(z + f'(r)t) \equiv 0 \pmod{p^{k+1}}$ (Substituting $f(s)$, terms die: p^{k+2} factor)

Hensel's Lemma

Theorem

- *Let $f(x)$ be a polynomial with integer or p-adic coefficients.*
- *If $f(r) \equiv 0 \pmod{p^k}$ and $f'(r) \not\equiv 0 \pmod{p}$ [non-degenerate], then*
- *(1) there is an integer s such that $f(s) \equiv 0 \pmod{p^{k+1}}$ [lifting]*
- *(2) and $r \equiv s \pmod{p^k}$ [consistency]*

- Since $r \equiv s \pmod{p^k}$ [consistency], we have $s = r + tp^k$ for some $t \in \mathbb{Z}$.
- If we find a t, then we are done, since that is the unknown to find s.
- $f(s) = f(r + tp^k) = f(r) + f'(r)tp^k + (tp^k)^2(\dots)$.
- $f(s) = f(r + tp^k) = f(r) + f'(r)tp^k + p^{2k}t^2 g(t)$ for some $g(t) \in \mathbb{Z}[t]$.
- Since $f(r) \equiv 0 \pmod{p^k}$, we have $f(r) = zp^k$ for some $z \in \mathbb{Z}$.
- $f(s) = f(r + tp^k) = zp^k + f'(r)tp^k + p^{2k}t^2 g(t)$.
- $f(s) = f(r + tp^k) = p^k(z + f'(r)t) + p^{2k}t^2 g(t)$.
- We need $f(s) \equiv 0 \pmod{p^{k+1}}$ for [lifting].
- $f(s) \equiv 0 \pmod{p^{k+1}}$ iff $p^k(z + f'(r)t) \equiv 0 \pmod{p^{k+1}}$ (Substituting $f(s)$, terms die: p^{k+2} factor)
- $(z + f'(r)t) \equiv 0 \pmod{p}$ [p^k factors common]
- $tf'(r) \equiv -z \pmod{p}$. Hence, $t = z[f'(r)]^{-1} \pmod{p}$.
- $f'(r)$ will have an inverse if $f'(r) \not\equiv 0 \pmod{p}$ by virtue of being prime.