Recall the usual absolute value:

\[ |x| := \begin{cases} 
  x & x \geq 0 \\
  -x & x < 0 
\end{cases} \]
Valuations: \( \mathbb{Q} \)

Recall the usual absolute value:

\[ |x| := \begin{cases} x & x \geq 0 \\ -x & x < 0 \end{cases} \]

Are there others?
Valuations: $\mathbb{Q}$

Recall the usual absolute value:

$$|x| := \begin{cases} x & x \geq 0 \\ -x & x < 0 \end{cases}$$

Are there others?

For $F = \mathbb{Q}$ consider

$$|x|_p := p^{-\nu_p(x)}.$$ 

We have

$$|x + y|_p \leq \max\{|x|_p, |y|_p\}, \quad 0|_p = 0.$$ 

The inequality is stronger!
For $F = \mathbb{Q}$ and $d = |\cdot|_p$ we have the stronger inequality

$$d(x, z) \leq \max\{d(x, y), d(y, z)\},$$

the corresponding space is called ultra-metric.
For \( F = \mathbb{Q} \) and \( d = | \cdot |_p \) we have the stronger inequality

\[
d(x, z) \leq \max\{d(x, y), d(y, z)\},
\]

the corresponding space is called ultra-metric. We have the notions of intervals or balls:

\[
\mathcal{B}(a, r) := \{x \in F \mid d(x, a) < r\} \subset \overline{\mathcal{B}}(a, r) := \{x \in F \mid d(x, a) \leq r\},
\]
Topology

For ultrametric absolute values, we have

\( b \in \mathcal{B}(a, r) \Rightarrow \mathcal{B}(a, r) = \mathcal{B}(b, r) \)
For ultrametric absolute values, we have

\[ b \in \mathcal{B}(a, r) \Rightarrow \mathcal{B}(a, r) = \mathcal{B}(b, r) \quad \text{(same for} \bar{\mathcal{B}}) \]
For ultrametric absolute values, we have

1. $b \in \mathcal{B}(a, r) \Rightarrow \mathcal{B}(a, r) = \mathcal{B}(b, r)$ (same for $\bar{\mathcal{B}}$)
2. $a, b \in F, r, s \in \mathbb{R}_{\geq 0} \Rightarrow$ If

   $$\mathcal{B}(a, r) \cap \mathcal{B}(b, s) \neq \emptyset$$

   then either

   $$\mathcal{B}(a, r) \subseteq \mathcal{B}(b, s) \quad \text{or} \quad \mathcal{B}(a, r) \supseteq \mathcal{B}(b, s).$$
Sequences, limits

\[ F, |\cdot| \]

**Cauchy sequence:** \( \{x_n\} \) for all \( \epsilon > 0 \) there exists an \( N = N(\epsilon) \) such that

\[ |x_n - x_m| < \epsilon \quad \forall n, m > N. \]
Sequences, limits

$F, | \cdot |$

**Cauchy sequence:** $\{x_n\}$ for all $\epsilon > 0$ there exists an $N = N(\epsilon)$ such that

$$|x_n - x_m| < \epsilon \quad \forall n, m > N.$$

$F$ is **complete** iff all Cauchy sequences in $F$ have a limit in $F$. 

Example: $\mathbb{Q}$ is dense in $\mathbb{R}$. 
Sequences, limits

$F, | \cdot |$

Cauchy sequence: \( \{ x_n \} \) for all \( \epsilon > 0 \) there exists an \( N = N(\epsilon) \) such that

\[
| x_n - x_m | < \epsilon \quad \forall n, m > N.
\]

\( F \) is complete iff all Cauchy sequences in \( F \) have a limit in \( F \).

A set \( S \subset F \) is dense if for all \( x \in F \) and all \( \epsilon > 0 \)

\[
\mathcal{B}(x, \epsilon) \cap S \neq \emptyset.
\]
Sequences, limits

\( F, |·| \)

**Cauchy sequence:** \( \{x_n\} \) for all \( \epsilon > 0 \) there exists an \( N = N(\epsilon) \) such that
\[
|x_n - x_m| < \epsilon \quad \forall n, m > N.
\]

\( F \) is **complete** iff all Cauchy sequences in \( F \) have a limit in \( F \).

A set \( S \subset F \) is **dense** if for all \( x \in F \) and all \( \epsilon > 0 \)
\[
B(x, \epsilon) \cap S \neq \emptyset.
\]

**Example:** \( \mathbb{Q} \) is dense in \( \mathbb{R} \).
Sequences, limits

Consider $F = \mathbb{Q}$ with $| \cdot |_p$. A sequence $\{x_n\}$ is **Cauchy** iff

$$\lim_{n \to \infty} |x_{n+1} - x_n|_p \to 0$$

Note the difference to the real case! In particular, $\sum x_n$ converges iff $|x_n|_p \to 0!$
Consider $F = \mathbb{Q}$ with $|\cdot|_p$. A sequence $\{x_n\}$ is Cauchy iff

$$\lim_{n \to \infty} |x_{n+1} - x_n|_p \to 0$$

Note the difference to the real case!

In particular, $\sum_n x_n$ converges iff $|x_n|_p \to 0$!
Consider $F = \mathbb{Q}$ with $| \cdot |_p$. A sequence $\{x_n\}$ is **Cauchy** iff

$$\lim_{{n \to \infty}} |x_{n+1} - x_n|_p \to 0$$

Note the difference to the real case!

In particular, $\sum_n x_n$ converges iff $|x_n|_p \to 0$!

$\mathbb{Q}$ is **not** complete with respect to $| \cdot |_p$. 
Just as in the classical case, we construct a completion as follows: embed \( \mathbb{Q} \) into \( C := \{ \text{Cauchy sequences} \} \), which contains \( \mathcal{N} := \{ \text{sequences converging to 0} \} \).
Just as in the classical case, we construct a completion as follows: embed \( \mathbb{Q} \) into

\[ C := \{ \text{Cauchy sequences} \}, \]

which contains

\[ \mathcal{N} := \{ \text{sequences converging to 0} \}. \]

Put

\[ \mathbb{Q}_p := C / \mathcal{N}. \]
Completions

Just as in the classical case, we construct a completion as follows: embedd $\mathbb{Q}$ into

$$C := \{ \text{ Cauchy sequences } \},$$

which contains

$$N := \{ \text{ sequences converging to 0} \}.$$ 

Put

$$\mathbb{Q}_p := C / N.$$ 

This is a complete field containing $\mathbb{Q}$:

$$\mathbb{Q} \hookrightarrow \mathbb{Q}_p.$$
Completions

\[ \mathbb{Q} \hookrightarrow \mathbb{R}, \quad \mathbb{Q} \hookrightarrow \mathbb{Q}_p = \left\{ \sum_{j \geq -r} a_j p^j, a_j \in [0, \ldots, p - 1] \right\}, \]

the Laurent power series ring. This representation is unique!
Completions

\( \mathbb{Q} \hookrightarrow \mathbb{R}, \quad \mathbb{Q} \hookrightarrow \mathbb{Q}_p = \left\{ \sum_{j \geq -r} a_j p^j, a_j \in [0, \ldots, p - 1] \right\}, \)

the Laurent power series ring. This representation is unique!

There is a distinguished subring

\( \mathbb{Z}_p := \left\{ \sum_{j \geq 0} a_j p^j, a_j \in [0, \ldots, p - 1] \right\}, \)

which contains an ideal

\( \mathfrak{m}_p := p\mathbb{Z}_p, \)

with quotient field

\( \mathbb{Z}_p / p\mathbb{Z}_p \cong \mathbb{Z} / p\mathbb{Z} \cong \mathbb{F}_p \)
Completions

How do we recognize $\mathbb{Q}$ in $\mathbb{R}$ or $\mathbb{Q}_p$?

Example:

$$\frac{1}{3} = 0.33333 \text{ periodic}$$
Completions

How do we recognize \( \mathbb{Q} \) in \( \mathbb{R} \) or \( \mathbb{Q}_p \)?

Example:

\[
\frac{1}{3} = 0.33333 \quad \text{periodic}
\]

Theorem

\[
x = \sum a_n p^n, \quad x \in \mathbb{Q} \quad \text{iff} \quad \{a_j\} \quad \text{is periodic}.
\]
Completions

How do we recognize $\mathbb{Q}$ in $\mathbb{R}$ or $\mathbb{Q}_p$?

Example:

$$\frac{1}{3} = 0.33333 \text{ periodic}$$

Theorem

$$x = \sum a_n p^n, \quad x \in \mathbb{Q} \quad \text{iff} \quad \{a_j\} \text{ is periodic.}$$

$\iff$ If it is periodic, then it is a finite linear combination of expressions

$$\sum_{j \geq 0} p^{s+jt} = p^s \cdot \frac{1}{1 - p^t} \in \mathbb{Q}.$$
Completions

How do we recognize $\mathbb{Q}$ in $\mathbb{R}$ or $\mathbb{Q}_p$?

Example:

$$\frac{1}{3} = 0.33333 \text{ periodic}$$

**Theorem**

$$x = \sum a_n p^n, \quad x \in \mathbb{Q} \iff \{a_j\} \text{ is periodic.}$$

$\iff$ If it is periodic, then it is a finite linear combination of expressions

$$\sum_{j \geq 0} p^{s+jt} = p^s \cdot \frac{1}{1 - p^t} \in \mathbb{Q}.$$

$$\sum p^{n^2}, \quad \sum p^{n!} \notin \mathbb{Q}.$$
$p$-adic numbers

$$-1 = \frac{p - 1}{1 - p} = (p - 1) + (p - 1) \cdot p + (p - 1) \cdot p^2 + \cdots$$
$p$-adic numbers

\(-1 = \frac{p - 1}{1 - p} = (p - 1) + (p - 1) \cdot p + (p - 1) \cdot p^2 + \cdots\)

\[
\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2 = \begin{cases} 
\mathbb{Z}/2 \times \mathbb{Z}/2 = \{1, p, v, pv\} & p > 2 \\
(\mathbb{Z}/2)^3 = \{\pm 1, \pm 5, \pm 2, \pm 10\} & p = 2
\end{cases}
\]
$p$-adic numbers

\[-1 = \frac{p - 1}{1 - p} = (p - 1) + (p - 1) \cdot p + (p - 1) \cdot p^2 + \cdots\]

\[
\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2 = \begin{cases} 
\mathbb{Z}/2 \times \mathbb{Z}/2 = \{1, p, v, pv\} & p > 2 \\
(\mathbb{Z}/2)^3 = \{\pm1, \pm5, \pm2, \pm10\} & p = 2
\end{cases}
\]

Recall:

\[
\mathbb{R}^\times / (\mathbb{R}^\times)^2 = \mathbb{Z}/2
\]
Hensel’s lemma

**Theorem**

Let

\[ f = \sum_{j=0}^{N} a_j x^j \in \mathbb{Z}_p[x]. \]

Assume that

- \( f(\alpha_0) \equiv 0 \pmod{p} \)
- \( f'(\alpha_0) \not\equiv 0 \pmod{p} \)

Then there exists an \( \alpha \in \mathbb{Z}_p \) with

\[ f(\alpha) = 0 \quad \text{and} \quad \alpha \equiv \alpha_0 \pmod{p}. \]

**Meaning:** Look for zeroes of polynomial functions in \( \mathbb{Q}_p \).
Hensel’s lemma

Analogy: Over $\mathbb{R}$, with $y = f(x)$, write

$$y = f'(\alpha_0)(x - \alpha_0) + f(\alpha_0)$$
Hensel’s lemma

**Analogy:** Over $\mathbb{R}$, with $y = f(x)$, write

$$y = f'(\alpha_0)(x - \alpha_0) + f(\alpha_0)$$

Then we can iterate (Newton’s method)

$$\alpha_1 := -\frac{f(\alpha_0)}{f'(\alpha_0)} + \alpha_0, \ldots$$
Newton’s method
Hensel’s lemma – proof

In \( \mathbb{Q}_p \), via Newton’s method, iteratively:

\[
\alpha_1 = \alpha_0 + b_0 p,
\]

\[
b_0 p = \alpha_1 - \alpha_0
\]

\[
f(\alpha_1) = f(\alpha_0) + f'(\alpha_0) \underbrace{b_0 p}_{p \cdot x} + \cdots
\]

\[
b_0 = -\frac{x}{f'(\alpha_0)}
\]

\[
\alpha_1 := -\left( \frac{f(\alpha_0)}{p} \right) \cdot \frac{1}{f'(\alpha_0)} \cdot p + \alpha_0
\]

\[
= -\frac{f(\alpha_0)}{f'(\alpha_0)} + \alpha_0 \cdots
\]
Hensel’s lemma – proof

Build a sequence, inductively,

\[ \alpha_n := \alpha_{n-1} - \frac{f(\alpha_{n-1})}{f'(\alpha_{n-1})} \]

- \( \alpha_{n+1} \equiv \alpha_n \pmod{p^{n+1}} \)
- \( f(\alpha_n) \equiv 0 \pmod{p^{n+1}} \)
Hensel’s lemma – proof

Build a sequence, inductively,

$$\alpha_n := \alpha_{n-1} - \frac{f(\alpha_{n-1})}{f'(\alpha_{n-1})}$$

- $\alpha_{n+1} \equiv \alpha_n \pmod{p^{n+1}}$
- $f(\alpha_n) \equiv 0 \pmod{p^{n+1}}$

This sequence satisfies the Cauchy condition. Put

$$\alpha = \lim_{n \to \infty} \alpha_n.$$
Newton’s method: convergence

In $\mathbb{R}$ this does not always converge.
Newton’s method: convergence

In $\mathbb{R}$ this does not always converge.

**Example:**

$$f(x) := x^3 - x$$

- $\alpha_1 = \frac{1}{\sqrt{5}}$

- $\alpha_2 = \frac{1}{\sqrt{5}} - \left( \frac{1}{5\sqrt{5}} - \frac{1}{\sqrt{5}} \right) \cdot \left( \frac{3}{5} - 1 \right)$

  $$= - \frac{1}{\sqrt{5}}$$

- $\alpha_3 = \frac{1}{\sqrt{5}}$
Newton’s method: convergence

The algorithm works for $\text{deg}(f) = 2$. 

Theorem (Smale’s conjecture / McMullen (1987))

If $\text{deg}(f) \geq 4$ then there does not exist an iterative algorithm for root finding which would be applicable to almost all polynomials for almost all initial values.

OK for $\text{deg}(f) = 3$. 

Newton’s method: convergence

The algorithm works for $\deg(f) = 2$.

**Theorem (Smale’s conjecture / McMullen (1987))**

If $\deg(f) \geq 4$ then there does not exist an iterative algorithm for root finding which would be applicable to almost all polynomials for almost all initial values.
Newton’s method: convergence

The algorithm works for $\text{deg}(f) = 2$.

**Theorem (Smale’s conjecture / McMullen (1987))**

*If $\text{deg}(f) \geq 4$ then there does not exist an iterative algorithm for root finding which would be applicable to almost all polynomials for almost all initial values.*

OK for $\text{deg}(f) = 3$. 
Applications of Hensel’s method

- \( p > 2, \ f(x) = x^2 - a, \ f'(x) = 2x. \)
Applications of Hensel’s method

- $p > 2$, $f(x) = x^2 - a$, $f'(x) = 2x$. If $\left(\frac{a}{p}\right) = -1$, then $a, p, ap$ have no roots in $\mathbb{Q}_p$. 

Indeed, consider $x^m - 1$. We seek $\alpha$ such that $\alpha^m \equiv 1 \pmod{p}$ and $\alpha^m \not\equiv 1 \pmod{p}$.
Applications of Hensel’s method

- $p > 2$, $f(x) = x^2 - a$, $f'(x) = 2x$. If $\left(\frac{a}{p}\right) = -1$, then $a, p, ap$ have no roots in $\mathbb{Q}_p$. If $\left(\frac{a}{p}\right) = 1$ we get roots in $\mathbb{Q}_p$. 

Indeed, consider $x^m - 1$. We seek $\alpha$ such that $\alpha^m \equiv 1 \pmod{p}$ and $\alpha \not\equiv 1 \pmod{p}$. 

Recall that $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$ is cyclic. It follows that $m \mid (p-1)$. 

Lecture 4
Applications of Hensel’s method

- $p > 2$, $f(x) = x^2 - a$, $f'(x) = 2x$. If $\left( \frac{a}{p} \right) = -1$, then $a, p, ap$ have no roots in $\mathbb{Q}_p$. If $\left( \frac{a}{p} \right) = 1$ we get roots in $\mathbb{Q}_p$.

- If $p \nmid m$ then
  
  \[ \zeta_m \in \mathbb{Q}_p \iff m \mid (p - 1). \]

  Indeed, consider $x^m - 1$. We seek $\alpha_1$ such that $\alpha_1^m \equiv 1 \pmod{p}$ and $\alpha_1 \neq 1 \pmod{p}$. 


Applications of Hensel’s method

- If \( p > 2 \), \( f(x) = x^2 - a \), \( f'(x) = 2x \). If \( \left( \frac{a}{p} \right) = -1 \), then \( a, p, ap \) have no roots in \( \mathbb{Q}_p \). If \( \left( \frac{a}{p} \right) = 1 \) we get roots in \( \mathbb{Q}_p \).

- If \( p \nmid m \) then

\[
\zeta_m \in \mathbb{Q}_p \iff m \mid (p - 1).
\]

Indeed, consider \( x^m - 1 \). We seek \( \alpha_1 \) such that \( \alpha_1^m \equiv 1 \pmod{p} \) and \( \alpha_1 \not\equiv 1 \pmod{p} \). Recall that \( (\mathbb{Z}/p)^\times \) is cyclic. It follows that \( m \mid (p - 1) \).
Artin’s conjecture

\[ \mu_{d,r} := \min \left\{ \mu \mid \forall \text{ system of } r \text{ forms of degree } d \text{ in } \mu \text{ variables} \right\} \]

is (nontrivially) solvable in \( \mathbb{Q}_p \)

\[ \mu_d := \mu_{d,1} \]

**Conjecture**

\[ \mu_{d,r} = rd^2. \]
Artin’s conjecture

\[ \mu_{d,r} := \min \{ \mu \mid \forall \text{ system of } r \text{ forms of degree } d \text{ in } \mu \text{ variables} \} \]

is (nontrivially) solvable in \( \mathbb{Q}_p \)

\[ \mu_d := \mu_{d,1} \]

**Conjecture**

\[ \mu_{d,r} = rd^2. \]

**Terjanian 1966:** NO / see homework, form of degree 4 in 18 variables
Artin’s conjecture

**Theorem (Ax-Kochen)**

There exists a $p_0(d)$ such that for all $p > p_0(d)$ one has

$$\mu_p(\mathbb{Q}_p) = d^2.$$
Functions on $\mathbb{Q}_p$

- polynomials
Functions on $\mathbb{Q}_p$

- polynomials
- rational functions
Functions on $\mathbb{Q}_p$

- polynomials
- rational functions
- series $\sum a_n x^n$ with $a_n \in \mathbb{Q}_p$
Functions on $\mathbb{Q}_p$

- polynomials
- rational functions
- series $\sum a_n x^n$ with $a_n \in \mathbb{Q}_p$

We have the notion of continuity:

$$f(x_n) \rightarrow f(x) \quad \text{for} \quad x_n \rightarrow x$$
Convergent series in $\mathbb{Q}_p$

Examples:

- $\sum n!$ is convergent in $\mathbb{Q}_p$
Convergent series in $\mathbb{Q}_p$

Examples:

- $\sum n!$ is convergent in $\mathbb{Q}_p$
- Consider

\[ e^x = \sum \frac{x^n}{n!}. \]

Where does it converge?
Convergent series in $\mathbb{Q}_p$

Examples:

- $\sum n!$ is convergent in $\mathbb{Q}_p$
- Consider $e^x = \sum \frac{x^n}{n!}$.

Where does it converge?

$$|x|_p < p^{-\frac{1}{p-1}}$$
Recall:

\[ \nu_p(n!) = \sum_{k=1}^{n} \nu_p(k). \]

Write \( k = \sum k_i p^i \) and put \( D_p(k) = \sum k_i. \)
Recall:

\[ \nu_p(n!) = \sum_{k=1}^{n} \nu_p(k). \]

Write \( k = \sum k_i p^i \) and put \( D_p(k) = \sum k_i \). Then

\[ \nu_p(k) = \frac{1}{p-1}(1 + D_p(k - 1) - D_p(k)) \]

\[ \nu_p(n!) = \frac{1}{p-1}(n - D_p(n)) \]
\[ \log_p(x + 1) := \sum_{n \geq 1} \frac{x^n}{n} (-1)^{n+1} \]
\( e^x \) in \( \mathbb{Q}_p \)

\[
\log_p(x + 1) := \sum_{n \geq 1} \frac{x^n}{n} (-1)^{n+1}
\]

**Theorem**

\( e^{x+1} \) and \( \log_p(x + 1) \) are inverse to each other for

\[
|x|_p < p^{-\frac{1}{p-1}}.
\]
Convergence of series

\[ f(x) = \sum_{n \geq 0} a_n x^n \]

Convergence radius: \[ r := \limsup \left| a_n \right|^{1/n} \]

For \( |x| < r \) the series converges to a continuous function. For \( a_n \in \mathbb{Z} \), the series converges for \( |x| < 1 \).
Convergence of series

\[ f(x) = \sum_{n \geq 0} a_n x^n \]

Convergence radius:

\[ r := \frac{1}{\limsup |a_n|^{1/n}} \]
Convergence of series

\[ f(x) = \sum_{n \geq 0} a_n x^n \]

Convergence radius:

\[ r := \limsup \frac{1}{n} \left| a_n \right|^{1/n} \]

For \( |x|_p < r \) the series converges to a continuous function.
Convergence of series

\[ f(x) = \sum_{n \geq 0} a_n x^n \]

Convergence radius:

\[ r := \frac{1}{\lim \sup |a_n|^{1/n}} \]

For \(|x|_p < r\) the series converges to a continuous function. For \(a_n \in \mathbb{Z}_p\), the series converges for \(|x|_p < 1\).
Convergence of series

Binomial series:

\[(1 + x)^a = \sum_{n \geq 0} \frac{a(a - 1) \cdots (a - n + 1)}{n!} x^n =: B_{a,p}(x)\]
Convergence of series

Binomial series:

\[(1 + x)^a = \sum_{n \geq 0} \frac{a(a - 1) \cdots (a - n + 1)}{n!} x^n =: B_{a,p}(x)\]

Converges in \(\mathbb{R}, \mathbb{C}\) for \(|x| < 1\) and diverges for \(|x| > 1\).
Convergence of series

**Theorem**

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

$$B_{a,p}(x) \in \mathbb{Z}_p[[x]],$$

in particular, it converges for $|x|_p < 1$. 
Convergence of series

**Theorem**

For \( a \in \mathbb{Z}_p \), we have

\[
B_{a,p}(x) \in \mathbb{Z}_p[[x]],
\]

*in particular, it converges for \( |x|_p < 1 \).*

**Proof:** Let \( a_0 \in \mathbb{N} \) be a good approximation to \( a \in \mathbb{Z}_p \),
\[a_0 > n, \nu_p(a_0 - a) > N.\]
Convergence of series

**Theorem**

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

$$B_{a,p}(x) \in \mathbb{Z}_p[[x]],$$

in particular, it converges for $|x|_p < 1$.

**Proof:** Let $a_0 \in \mathbb{N}$ be a good approximation to $a \in \mathbb{Z}_p$, $a_0 > n, \nu_p(a_0 - a) > N$. Recall that $\mathbb{Z} \subset \mathbb{Z}_p$ is dense.
Convergence of series

**Theorem**

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

$$B_{a,p}(x) \in \mathbb{Z}_p[[x]],$$

in particular, it converges for $|x|_p < 1$.

**Proof:** Let $a_0 \in \mathbb{N}$ be a good approximation to $a \in \mathbb{Z}_p$, $a_0 > n, \nu_p(a_0 - a) > N$. Recall that $\mathbb{Z} \subset \mathbb{Z}_p$ is dense. By the continuity of polynomials,

$$| \left( \frac{a_0}{n} \right) - \left( \frac{a}{n} \right) | \to 0$$
Convergence of series

\[
\frac{1}{1 - q} = 1 + q + q^2 + \cdots
\]

in \( \mathbb{R} \): converges for \(|q| < 1\)
Convergence of series

\[ \frac{1}{1 - q} = 1 + q + q^2 + \cdots \]

- in \( \mathbb{R} \): converges for \( |q| < 1 \)
- in \( \mathbb{Q}_3 \): \( \sum_{n \geq 0} 3^n \) converges to \( \frac{1}{1 - 3} = -\frac{1}{2} \)
Convergence of series

Example:

\[ B_{\frac{1}{2},7} \left( \frac{7}{9} \right) = 1 + \sum_{n \geq 1} \frac{\frac{1}{2}(\frac{1}{2} - 1) \cdots (\frac{1}{2} - n + 1)}{n!} \left( \frac{7}{9} \right)^n \]

converges in \( \mathbb{Z}_7 \).
Convergence of series

Example:

\[ B_{\frac{1}{2}, 7} \left( \frac{7}{9} \right) = 1 + \sum_{n \geq 1} \frac{\frac{1}{2}(\frac{1}{2} - 1) \cdots (\frac{1}{2} - n + 1)}{n!} \left( \frac{7}{9} \right)^n \]

converges in \( \mathbb{Z}_7 \). We have

\[ 1 > |(1 + \frac{7}{9})^{1/2} - 1|_7 = |\frac{4}{3} - 1|_7 = |\frac{1}{3}|_7 = 1 \]
Convergence of series

Example:

\[ B_{\frac{1}{2},7} \left( \frac{7}{9} \right) = 1 + \sum_{n \geq 1} \frac{\frac{1}{2} \left( \frac{1}{2} - 1 \right) \cdots \left( \frac{1}{2} - n + 1 \right)}{n!} \left( \frac{7}{9} \right)^n \]

converges in \( \mathbb{Z}_7 \). We have

\[ 1 > \left| (1 + \frac{7}{9})^{1/2} - 1 \right|_7 = \left| \frac{4}{3} - 1 \right|_7 = \left| \frac{1}{3} \right|_7 = 1 \]

Where is the problem?
Convergence of series

Example:

\[ B_{\frac{1}{2}, 7} \left( \frac{7}{9} \right) = 1 + \sum_{n \geq 1} \frac{\frac{1}{2} \left( \frac{1}{2} - 1 \right) \cdots \left( \frac{1}{2} - n + 1 \right)}{n!} \left( \frac{7}{9} \right)^n \]

converges in \( \mathbb{Z}_7 \). We have

\[ 1 > |(1 + \frac{7}{9})^{1/2} - 1|_7 = \left| \frac{4}{3} - 1 \right|_7 = \left| \frac{1}{3} \right|_7 = 1 \]

Where is the problem? It is with

\[ \frac{4}{3} = (1 + \frac{7}{9})^{1/2} = \pm \frac{4}{3}. \]
Convergence of series

Example:

\[ B_{\frac{1}{2}, 7} \left( \frac{7}{9} \right) = 1 + \sum_{n \geq 1} \frac{\frac{1}{2}(\frac{1}{2} - 1) \cdots (\frac{1}{2} - n + 1)}{n!} \left( \frac{7}{9} \right)^n \]

converges in \( \mathbb{Z}_7 \). We have

\[ 1 > \left| (1 + \frac{7}{9})^{1/2} - 1 \right|_7 = \left| \frac{4}{3} - 1 \right|_7 = \left| \frac{1}{3} \right|_7 = 1 \]

Where is the problem? It is with

\[ \frac{4}{3} = (1 + \frac{7}{9})^{1/2} = \pm \frac{4}{3}. \]

In \( \mathbb{R} \) the series converges to \( \frac{4}{3} \) and in \( \mathbb{Q}_7 \) to \( -\frac{4}{3} = 1 - \frac{7}{3} \).
Let us prove that $\pi \notin \mathbb{Q}$. Assume $\pi = \frac{a}{b}$.
Convergence of series

Let us prove that $\pi \notin \mathbb{Q}$. Assume $\pi = \frac{a}{b}$. Pick a prime $p \neq 2, p \nmid a$. 

\[
\sin(pb\pi) = \sin(pa) = \sum_{n \geq 0} (-1)^n \left(\frac{a}{b}\right)^{2n+1} (2n+1)! \equiv \frac{a}{b} \not\equiv 0 \pmod{p^2}
\]

This is a contradiction.

Have we proved the result? Where is the problem?
Convergence of series

Let us prove that $\pi \notin \mathbb{Q}$. Assume $\pi = \frac{a}{b}$. Pick a prime $p \neq 2, p \nmid a$.

$$0 = \sin(p b \pi) = \sin(pa)$$

$$= \sum_{n \geq 0} (-1)^n \frac{(pa)^{2n+1}}{(2n+1)!} \equiv pa \not\equiv 0 \pmod{p^2}$$

This is a contradiction.
Let us prove that $\pi \notin \mathbb{Q}$. Assume $\pi = \frac{a}{b}$. Pick a prime $p \neq 2, p \nmid a$.

$$0 = \sin(pb\pi) = \sin(pa)$$

$$= \sum_{n \geq 0} (-1)^n \frac{(pa)^{2n+1}}{(2n+1)!} \equiv pa \not\equiv 0 \pmod{p^2}$$

This is a contradiction.

Have we proved the result? Where is the problem?
Analogies

\[ Z \Leftrightarrow \mathbb{C}[x] \]
Analogies

\[ \mathbb{Z} \iff \mathbb{C}[x] \]

\[ n = \prod p_j^{n_j} \quad \quad f(x) = \prod (x - \alpha_j)^{n_j} \]
Analogies

\[ \mathbb{Z} \leftrightarrow \mathbb{C}[x] \]

\[ n = \prod p_j^{n_j} \quad \quad \quad \quad \quad \quad \quad f(x) = \prod (x - \alpha_j)^{n_j} \]

\[ n = \sum_{j=0}^{N} a_j p^j \quad \quad \quad \quad \quad \quad \quad f(x) = \sum_{j=0}^{N} a_j (x - \alpha)^j \]
Analogies

\[ \mathbb{Z} \iff \mathbb{C}[x] \]

\[ n = \prod_{j} p_{j}^{n_{j}} \]

\[ f(x) = \prod_{j} (x - \alpha_{j})^{n_{j}} \]

\[ n = \sum_{j=0}^{N} a_{j} p^{j} \]

\[ f(x) = \sum_{j=0}^{N} a_{j} (x - \alpha)^{j} \]

\[ \frac{n}{m} = \sum_{j \geq j_{0}} a_{j} p^{j} \]

formal power series

\[ f(x) = \sum_{j \geq j_{0}} a_{j} (x - \alpha)^{j} \]

Laurent series

\[ \frac{f(x)}{g(x)} = \sum_{j \geq j_{0}} a_{j} (x - \alpha)^{j} \]
Analogies

\[ \mathbb{Z} \quad \Leftrightarrow \quad \mathbb{C}[x] \]

\[ n = \prod p_j^{n_j} \quad \Rightarrow \quad f(x) = \prod (x - \alpha_j)^{n_j} \]

\[ n = \sum_{j=0}^{N} a_j p^j \quad \Rightarrow \quad f(x) = \sum_{j=0}^{N} a_j (x - \alpha)^j \]

\[ \frac{n}{m} = \sum_{j \geq j_0} a_j p^j \quad \text{formal power series} \]

\[ f(x) = \sum_{j \geq j_0} a_j (x - \alpha)^j \quad \text{Laurent series} \]

\[ \mathbb{Q} \hookrightarrow \mathbb{Q}_p \quad \Rightarrow \quad \mathbb{C}(x) \hookrightarrow \mathbb{C}((x - \alpha)) \]
Interpolation over $\mathbb{R}$

Given a finite set of pairs

$$(x_j, y_j), \quad j = 0, \ldots, m,$$

find a function (e.g., polynomial) $f$ such that $f(x_j) = y_j$ for all $j$. 
Interpolation over $\mathbb{R}$

Given a finite set of pairs

$$(x_j, y_j), \quad j = 0, \ldots, m,$$

find a function (e.g., polynomial) $f$ such that $f(x_j) = y_j$ for all $j$.

**Solution (Lagrange formula):**

$$f(x) := \sum_{k=0}^{m} y_k \cdot \frac{\prod_{j \neq k}(x - x_j)}{\prod_{j \neq k}(x_k - x_j)}$$

This is a polynomial interpolation of a finite set of points. Another instance of interpolation is approximation via continuity: how does $f(x)$? First for $x \in \mathbb{Q}$, then by continuity, since $\mathbb{Q}$ is dense in $\mathbb{R}$. Lecture 4
Interpolation over $\mathbb{R}$

Given a finite set of pairs

$$(x_j, y_j), \quad j = 0, \ldots, m,$$

find a function (e.g., polynomial) $f$ such that $f(x_j) = y_j$ for all $j$.

Solution (Lagrange formula):

$$f(x) := \sum_{k=0}^{m} y_k \cdot \frac{\prod_{j \neq k} (x - x_j)}{\prod_{j \neq k} (x_k - x_j)}$$

This is a polynomial interpolation of a finite set of points.
Interpolation over $\mathbb{R}$

Given a finite set of pairs

$$(x_j, y_j), \quad j = 0, \ldots, m,$$

find a function (e.g., polynomial) $f$ such that $f(x_j) = y_j$ for all $j$.

**Solution (Lagrange formula):**

$$f(x) := \sum_{k=0}^{m} y_k \cdot \frac{\prod_{j \neq k} (x - x_j)}{\prod_{j \neq k} (x_k - x_j)}$$

This is a polynomial interpolation of a finite set of points. Another instance of interpolation is approximation via continuity: how does one define $a^x$?
Interpolation over $\mathbb{R}$

Given a finite set of pairs

$$(x_j, y_j), \quad j = 0, \ldots, m,$$

find a function (e.g., polynomial) $f$ such that $f(x_j) = y_j$ for all $j$.

**Solution (Lagrange formula):**

$$f(x) := \sum_{k=0}^{m} y_k \cdot \frac{\prod_{j \neq k}(x - x_j)}{\prod_{j \neq k}(x_k - x_j)}$$

This is a polynomial interpolation of a finite set of points. Another instance of interpolation is approximation via continuity: how does one define $a^x$? First for $x \in \mathbb{Q}$, then by **continuity**, since $\mathbb{Q}$ is dense in $\mathbb{R}$. 
Recall that $\mathbb{Z}$ is dense in $\mathbb{Z}_p$. 

Given a finite set (or a sequence) $y_1, \ldots, y_n$ of elements in $\mathbb{Q}_p$ find a continuous function $f: \mathbb{Z}_p \to \mathbb{Q}_p$ such that $f(n) = y_n$, $\forall n$. When is this possible? How does one achieve this?
Interpolation over \( \mathbb{Q}_p \)

Recall that \( \mathbb{Z} \) is dense in \( \mathbb{Z}_p \). Given a finite set (or a sequence) \( y_1, \ldots, \) of elements in \( \mathbb{Q}_p \) find a continuous function

\[ f : \mathbb{Z}_p \rightarrow \mathbb{Q}_p \]

such that

\[ f(n) = y_n, \quad \forall n \]
Recall that \( \mathbb{Z} \) is dense in \( \mathbb{Z}_p \). Given a finite set (or a sequence) \( y_1, \ldots, \) of elements in \( \mathbb{Q}_p \) find a continuous function \( f : \mathbb{Z}_p \rightarrow \mathbb{Q}_p \) such that \( f(n) = y_n, \quad \forall n \).

When is this possible? How does one achieve this?
Interpolation over $\mathbb{Q}_p$

Let us try

$$a^x, \quad a \in \mathbb{Z},$$

$p$-adically.

Need to understand what happens when $x' := x + p^N$.

Consider $a = p$, $x = 0$. Then

$$|a^x - a^{x'}|_p = |1 - p^p p^N|_p = 1,$$

$\forall N$.

Not good, we are not getting closer.
Interpolation over $\mathbb{Q}_p$

Let us try $a^x$, $a \in \mathbb{Z}$, $p$-adically.

Need to understand what happens when $x' := x + p^N$. 
Let us try 

$$a^x, \quad a \in \mathbb{Z},$$

$p$-adically.

Need to understand what happens when $x' := x + p^N$.

Consider $a = p, x = 0$. Then

$$|a^x - a^{x'}|_p = |1 - p^{p^N}|_p = 1, \quad \forall N.$$
Interpolation over $\mathbb{Q}_p$

Let us try $a^x, \quad a \in \mathbb{Z}$, $p$-adically.

Need to understand what happens when $x' := x + p^N$.

Consider $a = p, x = 0$. Then

$$|a^x - a^{x'}|_p = |1 - p^{p^N}|_p = 1, \quad \forall N.$$  

Not good, we are not getting closer.
Interpolation over $\mathbb{Q}_p$: $a^x$

Assume that $1 < a < p$. Then

$$|a^x - a^{x'}|_p = |a^x|_p \cdot |1 - a^{p^N}|_p = 1, \quad \forall N.$$
Interpolation over $\mathbb{Q}_p$: $a^x$

Assume that $1 < a < p$. Then

$$|a^x - a^{x'}|_p = |a^x|_p \cdot |1 - a^{p^N}|_p = 1, \quad \forall N.$$ 

Again, we have a problem.
Interpolation over $\mathbb{Q}_p$: $a^x$

However, let $a \equiv 1 \pmod{p}$, $a = 1 + bp$ and $x' = x + x''p^N$. Then

$$|x' - x|_p \leq \frac{1}{p^N},$$

$$|a^x - a^{x'}|_p = |a^x|_p \cdot |1 - a^{x'-x}|_p = |1 - (1 + bp)^{x''p^N}|_p \leq |p^{N+1}|_p = \frac{1}{p^{N+1}}$$
Interpolation over $\mathbb{Q}_p$: $a^x$

However, let $a \equiv 1 \pmod{p}$, $a = 1 + bp$ and $x' = x + x''p^N$. Then

$$|x' - x|_p \leq \frac{1}{p^N},$$

$$|a^x - a^{x'}|_p = |a^x|_p \cdot |1 - a^{x'-x}|_p = |1 - (1 + bp)^{x''p^N}|_p \leq |p^{N+1}|_p = \frac{1}{p^{N+1}}$$

It follows that for $a \equiv 1 \pmod{p}$, the function

$$f(x) = a^x$$

is well-defined and continuous for $x \in \mathbb{Z}_p$. 
Interpolation over $\mathbb{Q}_p$: $a^x$

Can we do better? Let $a \not\equiv 0 \pmod{p}$. Let $x \equiv x_0 \pmod{p - 1}$. 

Then $a^x \equiv a^{x_0} \cdot (a^{p-1})^x$. The second factor gives a well-defined function.

Consider $S := \{x \in \mathbb{Z}_p \mid x \equiv x_0 \pmod{p-1}\} \subset \mathbb{Z}_p$

This set is dense. Thus, any $f : S \to \mathbb{Z}_p$ will have a unique continuous extension to $\mathbb{Z}_p$. 
Can we do better? Let $a \not\equiv 0 \pmod{p}$. Let $x \equiv x_0 \pmod{p-1}$. Then

$$a^x = a^{x_0} \cdot (a^{p-1})^{x_1}.$$
Can we do better? Let \( a \not\equiv 0 \pmod{p} \). Let \( x \equiv x_0 \pmod{p - 1} \). Then

\[
a^x = a^{x_0} \cdot (a^{p-1})^{x_1}.
\]

The second factor gives a well-defined function.
Can we do better? Let $a \not\equiv 0 \pmod{p}$. Let $x \equiv x_0 \pmod{p-1}$. Then
\[ a^x = a^{x_0} \cdot (a^{p-1})^{x_1}. \]

The second factor gives a well-defined function. Consider
\[ S := \{ x \in \mathbb{N} \mid x \equiv x_0 \pmod{p-1} \} \subset \mathbb{Z}_p \]
Interpolation over \( \mathbb{Q}_p: a^x \)

Can we do better? Let \( a \not\equiv 0 \pmod{p} \). Let \( x \equiv x_0 \pmod{p - 1} \). Then

\[
a^x = a^{x_0} \cdot (a^{p-1})^{x_1}.
\]

The second factor gives a well-defined function. Consider

\[
S := \{ x \in \mathbb{N} \mid x \equiv x_0 \pmod{p - 1} \} \subset \mathbb{Z}_p
\]

This set is dense. Thus, any

\[
f : S \rightarrow \mathbb{Z}_p
\]

will have a unique continuous extension to \( \mathbb{Z}_p \).
Interpolation: the $\Gamma$-function

Recall

$$\Gamma(n + 1) = \int_0^\infty e^{-x} x^n \, dx = n!$$
Recall

\[ \Gamma(n + 1) = \int_{0}^{\infty} e^{-x} x^n \, dx = n! \]

\[ \Gamma(s + 1) = \int_{0}^{\infty} e^{-x} x^s \, dx, \quad s \in \mathbb{C} \]

interpolates (over \( \mathbb{C} \)) between the values \( n! \)
Interpolation: the Γ-function

Note, there does not exist a continuous function

\[ f : \mathbb{Z}_p \to \mathbb{Z}_p, \quad f(n) = n!, \quad \forall n \in \mathbb{N}. \]

Why?  

\( n! \) is too divisible by \( p \).

Try:  

\[ \prod_{1 \leq j \leq n, p \nmid j} j \]

Does not work either.
Interpolation: the Γ-function

Note, there does not exist a continuous function

\[ f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p, \quad f(n) = n!, \quad \forall n \in \mathbb{N}. \]

Why?

\[ n! \text{ is too divisible by } p. \]

Try:

\[ \prod_{1 \leq j \leq n, p \nmid j} j \]

Does not work either.
Interpolation: the $\Gamma$-function

Note, there does not exist a continuous function

$$f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p, \quad f(n) = n!, \quad \forall n \in \mathbb{N}.$$  

Why? $n!$ is too divisible by $p$. 
Interpolation: the $\Gamma$-function

Note, there does not exist a continuous function

$$f : \mathbb{Z}_p \to \mathbb{Z}_p, \quad f(n) = n!, \quad \forall n \in \mathbb{N}.$$  

Why? $n!$ is too divisible by $p$.

Try:

$$\prod_{1 \leq j \leq n, \ p \nmid j} j$$
Interpolation: the $\Gamma$-function

Note, there does not exist a continuous function

$$f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p, \quad f(n) = n!, \quad \forall n \in \mathbb{N}.$$  

Why? $n!$ is too divisible by $p$.

Try:

$$\prod_{1 \leq j \leq n, \ p \nmid j} j$$

Does not work either.
Interpolation: the $\Gamma$-function

**Theorem**

Let $p \geq 3$ be a prime. The function

$$n \mapsto (-1)^n \prod_{j \leq n, \ p \nmid j} j$$

admits a continuous extension to

$$\Gamma_p : \mathbb{Z}_p \to \mathbb{Z}_p$$
Proof: We need to show that

\[ n' = n + n_1 p^N \quad \Rightarrow \quad \Gamma_p(n) \equiv \Gamma_p(n') \pmod{p^N}. \]
Proof: We need to show that

\[ n' = n + n_1 p^N \implies \Gamma_p(n) \equiv \Gamma_p(n') \pmod{p^N}. \]

First, observe that

\[ \Gamma_p(n) \in \mathbb{Z}_p^\times = \mathbb{Z}_p \setminus p\mathbb{Z}_p \]
\[ 1 \equiv \frac{\Gamma_p(n')}{\Gamma_p(n)} = (-1)^n \cdot \prod_{n \leq j < n'} j \quad (\text{mod } p^N) \]
\[ 1 \equiv \frac{\Gamma_p(n')}{\Gamma_p(n)} = (-1)^n \cdot \prod_{n \leq j < n'} j \quad \text{(mod } p^N) \]

Indeed, assume first \( n_1 = 1 \). Note that \((-1)^{p^N} = -1\), thus we need to show that

\[ \prod_{n \leq j < n + p^N} j \equiv -1 \quad \text{(mod } p^N) \]

\[ \equiv \prod_{0 < j < p^N, p \nmid j} j \]

\[ \equiv \prod_j jj' \cdot 1 \cdot (-1) \]

the only solutions to \( j^2 = 1 \) are \( j = 1, -1 \) (mod \( p^N \)).
\[ 1 \equiv \frac{\Gamma_p(n')}{\Gamma_p(n)} = (-1)^n \cdot \prod_{n \leq j < n'} j \quad (\text{mod } p^N) \]

Indeed, assume first \( n_1 = 1 \). Note that \((-1)^{p^N} = -1\), thus we need to show that

\[ \prod_{n \leq j < n+p^N} j \equiv -1 \quad (\text{mod } p^N) \]

\[ \equiv \prod_{0<j<p^N, p\nmid j} j \]

\[ \equiv \prod_{1} jj' \cdot 1 \cdot (-1) \]

The only solutions to \( j^2 = 1 \) are \( j = 1, -1 \) (mod \( p^N \)). A similar argument works for arbitrary \( n_1 \).
\[ \frac{\Gamma_p(a+1)}{\Gamma_p(a)} = \begin{cases} 
-1 & a \in \mathbb{Z}_p^* \\
-1 & a \in p\mathbb{Z}_p 
\end{cases} \]

Indeed, may assume that \( a \in \mathbb{N} \) and use the definition.
\( \Gamma_p: \) Properties

\[
\frac{\Gamma_p(a + 1)}{\Gamma_p(a)} = \begin{cases} 
-a & a \in \mathbb{Z}_p^\times \\
-1 & a \in p\mathbb{Z}_p
\end{cases}
\]

Indeed, may assume that \( a \in \mathbb{N} \) and use the definition.

Let \( a := a_0 + pa_1 \), with \( p \nmid a_0 \). Then

\[
\Gamma_p(a) \cdot \Gamma_p(1 - a) = (-1)^a_0
\]
\( \Gamma_p: \text{ Properties} \)

\[
\frac{\Gamma_p(a + 1)}{\Gamma_p(a)} = \begin{cases} 
-\frac{a}{a} & a \in \mathbb{Z}_p^\times \\
-1 & a \in p\mathbb{Z}_p
\end{cases}
\]

Indeed, may assume that \( a \in \mathbb{N} \) and use the definition.

Let \( a := a_0 + pa_1 \), with \( p \nmid a_0 \). Then

\[
\Gamma_p(a) \cdot \Gamma_p(1 - a) = (-1)^{a_0}
\]

Again, may assume \( a \in \mathbb{Z} \). Check \( a = 1 \):

\[
\Gamma_p(1) = -1, \quad \Gamma_p(0) = -\Gamma_p(1) = 1
\]
\[ \frac{\Gamma_p(a + 1)}{\Gamma_p(a)} = \begin{cases} -a & a \in \mathbb{Z}_p^\times \\ -1 & a \in p\mathbb{Z}_p \end{cases} \]

Indeed, may assume that \( a \in \mathbb{N} \) and use the definition.

Let \( a := a_0 + pa_1 \), with \( p \nmid a_0 \). Then

\[ \Gamma_p(a) \cdot \Gamma_p(1 - a) = (-1)^{a_0} \]

Again, may assume \( a \in \mathbb{Z} \). Check \( a = 1 \):

\[ \Gamma_p(1) = -1, \quad \Gamma_p(0) = -\Gamma_p(1) = 1 \]

Then apply induction:

\[ \frac{\Gamma_p(a + 1) \cdot \Gamma_p(1 - (a + 1))}{\Gamma_p(a) \cdot \Gamma_p(1 - a)} = \begin{cases} -a/(-(-a)) = -1 & a \in \mathbb{Z}_p^\times \\ -1/(-1) = 1 & a \in p\mathbb{Z}_p \end{cases} \]
$\Gamma_p: \text{ Properties}$

$$\Gamma_p \left( \frac{1}{2} \right)^2 = - \left( \frac{-1}{p} \right)$$
$\Gamma_p: \text{ Properties}$

\[
\Gamma_p \left( \frac{1}{2} \right)^2 = - \left( \frac{-1}{p} \right)
\]

Recall:

\[
\Gamma \left( \frac{1}{2} \right)^2 = \pi.
\]
Artin-Hasse exponential

\[ E_p(x) := \exp(x + \frac{x^p}{p} + \frac{x^{p^2}}{p^2} + \cdots) \]
Artin-Hasse exponential

\[ E_p(x) := \exp(x + \frac{x^p}{p} + \frac{x^{p^2}}{p^2} + \cdots) \]

**Theorem**

This converges for \( |x|_p < 1 \) (better than \( \exp(x) \)).
Artin-Hasse exponential

Proof:

\[\mu(n) := \begin{cases} 
(-1)^r & \text{if } n = p_1 \cdots p_r \text{ distinct primes} \\
0 & \text{otherwise}
\end{cases}\]
Artin-Hasse exponential

Proof:

\[ \mu(n) := \begin{cases} (-1)^r & \text{if } n = p_1 \cdots p_r \text{ distinct primes} \\ 0 & \text{otherwise} \end{cases} \]

Properties:

1. For \( n > 1 \), one has \( \sum_{d|n} \mu(d) = 0 \)
Artin-Hasse exponential

Proof:

\[ \mu(n) := \begin{cases} 
(-1)^r & \text{if } n = p_1 \cdots p_r \text{ distinct primes} \\
0 & \text{otherwise} 
\end{cases} \]

Properties:

1. For \( n > 1 \), one has \( \sum_{d|n} \mu(d) = 0 \)
2. \( \sum_{d|n} |\mu(d)| = 2^k \), where \( k = \# \) of distinct primes dividing \( n \)
Artin-Hasse exponential

Proof:

\[ \mu(n) := \begin{cases} 
(-1)^r & \text{if } n = p_1 \cdots p_r \text{ distinct primes} \\
0 & \text{otherwise} 
\end{cases} \]

Properties:

1. For \( n > 1 \), one has \( \sum_{d|n} \mu(d) = 0 \)

2. \( \sum_{d|n} |\mu(d)| = 2^k \), where \( k = \# \) of distinct primes dividing \( n \)

3. \( \sum_{n \geq 1} -\frac{\mu(n)}{n} \cdot \log(1 - x^n) = x \)
Artin-Hasse exponential

Proof:

\[ \mu(n) := \begin{cases} (-1)^r & \text{if } n = p_1 \cdots p_r \text{ distinct primes} \\ 0 & \text{otherwise} \end{cases} \]

Properties:

1. For \( n > 1 \), one has \( \sum_{d|n} \mu(d) = 0 \)
2. \( \sum_{d|n} |\mu(d)| = 2^k \), where \( k = \# \) of distinct primes dividing \( n \)
3. \( \sum_{n \geq 1} -\frac{\mu(n)}{n} \cdot \log(1 - x^n) = x \)
4. \( \sum_{n \geq 1, p|n} -\frac{\mu(n)}{n} \cdot \log(1 - x^n) = x + \frac{x^p}{p} + \cdots \)
Artin-Hasse exponential

(3) \[ e^x = \prod_{n \geq 1} (1 - x^n)^{-\frac{\mu(n)}{n}} \]
Artin-Hasse exponential

\[(3) \Rightarrow e^x = \prod_{n \geq 1} (1 - x^n)^{-\frac{\mu(n)}{n}}\]

\[(4) \Rightarrow E_p(x) = \prod_{n \geq 1, p \nmid n} (1 - x^n)^{-\frac{\mu(n)}{n}}\]
Artin-Hasse exponential

\[(3) \quad \Rightarrow e^x = \prod_{n \geq 1} (1 - x^n)^{-\frac{\mu(n)}{n}}\]

\[(4) \quad \Rightarrow E_p(x) = \prod_{n \geq 1, p \nmid n} (1 - x^n)^{-\frac{\mu(n)}{n}}\]

As formal power series.
Artin-Hasse exponential

(3) \[ e^x = \prod_{n \geq 1} (1 - x^n)^{-\frac{\mu(n)}{n}} \]

(4) \[ E_p(x) = \prod_{n \geq 1, \ p \nmid n} (1 - x^n)^{-\frac{\mu(n)}{n}} \]

As formal power series.

**Theorem**

\[ E_p(x) \in \mathbb{Z}_p[[x]] \]

and thus converges for \(|x|_p < 1\).
Artin-Hasse exponential

Proof: For $p 
mid n$, we have $-\frac{\mu(n)}{n} \in \mathbb{Z}_p$. 
Artin-Hasse exponential

**Proof:** For $p 
mid n$, we have $-\frac{\mu(n)}{n} \in \mathbb{Z}_p$. Thus

$$(1 - x)^{-\frac{\mu(n)}{n}} \in \mathbb{Z}_p[[x]]$$

binomial series expansion
Artin-Hasse exponential

**Proof:** For $p 
mid n$, we have $-\frac{\mu(n)}{n} \in \mathbb{Z}_p$. Thus

$$(1 - x)^{-\frac{\mu(n)}{n}} \in \mathbb{Z}_p[[x]] \quad \text{binomial series expansion}$$

Thus

$$\prod_{n, p \nmid n} (\cdots) \in \mathbb{Z}_p[[x]]$$