Plan

- $p$-adic measures
Plan

- $p$-adic measures
- Kummer congruences
- $p$-adic L-functions
Let $X, T$ be topological spaces.
Let $X, \mathcal{T}$ be topological spaces. A map

$$f : X \to \mathcal{T}$$

is called **locally constant** if for all $x \in X$ there exists an open neighborhood $U := U_x \subset X$ such that the restriction $f|_U$ is constant.
Let $X, \mathcal{T}$ be topological spaces. A map

$$f : X \to \mathcal{T}$$

is called **locally constant** if for all $x \in X$ there exists an open neighborhood $U := U_x \subset X$ such that the restriction $f|_U$ is constant.

**Example:** $X = \mathbb{R}, \mathbb{C}$. Locally constant implies constant.
Measure and integration

Let \( X, \mathcal{T} \) be topological spaces. A map

\[
f : X \to \mathcal{T}
\]

is called **locally constant** if for all \( x \in X \) there exists an open neighborhood \( U := U_x \subset X \) such that the restriction \( f|_U \) is constant.

**Example:** \( X = \mathbb{R}, \mathbb{C} \). Locally constant implies constant.

**Example:** \( X = \mathbb{Z}_p, \mathcal{T} = \mathbb{Q}_p \). Locally constant implies that \( f \) is a finite linear combination of characteristic functions of compact open subsets of the form

\[
\{ a + p^N \mathbb{Z}_p \}.
\]
$p$-adic distributions

Recall that compact open subsets of $\mathbb{Z}_p$ have the form $a + p^n\mathbb{Z}_p$. 
$p$-adic distributions

Recall that compact open subsets of $\mathbb{Z}_p$ have the form $a + p^n\mathbb{Z}_p$.

A $p$-adic distribution $\mu$ on $X \subset \mathbb{Z}_p$ is an additive map from the set of compact open subsets $Y \subseteq X$ to $\mathbb{Q}_p$. 
$p$-adic distributions

Recall that compact open subsets of $\mathbb{Z}_p$ have the form $a + p^n \mathbb{Z}_p$.

A $p$-adic distribution $\mu$ on $X \subset \mathbb{Z}_p$ is an additive map from the set of compact open subsets $Y \subseteq X$ to $\mathbb{Q}_p$.

For all $a + p^N \mathbb{Z}_p \subset X$ one has

$$
\mu(a + p^N \mathbb{Z}_p) = \sum_{b=0}^{p-1} \mu(a + bp^N + p^{N+1} \mathbb{Z}_p).
$$
Recall that compact open subsets of $\mathbb{Z}_p$ have the form $a + p^n\mathbb{Z}_p$.

A $p$-adic distribution $\mu$ on $X \subset \mathbb{Z}_p$ is an additive map from the set of compact open subsets $Y \subseteq X$ to $\mathbb{Q}_p$.

For all $a + p^N\mathbb{Z}_p \subset X$ one has

$$\mu(a + p^N\mathbb{Z}_p) = \sum_{b=0}^{p-1} \mu(a + bp^N + p^{N+1}\mathbb{Z}_p).$$

Conversely, every such map defines a unique distribution.
Recall that compact open subsets of $\mathbb{Z}_p$ have the form $a + p^n\mathbb{Z}_p$.

A $p$-adic distribution $\mu$ on $X \subset \mathbb{Z}_p$ is an additive map from the set of compact open subsets $Y \subseteq X$ to $\mathbb{Q}_p$.

For all $a + p^N\mathbb{Z}_p \subset X$ one has

$$
\mu(a + p^N\mathbb{Z}_p) = \sum_{b=0}^{p-1} \mu(a + bp^N + p^{N+1}\mathbb{Z}_p).
$$

Conversely, every such map defines a unique distribution.

This is called the distribution relation.
Assume we have a distribution of the form

$$\mu_k(a + p^N \mathbb{Z}_p) = p^{N(k-1)} f_k\left(\frac{a}{p^N}\right), \quad a = 0, \ldots, p^N - 1,$$

where $f_k$ is a (monic) polynomial of degree $k$. 
\[ \mu_k(a + p^N \mathbb{Z}_p) = p^{N(k-1)} f_k\left(\frac{a}{p^N}\right), \quad a = 0, \ldots, p^N - 1, \]

Assume we have a distribution of the form

where \( f_k \) is a (monic) polynomial of degree \( k \).

The distribution relation implies that

\[ f_k(x) = p^{-1} \sum_{a=0}^{p-1} f_k\left(\frac{x+a}{p}\right) \]
There is a unique such polynomial, for all $k \geq 1$, namely, the Bernoulli polynomial $B_k(x)$, defined by

$$\frac{te^x}{e^t - 1} = \sum_{k \geq 0} B_k(x) \frac{t^k}{k!}$$
There is a unique such polynomial, for all $k \geq 1$, namely, the Bernoulli polynomial $B_k(x)$, defined by

$$\frac{te^{xt}}{e^t - 1} = \sum_{k \geq 0} B_k(x) \frac{t^k}{k!}$$

Recall, that

$$B_0(x) = 1, \quad B_1(x) = x - 1/2, \quad B_2(x) = x^2 - x + 1/6, \ldots,$$

$$B_k(x) = x^k - \frac{k}{2}x^{k-1} \ldots$$
Thus we have

\[ \mu_{B,k}(a + p^N \mathbb{Z}_p) := p^{N(k-1)} B_k\left( \frac{a}{p^N} \right) \]
$p$-adic distributions

Thus we have

$$\mu_{B,k}(a + p^N \mathbb{Z}_p) := p^{N(k-1)} B_k \left( \frac{a}{p^N} \right)$$

$$\mu_{B,0} = \mu_{Haar}, \quad \text{invariant under translations}$$

$$\mu_{B,1} = \mu_{Mazur}$$
A $p$-adic measure is a distribution $\mu$ such that there exists a $B > 0$ with

$$|\mu(U)|_p \leq B$$

for all compact open $U \subset X$. 
Let $\mu$ be a $p$-adic measure on $\mathbb{Z}_p$ and $f : \mathbb{Z}_p \to \mathbb{Q}_p$ a continuous function.
Let $\mu$ be a $p$-adic measure on $\mathbb{Z}_p$ and $f : \mathbb{Z}_p \rightarrow \mathbb{Q}_p$ a continuous function. Let

$$S_N := \sum_{0 \leq a \leq p^N - 1} f(x_{a,N}) \mu(a + p^N \mathbb{Z}_p),$$

where $x_{a,N} \in a + p^N \mathbb{Z}_p$. Then there exists a limit

$$\lim_{N \to \infty} S_N =: \int_{\mathbb{Z}_p} f \, d\mu.$$

p-adic measures

Let $\mu$ be a $p$-adic measure on $\mathbb{Z}_p$ and $f : \mathbb{Z}_p \rightarrow \mathbb{Q}_p$ a continuous function. Let

$$S_N := \sum_{0 \leq a \leq p^N - 1} f(x_{a,N}) \mu(a + p^N \mathbb{Z}_p),$$

where $x_{a,N} \in a + p^N \mathbb{Z}_p$. Then there exists a limit

$$\lim_{N \to \infty} S_N = : \int_{\mathbb{Z}_p} f \, d\mu$$
**p-adic measures**

**Proof:** Note that

\[
a + p^N \mathbb{Z}_p = \bigcup_{0 \leq \tilde{a} \leq p^M - 1, \tilde{a} \equiv a \pmod{p^N}} (\tilde{a} + p^M \mathbb{Z}_p)
\]
Proof: Note that

\[ a + p^N \mathbb{Z}_p = \bigsqcup_{0 \leq \tilde{a} \leq p^M - 1, \tilde{a} \equiv a \pmod{p^N}} (\tilde{a} + p^M \mathbb{Z}_p) \]

We have

\[ |S_N - S_M|_p = \left| \sum_{0 \leq a \leq p^M - 1} \left( f(x_{\tilde{a},N}) - f(x_{a,M}) \right) \mu(a + p^M \mathbb{Z}_p)|_p \right| \leq \epsilon \cdot B \]

(since \( \mathbb{Z}_p \) is compact, we have uniform continuity).
p-adic measures

Proof: Note that

\[ a + p^N \mathbb{Z}_p = \bigsqcup_{0 \leq \tilde{a} \leq p^M - 1, \tilde{a} \equiv a \pmod{p^N}} \left( \tilde{a} + p^M \mathbb{Z}_p \right) \]

We have

\[ |S_N - S_M|_p = \left| \sum_{0 \leq a \leq p^M - 1} \left( f(x_{\tilde{a},N}) - f(x_{a,M}) \right) \right|_p \leq \epsilon \cdot B \]

(since \( \mathbb{Z}_p \) is compact, we have uniform continuity). Thus, we have a Cauchy sequence, and a limit in \( \mathbb{Q}_p \), independent of the choice of \( x_{\tilde{a},N} \).
Haar “measure”

\[
\mu_{\text{Haar}}(p^N\mathbb{Z}_p) = \frac{1}{p^N} + \text{translation invariance, i.e.,}
\]

\[
\mu_{\text{Haar}}(a + p^N\mathbb{Z}_p) = \frac{1}{p^N}, \quad \forall a.
\]
Haar “measure”

\[
\mu_{\text{Haar}}(p^N \mathbb{Z}_p) = \frac{1}{p^N} + \text{ translation invariance, i.e.,}
\]

\[
\mu_{\text{Haar}}(a + p^N \mathbb{Z}_p) = \frac{1}{p^N}, \quad \forall a.
\]

This satisfies the distribution relation, i.e., \( \mu_{\text{Haar}} \) is a distribution.
Problems: Let

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

\[ x \mapsto x \]
Problems: Let

\[ f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p \]
\[ x \mapsto x \]

Write

\[ \mathbb{Z}_p = \bigsqcup_{a=0}^{p^N-1} (a + p^N\mathbb{Z}_p) \]
Problems: Let

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

\[ x \mapsto x \]

Write

\[ \mathbb{Z}_p = \bigsqcup_{a=0}^{p^N-1} (a + p^N \mathbb{Z}_p) \]

\[ S_{N,\{x_{a,N}\}} = \sum_{a=0}^{p^N-1} f(x_{a,N}) \mu(a + p^N \mathbb{Z}_p) = \sum_a \frac{x_{a,N}}{p^N} \]
For $x_{a,N} := a \in a + p^N \mathbb{Z}_p$ we get

$$
\frac{1}{p^N} \sum_{a=0}^{p^N-1} a = \frac{(p^N - 1)p^N}{2} \cdot \frac{1}{p^N} = \frac{p^N - 1}{2} \rightarrow -\frac{1}{2}
$$
Haar “measure”

For \( x_{a,N} := a \in a + p^N \mathbb{Z}_p \) we get

\[
\frac{1}{p^N} \sum_{a=0}^{p^N-1} a = \frac{(p^N - 1)p^N}{2} \cdot \frac{1}{p^N} = \frac{p^N - 1}{2} \to -\frac{1}{2}
\]

For one \( a \), choose \( x_{a,N} := a + a_0 p^N \in a + p^N \mathbb{Z}_p \), with some \( a_0 \neq 0 \). Then we have

\[
\left( \frac{1}{p^N} \sum_{a=0}^{p^N-1} a \right) + a_0 p^N \cdot \frac{1}{p^N} = \frac{p^N - 1}{2} + a_0 \to -\frac{1}{2} + a_0.
\]
For $x_{a,N} := a \in a + p^N \mathbb{Z}_p$ we get

$$\frac{1}{p^N} \sum_{a=0}^{p^N-1} a = \frac{(p^N - 1)p^N}{2} \cdot \frac{1}{p^N} = \frac{p^N - 1}{2} \to -\frac{1}{2}$$

For one $a$, choose $x_{a,N} := a + a_0 p^N \in a + p^N \mathbb{Z}_p$, with some $a_0 \neq 0$. Then we have

$$\left( \frac{1}{p^N} \sum_{a=0}^{p^N-1} a \right) + a_0 p^N \cdot \frac{1}{p^N} = \frac{p^N - 1}{2} + a_0 \to -\frac{1}{2} + a_0.$$ 

So even simple continuous functions $f$ are not integrable on the compact $\mathbb{Z}_p$. 
p-adic measures

$$\mu_{B,k}(a + p^N \mathbb{Z}_p) := p^{N(k-1)} B_k\left(\frac{a}{p^N}\right)$$
$\mu_{B,k}(a + p^N\mathbb{Z}_p) := p^{N(k-1)}B_k\left(\frac{a}{p^N}\right)$

As we saw, these are distributions.
\[ \mu_{B,k}(a + p^N \mathbb{Z}_p) := p^{N(k-1)} B_k\left(\frac{a}{p^N}\right) \]

As we saw, these are distributions. There is a way to regularize them, i.e., turn them into measures.
As we saw, these are distributions. There is a way to regularize them, i.e., turn them into measures.

For a fixed $\alpha \in \mathbb{Q} \cap \mathbb{Z}_p^\times$, define

$$\mu_{k,\alpha}(U) := \mu_{B,k}(U) - \frac{\mu_{B,k}(\alpha U)}{\alpha^k}$$
Theorem

$\mu_{k,\alpha}$ is a measure for all $k \geq 1$. 

Proof:
First, we show that $|\mu_{1,\alpha}(a + p^N \mathbb{Z}_p)|_p \leq 1, \forall N \geq 1$.

Indeed, by definition,

\[
\mu_{1,\alpha}(a + p^N \mathbb{Z}_p) = a^{p^N - \frac{1}{2} - \frac{1}{2^\alpha}} a^{\frac{\alpha}{2^\alpha} (a^{p^N} - \lfloor a^{p^N} \rfloor)} = \frac{1}{\alpha} - \frac{1}{2} + \frac{1}{\alpha} \lfloor a^{p^N} \rfloor \in \mathbb{Z}_p
\]
Theorem

$\mu_{k,\alpha}$ is a measure for all $k \geq 1$.

Proof: First, we show that

$$|\mu_{1,\alpha}(a + p^N\mathbb{Z}_p)|_p \leq 1, \quad \forall N \geq 1.$$ 

Indeed, by definition,

$$\mu_{1,\alpha}(a + p^N\mathbb{Z}_p) = \frac{a}{p^N} - \frac{1}{2} - \frac{1}{\alpha} \left( \frac{\alpha a}{p^N} - \frac{1}{2} \right)$$

$$= \frac{1/\alpha - 1}{2} + \frac{a}{p^N} - \frac{1}{\alpha} \left( \frac{\alpha a}{p^N} - \left[ \frac{\alpha a}{p^N} \right] \right)$$

$$= \frac{1/\alpha - 1}{2} + \frac{1}{\alpha} \left[ \frac{\alpha a}{p^N} \right] \quad \in \mathbb{Z}_p$$
For $\alpha \in \mathbb{Q} \cap \mathbb{Z}_p^\times$, the element is in $\mathbb{Z}_p$. 

Since any $U$ is a finite (disjoint) union of sets of the form $a_i + pN_i \mathbb{Z}_p$, we obtain the result.

Thus, $\mu_1,\alpha$ is a measure on $\mathbb{Z}_p$. 

---

**p-adic measures**
p-adic measures

For $\alpha \in \mathbb{Q} \cap \mathbb{Z}_p^\times$, the element is in $\mathbb{Z}_p$.

Since any $U$ is a finite (disjoint) union of sets of the form $a_i + p^{N_i} \mathbb{Z}_p$,

$$|\mu_{1,\alpha}(U)|_p \leq \max \ldots$$

and we obtain the result.
p-adic measures

For $\alpha \in \mathbb{Q} \cap \mathbb{Z}_p^\times$, the element is in $\mathbb{Z}_p$.

Since any $U$ is a finite (disjoint) union of sets of the form $a_i + p^{N_i}\mathbb{Z}_p$,

$$|\mu_{1,\alpha}(U)|_p \leq \max \ldots$$

and we obtain the result.

Thus, $\mu_{1,\alpha}$ is a measure on $\mathbb{Z}_p$. 
Now we treat $k \geq 2$. 

Let $d_k$ be the lcm of denominators of coefficients of $B_k(x)$, so that $d_k B_k(x) \in \mathbb{Z}[x]$.

$d_1 = 2$, $d_2 = 6$, $d_3 = 2$, ...
Now we treat $k \geq 2$. Let $d_k$ be the lcm of denominators of coefficients of $B_k(x)$, so that $d_k B_k(x) \in \mathbb{Z}[x]$. 
Now we treat $k \geq 2$. Let $d_k$ be the lcm of denominators of coefficients of $B_k(x)$, so that $d_k B_k(x) \in \mathbb{Z}[x]$.

$$d_1 = 2, \quad d_2 = 6, \quad d_3 = 2, \ldots$$
Now we treat $k \geq 2$. Let $d_k$ be the lcm of denominators of coefficients of $B_k(x)$, so that $d_k B_k(x) \in \mathbb{Z}[x]$.

$$d_1 = 2, \quad d_2 = 6, \quad d_3 = 2, \ldots$$

We will show that

$$|\mu_{k,\alpha}(a + p^N \mathbb{Z}_p)|_p \leq \max \left( \frac{1}{|d_k|_p}, |\mu_{1,\alpha}(a + p^N \mathbb{Z}_p)|_p \right)$$
Recall,

\[ B_k(x) = x^k - \frac{k}{2} x^{k-1} + \ldots \]
We compute $d_k \mu_{k,\alpha}(a + p^N \mathbb{Z}_p)$ as follows:

$$= d_k p^{N(k-1)} \left( B_k \left( \frac{a}{p^N} \right) - \frac{1}{\alpha^k} B_k \left( \frac{\overline{\alpha a}}{p^N} \right) \right)$$
p-adic measures

We compute $d_k \mu_{k, \alpha}(a + p^N \mathbb{Z}_p)$ as follows:

$$= d_k p^{N(k-1)} \left( B_k \left( \frac{a}{p^N} \right) - \frac{1}{\alpha^k} B_k \left( \frac{\alpha a}{p^N} \right) \right)$$

$$\equiv d_k p^{N(k-1)} \left( \left( \frac{a}{p^N} \right)^k - \frac{1}{\alpha^k} \left( \frac{\alpha a}{p^N} \right)^k - \frac{k}{2} \left( \frac{a^{k-1}}{p^{N(k-1)}} - \frac{1}{\alpha^k} \left( \frac{\alpha a}{p^N} \right)^{k-1} \right) \right) \pmod{p^N}$$
p-adic measures

We compute $d_k \mu_{k, \alpha}(a + p^N \mathbb{Z}_p)$ as follows:

$$
= d_k p^{N(k-1)} \left( B_k \left( \frac{a}{p^N} \right) - \frac{1}{\alpha^k} B_k \left( \frac{\overline{\alpha a}}{p^N} \right) \right)
$$

$$
\equiv d_k p^{N(k-1)} \left( \left( \frac{a}{p^N} \right)^k - \frac{1}{\alpha^k} \left( \frac{\overline{\alpha a}}{p^N} \right)^k - \frac{k}{2} \left( \frac{a^{k-1}}{p^{N(k-1)}} - \frac{1}{\alpha^k} \left( \frac{\overline{\alpha a}}{p^N} \right)^{k-1} \right) \right) \pmod{p^N}
$$

Writing

$$
\frac{\overline{\alpha a}}{p^N} = \frac{\alpha a}{p^N} - \left[ \frac{\alpha a}{p^N} \right],
$$

substituting, and simplifying, we obtain:

$$
\equiv d_k \cdot k \cdot a^{k-1} \left( \frac{1}{\alpha} \left[ \frac{\alpha a}{p^N} \right] + \frac{1}{\alpha} - 1 \right) = d_k \cdot k \cdot a^{k-1} \mu_{1, \alpha}(a + p^N \mathbb{Z}_p)
$$
What were we doing?

Over $\mathbb{R}$:

$$\frac{dx^k}{dx} = kx^{k-1}, \quad \mu_k[a, b] = b^k - a^k$$
What were we doing?

Over $\mathbb{R}$:

$$\frac{dx^k}{dx} = kx^{k-1}, \quad \mu_k[a, b] = b^k - a^k$$

$$\lim_{b \to a} \frac{\mu_k([a, b])}{\mu_1([a, b])} = k \cdot a^{k-1}$$
What were we doing?

Over \( \mathbb{R} \):

\[
\frac{dx^k}{dx} = kx^{k-1}, \quad \mu_k[a, b] = b^k - a^k
\]

\[
\lim_{b \to a} \frac{\mu_k([a, b])}{\mu_1([a, b])} = k \cdot a^{k-1}
\]

Over \( \mathbb{Q}_p \):

\[
\frac{\mu_k(a + p^N \mathbb{Z}_p)}{\mu_1(a + p^N \mathbb{Z}_p)} = k \cdot a^{k-1}
\]
What were we doing?

Over \( \mathbb{R} \):

\[
\frac{dx^k}{dx} = kx^{k-1}, \quad \mu_k[a, b] = b^k - a^k
\]

\[
\lim_{b \to a} \frac{\mu_k([a, b])}{\mu_1([a, b])} = k \cdot a^{k-1}
\]

Over \( \mathbb{Q}_p \):

\[
\frac{\mu_k(a + p^N\mathbb{Z}_p)}{\mu_1(a + p^N\mathbb{Z}_p)} = k \cdot a^{k-1}
\]

\[
dx^k \iff \mu_{k, \alpha}
\]
Consider

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

\[ x \mapsto x^{k-1} \]

Let \( X \subset \mathbb{Z}_p \) be a compact open subset. Then

\[ \int_X \mu, \alpha = k \cdot \int_X f \mu, \alpha \]

In particular,

\[ \frac{1}{k} \int_{\mathbb{Z} \times \mathbb{Z}_p} \mu, \alpha = \int_{\mathbb{Z} \times \mathbb{Z}_p} x^{k-1} \mu, \alpha. \]

**Proof:**

It suffices to consider \( a + p^N \mathbb{Z}_p \). We have

\[ \mu, \alpha(a + p^N \mathbb{Z}_p) \equiv k \cdot a^{k-1} \mu, \alpha(a + p^N \mathbb{Z}_p) \pmod{p^N - \nu^d_k} , \]

take \( N \rightarrow \infty \).
Consider

\[ f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p \]
\[ x \mapsto x^{k-1} \]

Let \( X \subset \mathbb{Z}_p \) be a compact open subset. Then

\[ \int_X \mu_{k,\alpha} = k \cdot \int_X f \mu_{1,\alpha} \]
Consider
\[
f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p \\
x \mapsto x^{k-1}
\]
Let \( X \subset \mathbb{Z}_p \) be a compact open subset. Then
\[
\int_X \mu_{k,\alpha} = k \cdot \int_X f \mu_{1,\alpha}
\]
In particular,
\[
\frac{1}{k} \int_{\mathbb{Z}_p^\times} \mu_{k,\alpha} = \int_{\mathbb{Z}_p^\times} x^{k-1} \mu_{1,\alpha}.
\]
Consider
\[ f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p \]
\[ x \mapsto x^{k-1} \]

Let \( X \subset \mathbb{Z}_p \) be a compact open subset. Then
\[
\int_X \mu_{k,\alpha} = k \cdot \int_X f \mu_{1,\alpha}
\]

In particular,
\[
\frac{1}{k} \int_{\mathbb{Z}_p^\times} \mu_{k,\alpha} = \int_{\mathbb{Z}_p^\times} x^{k-1} \mu_{1,\alpha}.
\]

**Proof:** It suffices to consider \( a + p^N\mathbb{Z}_p \). We have
\[
\mu_{k,\alpha}(a + p^N\mathbb{Z}_p) \equiv k \cdot a^{k-1} \mu_{1,\alpha}(a + p^N\mathbb{Z}_p) \pmod{p^{N-\nu_p(d_k)}},
\]

take \( N \rightarrow \infty \).
\[ \int_{\mathbb{Z}_p^\times} \mu_{k,\alpha} = \]
\[ = \mu_{k,\alpha}(\mathbb{Z}_p) - \mu_{k,\alpha}(p\mathbb{Z}_p) \]
\[ = \left( \mu_{B,k}(\mathbb{Z}_p) - \frac{\mu_{B,k}(\alpha\mathbb{Z}_p)}{\alpha^k} \right) - \left( \mu_{B,k}(p\mathbb{Z}_p) - \frac{\mu_{B,k}(\alpha p\mathbb{Z}_p)}{\alpha^k} \right) \]
\[ = (B_k - \frac{B_k}{\alpha^k}) - (B_k \cdot p^{k-1} - \frac{B_k p^{k-1}}{\alpha^k}) \]
\[ = B_k(1 - \frac{1}{\alpha^k})(1 - p^{k-1}) \]
\[ \int_{\mathbb{Z}_p^\times} \mu_{k,\alpha} = \]
\[ = \mu_{k,\alpha}(\mathbb{Z}_p) - \mu_{k,\alpha}(p\mathbb{Z}_p) \]
\[ = \left( \mu_{B,k}(\mathbb{Z}_p) - \frac{\mu_{B,k}(\alpha\mathbb{Z}_p)}{\alpha^k} \right) - \left( \mu_{B,k}(p\mathbb{Z}_p) - \frac{\mu_{B,k}(\alpha p\mathbb{Z}_p)}{\alpha^k} \right) \]
\[ = (B_k - \frac{B_k}{\alpha^k}) - (B_k \cdot p^{k-1} - \frac{B_k p^{k-1}}{\alpha^k}) \]
\[ = B_k \left( 1 - \frac{1}{\alpha^k} \right) \left( 1 - p^{k-1} \right) \]

Thus,
\[ (1 - p^{k-1})\left(-\frac{B_k}{k}\right) = \frac{1}{\alpha^{-k} - 1} \cdot \int_{\mathbb{Z}_p^\times} x^{k-1} \mu_{1,\alpha} \]
Let $S := \{ s \equiv s_0 \pmod{(p - 1)} \} \subset \mathbb{Z}_p$. It is dense.
Back to interpolation

Let \( S := \{ s \equiv s_0 \pmod{(p - 1)} \} \subset \mathbb{Z}_p \). It is dense.

For all \( s, s' \in S \) with \( |s - s'|_p \to 0 \) we have \( |n^s - n^{s'}|_p \to 0 \).

**Proof:** already did this.
Let $S := \{ s \equiv s_0 \pmod{(p - 1)} \} \subset \mathbb{Z}_p$. It is dense.

For all $s, s' \in S$ with $|s - s'|_p \to 0$ we have $|n^s - n^{s'}|_p \to 0$.

**Proof:** already did this.
Thus there is a **continuous** function that interpolates $n^s$. 
Interpolation

For all $k \equiv k' \pmod{(p - 1)p^N}$ we have

$$|x^{k'-1} - x^{k-1}|_p \leq \frac{1}{p^{N+1}}, \quad \forall x \in \mathbb{Z}_p^\times.$$
Interpolation

For all $k \equiv k' \pmod{(p - 1)p^N}$ we have

$$|x^{k'-1} - x^{k-1}|_p \leq \frac{1}{p^{N+1}}, \quad \forall x \in \mathbb{Z}_p^\times.$$

It follows that

$$|\int_{\mathbb{Z}_p^\times} x^{k'-1} \mu_{1,\alpha} - \int_{\mathbb{Z}_p^\times} x^{k-1} \mu_{1,\alpha}| \leq \frac{1}{p^{N+1}}.$$
Interpolation

For all $k \equiv k' \pmod{(p - 1)p^N}$ we have

$$|x^{k'-1} - x^{k-1}|_p \leq \frac{1}{p^{N+1}}, \forall x \in \mathbb{Z}_p^\times.$$

It follows that

$$|\int_{\mathbb{Z}_p^\times} x^{k'-1} \mu_{1, \alpha} - \int_{\mathbb{Z}_p^\times} x^{k-1} \mu_{1, \alpha}| \leq \frac{1}{p^{N+1}}.$$

Thus,

$$k \mapsto \int_{\mathbb{Z}_p^\times} x^{k-1} \mu_{1, \alpha} = \frac{1}{k} \int_{\mathbb{Z}_p^\times} 1 \mu_{1, \alpha}$$

is interpolates to a continuous function on $\mathbb{Z}_p$.  

Theorem (Kummer / Clausen-von Staudt)

1. \( p - 1 \nmid k \Rightarrow |\frac{B_k}{k}|_p \leq 1 \)
Theorem (Kummer / Clausen-von Staudt)

1. \( p - 1 \nmid k \Rightarrow \left| \frac{B_k}{k} \right|_p \leq 1 \)

2. \( p - 1 \nmid k \) and \( k \equiv k' \pmod{(p - 1)p^N} \) \( \Rightarrow \)

\[
(1 - p^{k-1}) \frac{B_k}{k} \equiv (1 - p^{k'-1}) \frac{B_{k'}}{k'} \pmod{p^{N+1}}
\]
Kummer congruences

Theorem (Kummer / Clausen-von Staudt)

1. $p - 1 \nmid k \Rightarrow |\frac{B_k}{k}|_p \leq 1$

2. $p - 1 \nmid k$ and $k \equiv k' \pmod{(p - 1)p^N} \Rightarrow$

\[
(1 - p^{k-1})\frac{B_k}{k} \equiv (1 - p^{k'-1})\frac{B_{k'}}{k'} \pmod{p^{N+1}}
\]

3. $p > 2$, $(p - 1) \mid k \Rightarrow pB_k \equiv -1 \pmod{p}$
Kummer congruences

**Proof:** We will assume \( p > 2 \). Let \( \alpha \) be a primitive root modulo \( p \) (generator of \( (\mathbb{Z}/p\mathbb{Z})^\times \)).
Kummer congruences

**Proof:** We will assume $p > 2$. Let $\alpha$ be a primitive root modulo $p$ (generator of $(\mathbb{Z}/p\mathbb{Z})^\times$). For $k = 1$ we have

$$\left| \frac{B_1}{1} \right|_p = \left| -\frac{1}{2} \right|_p = 1$$

and we are done.
Kummer congruences

Proof: We will assume $p > 2$. Let $\alpha$ be a primitive root modulo $p$ (generator of $(\mathbb{Z}/p\mathbb{Z})^\times$). For $k = 1$ we have

$$\left| \frac{B_1}{1} \right|_p = \left| \frac{1}{2} \right|_p = 1$$

and we are done. For $k \geq 2$, we have

$$\left| \frac{B_k}{k} \right|_p = \left| \frac{1}{\alpha^k - 1} \right|_p \cdot \left| \frac{1}{(1 - p^{k-1})} \right|_p \cdot \left| \int_{\mathbb{Z}_p^\times} x^{k-1} \mu_{1,\alpha} \right|_p$$

$$\left| \int_{\mathbb{Z}_p^\times} x^{k-1} \mu_{1,\alpha} \right|_p \leq 1.$$
Kummer congruences

**Proof:** We will assume $p > 2$. Let $\alpha$ be a primitive root modulo $p$ (generator of $(\mathbb{Z}/p\mathbb{Z})^\times$). For $k = 1$ we have

$$\left| \frac{B_1}{1} \right|_p = \left| -\frac{1}{2} \right|_p = 1$$

and we are done. For $k \geq 2$, we have

$$\left| \frac{B_k}{k} \right|_p = \left| \frac{1}{\alpha^k - 1} \right|_p \cdot \left| \frac{1}{(1 - p^{k-1})} \right|_p \cdot \left| \int_{\mathbb{Z}_p^\times} x^{k-1} \mu_{1,\alpha} \right|_p$$

$$\left| \int_{\mathbb{Z}_p^\times} x^{k-1} \mu_{1,\alpha} \right|_p \leq 1.$$

This proves the first point.
To show the second point, it suffices to establish

$$\frac{1}{\alpha^{-k} - 1} \int_{\mathbb{Z}_p^\times} x^{k-1} \mu_{1,\alpha} \equiv \frac{1}{\alpha^{-k'} - 1} \int_{\mathbb{Z}_p^\times} x^{k'-1} \mu_{1,\alpha} \pmod{p^{N+1}}$$
Kummer congruences

To show the second point, it suffices to establish

$$\frac{1}{\alpha^{-k} - 1} \int_{\mathbb{Z}_p^\times} x^{k-1} \mu_{1,\alpha} \equiv \frac{1}{\alpha^{-k'} - 1} \int_{\mathbb{Z}_p^\times} x^{k'-1} \mu_{1,\alpha} \quad (\text{mod } p^{N+1})$$

With our assumptions, we have

$$(\alpha^{-k} - 1)^{-1} \equiv (\alpha^{-k'} - 1)^{-1} \quad (\text{mod } p^{N+1}) \iff$$

$$\alpha^k \equiv \alpha^{k'} \quad (\text{mod } p^{N+1})$$
Kummer congruences

To show the second point, it suffices to establish

\[
\frac{1}{\alpha^{-k} - 1} \int_{\mathbb{Z}_p^\times} x^{k-1} \mu_{1,\alpha} \equiv \frac{1}{\alpha^{-k'} - 1} \int_{\mathbb{Z}_p^\times} x^{k'-1} \mu_{1,\alpha} \pmod{p^{N+1}}
\]

With our assumptions, we have

- \((\alpha^{-k} - 1)^{-1} \equiv (\alpha^{-k'} - 1)^{-1} \pmod{p^{N+1}} \iff \alpha^k \equiv \alpha^{k'} \pmod{p^{N+1}}

- \(x^{k-1} \equiv x^{k'-1} \pmod{p^{N+1}}\)
Kummer congruences

To show the second point, it suffices to establish

\[ \frac{1}{\alpha^{-k} - 1} \int_{\mathbb{Z}_p^\times} x^{k-1} \mu_{1, \alpha} \equiv \frac{1}{\alpha^{-k'} - 1} \int_{\mathbb{Z}_p^\times} x^{k'-1} \mu_{1, \alpha} \pmod{p^{N+1}} \]

With our assumptions, we have

\( (\alpha^{-k} - 1)^{-1} \equiv (\alpha^{-k'} - 1)^{-1} \pmod{p^{N+1}} \iff \alpha^k \equiv \alpha^{k'} \pmod{p^{N+1}} \)

\( x^{k-1} \equiv x^{k'-1} \pmod{p^{N+1}} \)

same for the integral.
Kummer congruences

To prove the third point, put $\alpha = p + 1$. Then

$$pB_k = -kp\left(-\frac{B_k}{k}\right) = \frac{-kp}{\alpha^{-k} - 1}(1 - p^{k-1}) \int_{\mathbb{Z}_p^\times} x^{k-1} \mu_{1,\alpha}$$
Kummer congruences

To prove the third point, put $\alpha = p + 1$. Then

$$pB_k = -kp\left(-\frac{B_k}{k}\right) = \frac{-kp}{\alpha^{-k} - 1} (1 - p^{k-1}) \int_{\mathbb{Z}_p^\times} x^{k-1} \mu_{1,\alpha}$$

Let $d = \nu_p(k)$. Then

$$(\alpha^{-k} - 1) = (1 + p)^{-k} - 1 \equiv -kp \pmod{p^{d+2}}$$
Kummer congruences

To prove the third point, put $\alpha = p + 1$. Then

$$pB_k = -kp\left(-\frac{B_k}{k}\right) = \frac{-kp}{\alpha^{-k} - 1}(1 - p^{k-1}) \int_{\mathbb{Z}_p^\times} x^{k-1} \mu_{1,\alpha}$$

Let $d = \nu_p(k)$. Then

$$(\alpha^{-k} - 1) = (1 + p)^{-k} - 1 \equiv -kp \pmod{p^{d+2}}$$

We have

$$1 \equiv \frac{-kp}{\alpha^{-k} - 1} \pmod{p}$$
Kummer congruences

To prove the third point, put $\alpha = p + 1$. Then

$$pB_k = -kp\left(-\frac{B_k}{k}\right) = \frac{-kp}{\alpha^{-k} - 1}(1 - p^{k-1}) \int_{\mathbb{Z}_p^\times} x^{k-1} \mu_{1,\alpha}$$

Let $d = \nu_p(k)$. Then

$$(\alpha^{-k} - 1) = (1 + p)^{-k} - 1 \equiv -kp \pmod{p^{d+2}}$$

We have

- $$(\alpha^{-k} - 1) = (1 + p)^{-k} - 1 \equiv -kp \pmod{p^{\nu_p(d)+2}}$$

$$1 \equiv \frac{-kp}{\alpha^{-k} - 1} \pmod{p}$$
Kummer congruences

Since \((p - 1) \mid k\), we have

\[ x^{k-1} \equiv x^{-1} \pmod{p} \]

Then

\[ pB_k \equiv \int_{\mathbb{Z}_p^\times} x^{k-1} \mu_{1,\alpha} \equiv \int_{\mathbb{Z}_p^\times} x^{-1} \mu_{1,\alpha} \]
Kummer congruences

Since \((p - 1) \mid k\), we have

\[ x^{k-1} \equiv x^{-1} \pmod{p} \]

Then

\[ pB_k \equiv \int_{\mathbb{Z}_p^\times} x^{k-1} \mu_{1,\alpha} \equiv \int_{\mathbb{Z}_p^\times} x^{-1} \mu_{1,\alpha} \equiv -1 \pmod{p}, \]

the last congruence by direct computation.
Bernoulli numbers

IRREGULAR PRIMES TO TWO BILLION

WILLIAM HART, DAVID HARVEY, AND WILSON ONG

Abstract. We compute all irregular primes less than \(2^{31} = 2147483648\). We verify the Kummer–Vandiver conjecture for each of these primes, and we check that the \(p\)-part of the class group of \(\mathbb{Q}(\zeta_p)\) has the simplest possible structure consistent with the index of irregularity of \(p\). Our method for computing the irregular indices saves a constant factor in time relative to previous methods, by adapting Rader’s algorithm for evaluating discrete Fourier transforms.

1. Introduction and Summary of Results

For each of the 105,097,564 odd primes less than \(2^{31} = 2147483648\), we performed the following tasks:

(1) We computed the irregular indices for \(p\), that is, the integers \(r \in \{2, 4, \ldots, p-3\}\) for which \(B_r \equiv 0 \pmod{p}\), where \(B_r\) is the \(r\)-th Bernoulli number. A pair \((p, r)\), with \(r\) as above, is called an irregular pair, and such an integer \(r\) is called an irregular index for \(p\). The number of such \(r\) is called the index of irregularity of \(p\), denoted \(i_p\). A prime \(p\) is called regular if \(i_p = 0\), and irregular if \(i_p > 0\).
Bernoulli numbers

The total running time of our computation was approximately 8.6 million core-hours (almost 1000 core-years).
Bernoulli numbers

The total running time of our computation was approximately 8.6 million core-hours (almost 1000 core-years).

We found many new primes with \( i_p = 7 \), four primes with \( i_p = 8 \), namely

\[
p = 381348997, 717636389, 778090129, 1496216791,
\]

and exactly one prime with \( i_p = 9 \), namely \( p = 1767218027 \). For this last \( p \), we found that \( B_r \equiv 0 \pmod{p} \) for the following nine values of \( r \):

\[
63562190, 274233542, 290632386, 619227758, 902737892, 1279901568, 1337429618, 1603159110, 1692877044.
\]
Bernoulli numbers

The main irregular prime computation was performed over a period of about ten months, starting in late 2012.
Bernoulli numbers

*The main irregular prime computation was performed over a period of about ten months, starting in late 2012. Any computation is susceptible to errors; in a computation of this magnitude it would be a great surprise if nothing went wrong. Consequently, we took careful precautions to maximize the chance of detecting any problems.*
Bernoulli numbers

The main irregular prime computation was performed over a period of about ten months, starting in late 2012. Any computation is susceptible to errors; in a computation of this magnitude it would be a great surprise if nothing went wrong. Consequently, we took careful precautions to maximize the chance of detecting any problems.

Indeed, a number of errors were detected. The consumer-grade machines in the Condor pool tended to have lower quality RAM, and on a handful of them the checksum test would reliably fail several times a day. The other systems had high-quality error-correcting RAM modules, and we did not detect any errors on them except for one problematic node on Katana. If any machine exhibited even a single checksum error, we excluded it from all computations and reprocessed all primes that had been handled on that machine.
Bernoulli numbers

- There are infinitely many irregular primes.
Bernoulli numbers

- There are infinitely many irregular primes.
- It is unknown whether or not there are infinitely many regular primes.
Special values of $\zeta(s)$

We compute special values formally – we gave a rigorous computation previously.
Special values of $\zeta(s)$

We compute special values formally – we gave a rigorous computation previously.

$$\zeta(1 - k) = \sum_{n \geq 1} (\frac{d}{dt})^{k-1} e^{nt} \bigg|_{t=0}$$

$$= (\frac{d}{dt})^{k-1} \left( \sum_{n \geq 1} e^{nt} \right) \bigg|_{t=0}$$

$$= (\frac{d}{dt})^{k-1} \left( \frac{1}{1 - e^t} - 1 \right) \bigg|_{t=0}$$

$$= (\frac{d}{dt})^{k-1} \left( \frac{1}{1 - e^t} \right) \bigg|_{t=0}$$
Special values of $\zeta(s)$

\[
\begin{align*}
\zeta(1 - k) &= -B_k k \\
&= (d/dt)^{k-1} \left( \frac{1}{t} \cdot \left( \sum_{k \geq 1} B_k t^k \frac{1}{k!} \right) \right) \bigg|_{t=0} \\
&= (d/dt)^{k-1} \left( \sum_{k \geq 1} \left( -\frac{B_k}{k} \right) t^{k-1} \frac{1}{(k-1)!} \right) \bigg|_{t=0}
\end{align*}
\]
Special values of $\zeta(s)$

\[
= \left(\frac{d}{dt}\right)^{k-1} \left( -\frac{1}{t} \cdot \left( \sum_{k \geq 1} B_k \frac{t^k}{k!} \right) \right) \bigg|_{t=0}
\]

\[
= \left(\frac{d}{dt}\right)^{k-1} \left( \sum_{k \geq 1} \left( -\frac{B_k}{k} \right) \frac{t^{k-1}}{(k-1)!} \right) \bigg|_{t=0}
\]

It follows that

\[
\zeta(1-k) = -\frac{B_k}{k}
\]
Now put

$$\zeta_p(1 - k) := (1 - p^{k-1}) \left( -\frac{B_k}{k} \right)$$
Special values of $\zeta(s)$

Now put

$$\zeta_p(1 - k) := (1 - p^{k-1}) \left( -\frac{B_k}{k} \right) = \frac{1}{\alpha^{-k} - 1} \int_{\mathbb{Z}_p^\times} x^{k-1} \mu_{1,\alpha}$$
Now put

\[ \zeta_p(1 - k) := (1 - p^{k-1}) \left( -\frac{B_k}{k} \right) = \frac{1}{\alpha^{-k} - 1} \int_{\mathbb{Z}_p^\times} x^{k-1} \mu_{1,\alpha} \]

As before, it can be interpolated for \( k \equiv s_0 \pmod{p - 1} \), and gives a **continuous** function from \( \mathbb{Z}_p \) to \( \mathbb{Q}_p \), (independent of \( \alpha \)).
Let \( \chi \) be a Dirichlet character of conductor \( f = f_\chi \).

\[
F_\chi(t, x) := \sum_{a=1}^{f} \chi(a) \cdot t \cdot \frac{e^{(a+x)t}}{e^{ft} - 1} = 
\]
Let $\chi$ be a Dirichlet character of conductor $f = f_{\chi}$.

$$F_{\chi}(t, x) := \sum_{a=1}^{f} \chi(a) \cdot t \cdot \frac{e^{(a+x)t}}{e^{ft} - 1} = \sum_{n \geq 0} B_{n, \chi}(x) \frac{t^n}{n!}$$
Let $\chi$ be a Dirichlet character of conductor $f = f_\chi$.

$$F_\chi(t, x) := \sum_{a=1}^{f} \chi(a) \cdot t \cdot \frac{e^{(a+x)t}}{e^{ft} - 1} = \sum_{n \geq 0} B_{n,\chi}(x) \frac{t^n}{n!}$$

Put

$$B_{n,\chi} := B_{n,\chi}(0).$$
Back to Bernoulli

We have:

- $B_{n,\chi}(x) \in \mathbb{Q}(\chi)[x]$, where $\mathbb{Q}(\chi) = \mathbb{Q}(\chi(a), a \in \mathbb{Z})$ is the smallest field containing all the indicated roots of 1,
We have:

- $B_{n,\chi}(x) \in \mathbb{Q}(\chi)[x]$, where $\mathbb{Q}(\chi) = \mathbb{Q}(\chi(a), a \in \mathbb{Z})$ is the smallest field containing all the indicated roots of 1,
- $B_{0,\chi} = \frac{1}{f} \sum_{a=1}^{f} \chi(a) = 0$, for $\chi \neq \chi_0$; it follows that $\deg(B_{n,\chi}) < n$, 

Back to Bernoulli

We have:

- \( B_{n,\chi}(x) \in \mathbb{Q}(\chi)[x] \), where \( \mathbb{Q}(\chi) = \mathbb{Q}(\chi(a), a \in \mathbb{Z}) \) is the smallest field containing all the indicated roots of 1,
- \( B_{0,\chi} = \frac{1}{f} \sum_{a=1}^{f} \chi(a) = 0 \), for \( \chi \neq \chi_{0} \); it follows that \( \deg(B_{n,\chi}) < n \),
- \( B_{n,\chi}(x) = \sum_{k=0}^{n} \binom{n}{k} B_{k,\chi} x^{n-k} \).
Back to Bernoulli

Since

\[ F_{\chi}(-t, -x) = \sum_{a=1}^{f} \chi(a) \cdot (-t) \cdot e^{-(a-x)t} \cdot \frac{e^{-ft} - 1}{e^{-ft} - 1} = \]
Back to Bernoulli

Since

\[ F_\chi(-t, -x) = \sum_{a=1}^{f} \chi(a) \cdot (-t) \cdot \frac{e^{-(a-x)t}}{e^{-ft} - 1} = \sum_{a=1}^{f} \chi(-1) \chi(f-a) t \cdot \frac{e^{(f-a+x)t}}{e^{ft} - 1}, \]
Back to Bernoulli

Since

\[ F_\chi(-t, -x) = \sum_{a=1}^{\mathcal{f}} \chi(a) \cdot (-t) \cdot \frac{e^{-(a-x)t}}{e^{-ft} - 1} = \sum_{a=1}^{\mathcal{f}} \chi(-1) \chi(f-a)t \cdot \frac{e^{(f-a+x)t}}{e^{ft} - 1}, \]

we have

\[ F_\chi(-t, -x) = \chi(-1) F_\chi(t, x), \quad \chi \neq \chi_0, \]
Back to Bernoulli

Since

\[ F_{\chi}(-t, -x) = \sum_{a=1}^{f} \chi(a) \cdot (-t) \cdot \frac{e^{-(a-x)t}}{e^{-ft} - 1} = \sum_{a=1}^{f} \chi(-1) \chi(f-a) t \cdot \frac{e^{(-a+x)t}}{e^{ft} - 1}, \]

we have

\[ F_{\chi}(-t, -x) = \chi(-1) F_{\chi}(t, x), \quad \chi \neq \chi_0, \]

and

\[ (-1)^n B_{n, \chi}(-x) = \chi(-1) B_{n, \chi}(x), \quad n \geq 0. \]
Back to Bernoulli

We have

\[ B_{n,\chi} = 0, \quad \chi \neq \chi_0, \quad n \not\equiv \delta_\chi \pmod{2}, \]

where

\[ \delta_\chi := \begin{cases} 
0 & \chi(-1) = 1 \\
1 & \chi(-1) = -1
\end{cases}. \]
We can express these new numbers through classical Bernoulli numbers.
We can express these new numbers through classical Bernoulli numbers. Starting with

$$F_{\chi}(t, x) = \frac{1}{f} \sum_{a=1}^{f} \chi(a) F(\frac{a - f + x}{f})$$

we obtain

$$B_{n, \chi}(x) = \frac{1}{f} \sum_{a=1}^{f} \chi(a) f^n B_n(\frac{a - f + x}{f}), \quad n \geq 0,$$

and in particular

$$B_{n, \chi} = \frac{1}{f} \sum_{a=1}^{f} \chi(a) f^n B_n(\frac{a - f}{f}), \quad n \geq 0.$$
Consider

\[ S_{n,\chi}(k) := \sum_{a=1}^{k-1} \chi(a)a^n, \quad n \geq 0, \]

\[ S_n(k) := \sum_{a=1}^{k-1} a^n. \]
Consider

\[ S_{n,\chi}(k) := \sum_{a=1}^{k-1} \chi(a)a^n, \quad n \geq 0, \]

\[ S_n(k) := \sum_{a=1}^{k-1} a^n. \]

E.g.,

\[ S_1(k) = \frac{k(k-1)}{2}. \]
Consider

\[ S_{n,\chi}(k) := \sum_{a=1}^{k-1} \chi(a)a^n, \quad n \geq 0, \]

and

\[ S_n(k) := \sum_{a=1}^{k-1} a^n. \]

E.g.,

\[ S_1(k) = \frac{k(k-1)}{2}. \]

These were computed by Bernoulli, in closed form. Before that, people published books (!), with tables of these numbers.
Back to Bernoulli

\[ F_{\chi}(t, x) - F_{\chi}(t, x - f) = \sum_{a = 1}^{f} \chi(a) t e^{(a + x - f)t}, \]
so that

\[ B_{n,\chi}(x) - B_{n,\chi}(x - f) = n \sum_{a=1}^{f} \chi(a)(a + x - f)^{n-1}. \]
Back to Bernoulli

\[
F_\chi(t, x) - F_\chi(t, x - f) = \sum_{a=1}^{a} f \chi(a) t e^{(a+x-f)t},
\]

so that

\[
B_{n,\chi}(x) - B_{n,\chi}(x - f) = n \sum_{a=1}^{f} \chi(a)(a + x - f)^{n-1}.
\]

Now, replace \( n \mapsto n + 1 \), and sum over \( x = f, 2f, \ldots, kf \).
Back to Bernoulli

We obtain

\[ S_{n,\chi}(kf) = \frac{1}{n+1} (B_{n+1,\chi}(kf) - B_{n+1,\chi}(0)) \]
We obtain

\[ S_{n,\chi}(kf) = \frac{1}{n+1} \left( B_{n+1,\chi}(kf) - B_{n+1,\chi}(0) \right) \]

From this we can compute

\[ B_{n,\chi} = \lim_{h \to \infty} S_{n,\chi}(p^h f), \]
Back to Bernoulli

We obtain

\[ S_{n,\chi}(kf) = \frac{1}{n + 1} (B_{n+1,\chi}(kf) - B_{n+1,\chi}(0)) \]

From this we can compute

\[ B_{n,\chi} = \lim_{h \to \infty} S_{n,\chi}(p^hf), \]

and also

\[ S_n(k) = \frac{1}{n + 1} (B_{n+1}(k) - B_{n+1}(0)) \]
Back to Bernoulli

We obtain

$$S_{n,\chi}(kf) = \frac{1}{n+1} (B_{n+1,\chi}(kf) - B_{n+1,\chi}(0))$$

From this we can compute

$$B_{n,\chi} = \lim_{h \to \infty} S_{n,\chi}(p^h f),$$

and also

$$S_n(k) = \frac{1}{n+1} (B_{n+1}(k) - B_{n+1}(0))$$

$$B_n = \lim_{h \to \infty} S_n(p^h),$$
Back to Bernoulli

We obtain

\[ S_{n,\chi}(kf) = \frac{1}{n+1} (B_{n+1,\chi}(kf) - B_{n+1,\chi}(0)) \]

From this we can compute

\[ B_{n,\chi} = \lim_{h \to \infty} S_{n,\chi}(p^hf), \]

and also

\[ S_{n}(k) = \frac{1}{n+1} (B_{n+1}(k) - B_{n+1}(0)) \]

\[ B_{n} = \lim_{h \to \infty} S_{n}(p^{h}), \]

In particular,

\[ S_{1}(k) = \frac{1}{2} (B_{2}(k) - B_{2}(0)) \]
Back to Bernoulli

We obtain

\[ S_{n,\chi}(kf) = \frac{1}{n+1} (B_{n+1,\chi}(kf) - B_{n+1,\chi}(0)) \]

From this we can compute

\[ B_{n,\chi} = \lim_{h \to \infty} S_{n,\chi}(p^hf), \]

and also

\[ S_n(k) = \frac{1}{n+1} (B_{n+1}(k) - B_{n+1}(0)) \]

\[ B_n = \lim_{h \to \infty} S_n(p^h), \]

In particular,

\[ S_1(k) = \frac{1}{2} (B_2(k) - B_2(0)) = \frac{1}{2} \left( (k^2 - k + \frac{1}{6}) - \frac{1}{6} \right) = \frac{1}{2} k(k - 1). \]
Generalized Kummer congruences

**Theorem**

Let $\chi$ be a Dirichlet character, and

$$\omega : (\mathbb{Z}/p\mathbb{Z})^\times \rightarrow \mathbb{C}, \quad p \geq 3.$$ 

Put $\chi_n := \chi \cdot \omega^{-n}$. 


Theorem

Let \( \chi \) be a Dirichlet character, and

\[
\omega : \left( \mathbb{Z}/p\mathbb{Z} \right)^\times \rightarrow \mathbb{C}, \quad p \geq 3.
\]

Put \( \chi_n := \chi \cdot \omega^{-n} \). Then there exists a power series \( A = A_\chi \in K[[x]] \), such that

- \( K \) is a finite extension of \( \mathbb{Q}_p \),
Generalized Kummer congruences

**Theorem**

Let \( \chi \) be a Dirichlet character, and

\[
\omega : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}, \quad p \geq 3.
\]

Put \( \chi_n := \chi \cdot \omega^{-n} \). Then there exists a power series \( A = A_\chi \in K[[x]] \), such that

- \( K \) is a finite extension of \( \mathbb{Q}_p \),
- the radius of convergence \( r_A \geq p^{\frac{p}{p-1}} \).
Theorem

Let $\chi$ be a Dirichlet character, and

$$\omega : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}, \quad p \geq 3.$$ 

Put $\chi_n := \chi \cdot \omega^{-n}$. Then there exists a power series $A = A_\chi \in K[[x]]$, such that

- $K$ is a finite extension of $\mathbb{Q}_p$,
- the radius of convergence $r_A \geq p^{\frac{p}{p-1}}$

$$A_\chi(n) = (1 - \chi_n(p)p^{n-1})B_{n,\chi_n}.$$
Proof

Let $K/\mathbb{Q}_p$ be a finite extension.
Proof

Let $K/\mathbb{Q}_p$ be a finite extension.

**Theorem**

Let $A, B \in K[[x]]$, with $r_A, r_B > 0$. Let $\{x_n\}$ be a sequence with $\lim x_n = 0$. Assume that $A(x_n) = B(x_n)$ for all $n$. Then $A = B$. 

Proof: Consider the difference $A(x) - B(x) = \sum c_n x^n$, let $c_{n_0}$ be the first nonzero coefficient. We have $-c_{n_0} = x^{i_n} \to 0 \cdot \sum_{n > n_0} c_n x^n - n_0 - 1$, bounded, $\forall x$.
Proof

Let $K / \mathbb{Q}_p$ be a finite extension.

**Theorem**

Let $A, B \in K[[x]]$, with $r_A, r_B > 0$. Let $\{x_n\}$ be a sequence with $\lim x_n = 0$. Assume that $A(x_n) = B(x_n)$ for all $n$. Then

$$A = B.$$
Proof

Let $K/\mathbb{Q}_p$ be a finite extension.

**Theorem**

Let $A, B \in K[[x]]$, with $r_A, r_B > 0$. Let $\{x_n\}$ be a sequence with $\lim x_n = 0$. Assume that $A(x_n) = B(x_n)$ for all $n$. Then

$$A = B.$$

**Proof:** Consider the difference $A(x) - B(x) = \sum c_n x^n$, let $c_{n_0}$ be the first nonzero coefficient.
Proof

Let $K/Q_p$ be a finite extension.

Theorem

Let $A, B \in K[[x]]$, with $r_A, r_B > 0$. Let $\{x_n\}$ be a sequence with $\lim x_n = 0$. Assume that $A(x_n) = B(x_n)$ for all $n$. Then

$$A = B.$$

Proof: Consider the difference $A(x) - B(x) = \sum c_n x^n$, let $c_{n_0}$ be the first nonzero coefficient. We have

$$-c_{n_0} = \underbrace{x_i}_{\to 0} \cdot \sum_{n>n_0} c_n x_i^{n-n_0-1}, \quad \forall x_i$$

bounded
Proof

Put

\[ \|A\| = \sup_n (|a_n|_p), \]

and let \( P_K : = \{ A \in K \mid \|A\| < \infty \} \).

Theorem
This is a norm and \( P_K \) is complete, i.e., a Banach algebra over the local field \( K \).
Proof

Put

\[ \|A\| = \sup_n(|a_n|_p), \]

and let

\[ \mathcal{P}_K := \{ A \in K[[x]] \mid \|A\| < \infty \}. \]
Proof

Put

\[ \|A\| = \sup_n (|a_n|^p), \]

and let

\[ \mathcal{P}_K := \{ A \in K[[x]] \mid \|A\| < \infty \}. \]

**Theorem**

This is a norm and \( \mathcal{P}_K \) is complete, i.e., a Banach algebra over the local field \( K \).
Reminder

\[ c_n := \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} b_i \]
Reminder

\[ c_n := \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} b_i \]

\[ b_n := \sum_{i=0}^{n} \binom{n}{i} c_i \]
\[ c_n := \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} b_i \]

\[ b_n := \sum_{i=0}^{n} \binom{n}{i} c_i \]

\[ \|n!\|_p \geq p^{\frac{n}{p-1}}. \]
Let $0 < r < |p|^{\frac{1}{p-1}}$ and $|c_n|_p \leq Cr^n$, $\forall n$, and some $C > 0$. 
Let $0 < r < |p|^{\frac{1}{p-1}}$ and $|c_n|_p \leq C r^n$, $\forall n$, and some $C > 0$. Then there exists a unique $A \in \mathcal{P}_K$ such that

- $r_A \geq |p|^{\frac{1}{p-1}} r^{-1}$,
- $A(n) = b_n$, for all $n$. 
Application

\[ b_n := (1 - \chi_n(p)p^{n-1})B_{n,\chi_n} \]

\[ c_n := \sum_{i=0}^{n} \binom{n}{i} b_i \]
Application

\[ b_n := (1 - \chi_n(p)p^{n-1})B_{n,\chi_n} \]

\[ c_n := \sum_{i=0}^{n} \binom{n}{i} b_i \]

So the basic estimate one has to show is:

\[ |c_n|_p \leq |p^{-2}f^{-1}| \cdot |p|_p^n, \quad \forall n \]

\[ \ldots \]
Analysis on the $p$-adics

We have looked at functions $f : \mathbb{Z}_p \to \mathbb{Q}_p$. But we can also study functions $f : \mathbb{Q}_p \to \mathbb{C}$. Basic examples: characteristic functions $\chi_U$ of $U := \{a + pN \in \mathbb{Z}_p\}$, $|x|^s_p$, for $s \in \mathbb{C}$. 

Lecture 8
Analysis on the $p$-adics

We have looked at functions $f : \mathbb{Z}_p \to \mathbb{Q}_p$. But we can also study functions

$$f : \mathbb{Q}_p \to \mathbb{C}.$$
Analysis on the $p$-adics

We have looked at functions $f : \mathbb{Z}_p \to \mathbb{Q}_p$. But we can also study functions

$$f : \mathbb{Q}_p \to \mathbb{C}.$$ 

Basic examples:

- characteristic functions $\chi_U$ of $U := \{a + p^N\mathbb{Z}_p\},$
Analysis on the $p$-adics

We have looked at functions $f : \mathbb{Z}_p \to \mathbb{Q}_p$. But we can also study functions

$$f : \mathbb{Q}_p \to \mathbb{C}.$$  

Basic examples:

- characteristic functions $\chi_U$ of $U := \{a + p^N \mathbb{Z}_p\}$,
- $|x|^s_p$, for $s \in \mathbb{C}$
Now we can consider
\[ \int_{\mathbb{Q}_p} f(x) \, dx_p \]
where \( dx_p = \mu_p \) is the \textbf{Haar measure}, i.e., translation invariant measure,
Now we can consider
\[ \int_{\mathbb{Q}_p} f(x) \, d\mu_p \]
where \( d\mu_p = \mu_p \) is the Haar measure, i.e., translation invariant measure, normalized by
\[ \int_{\mathbb{Z}_p} d\mu_p = 1. \]
Basic computation

\[ \int_{\mathbb{Q}_p} \chi_{\mathbb{Z}_p}(x) \cdot |x|_p^{s-1} \, dx_p \]
Basic computation

\[
\int_{\mathbb{Q}_p} \chi_{\mathbb{Z}_p}(x) \cdot |x|^{s-1}_p \, dx_p = \sum_{n \geq 0} p^{-n(s-1)} \cdot \int_{p^n \mathbb{Z}_p \setminus p^{n+1} \mathbb{Z}_p} dx_p
\]

\[
= \sum_{n \geq 0} p^{-n(s-1)} \frac{1}{p^n} \cdot \left(1 - \frac{1}{p}\right)
\]
Basic computation

\[ \int_{\mathbb{Q}_p} \chi_{\mathbb{Z}_p}(x) \cdot |x|_p^{s-1} \, dx_p = \sum_{n \geq 0} p^{-n(s-1)} \cdot \int_{p^n \mathbb{Z}_p \setminus p^{n+1} \mathbb{Z}_p} \, dx_p \]

= \sum_{n \geq 0} p^{-n(s-1)} \frac{1}{p^n} \cdot \left( 1 - \frac{1}{p} \right) = \frac{1}{1 - p^{-s}} \cdot \left( 1 - \frac{1}{p} \right) \]
Basic computation

\[ \int_{\mathbb{Q}_p} \chi_{\mathbb{Z}_p}(x) \cdot |x|_p^{s-1} \, dx_p = \sum_{n \geq 0} p^{-n(s-1)} \cdot \int_{\mathbb{Z}_p \setminus \mathbb{p}^{n+1}\mathbb{Z}_p} d\mathbb{x}_p \]

\[ = \sum_{n \geq 0} p^{-n(s-1)} \frac{1}{p^n} \cdot \left(1 - \frac{1}{p}\right) = \frac{1}{1 - p^{-s}} \cdot \left(1 - \frac{1}{p}\right) \]

So we can formally write

\[ \zeta(s) = \prod_{p} \int_{\mathbb{Q}_p} \chi_{\mathbb{Z}_p}(x) \cdot |x|_p^{s-1} \, dx_p \cdot \prod_{p} \left(1 - \frac{1}{p}\right)^{-1}. \]