Chapter 11
p-adic Measure and Kummer's Congruence

In modern number theory, the p-adic method or p-adic way of thinking plays an important role. As an example, there are objects called p-adic L-functions which correspond to the Dirichlet L-functions, and in fact the natural setup to understand the Kummer congruence described in Sect. 3.2 is in the context of the p-adic L-functions. To be precise, a modified version (by a suitable "Euler factor") of Kummer's congruence guarantees the existence of the p-adic L-function.

To discuss this aspect fully is beyond the scope of this book, but in this chapter we explain the p-adic integral expression of the Bernoulli number and prove Kummer's congruence using it. Interested readers are advised to read books such as Iwasawa [51], Washington [100], Lang [66].

We assume the basics of p-adic numbers. For this we refer readers to Serre [83, Ch. 1] or Gouvea [37]. The results in this chapter are not used in other chapters.

11.1 Measure on the Ring of p-adic Integers and the Ring of Formal Power Series

In this section we review the general correspondence between measures on the ring of p-adic integers $\mathbf{Z}_p$ and the ring of formal power series. We use this setup in the next section to define the Bernoulli measure on $\mathbf{Z}_p$ and to express Bernoulli numbers as integrals. This expression turns out to be very useful in proving Kummer's congruence relation.

Let $\overline{\mathbf{Q}}_p$ be the algebraic closure of the field $\mathbf{Q}_p$ of p-adic numbers. The p-adic absolute value $|\ \ |$ of $\mathbf{Q}_p$ (normalized by $|p| = 1/p$) is extended uniquely to $\overline{\mathbf{Q}}_p$. We use the same notation $|\ \ |$ for this extension. Then $\overline{\mathbf{Q}}_p$ is not complete with respect to this absolute value, and the completion is denoted by $\mathbf{C}_p$. The absolute value $|\ \ |$ also extends naturally to $\mathbf{C}_p$. Let $\mathcal{O}_p$ be the ring of integers of $\mathbf{C}_p$:

$$\mathcal{O}_p = \{x \in \mathbf{C}_p \mid |x| \leq 1\}.$$

T. Arakawa et al., *Bernoulli Numbers and Zeta Functions*, Springer Monographs in Mathematics, DOI 10.1007/978-4-431-54919-2_11, © Springer Japan 2014

Remark 11.1. Like the complex number field $\mathbf{C}$, the field $\mathbf{C}_p$ is complete and algebraically closed. To do analysis in the p-adic setting, we need this big field.

First we review the general theory of measures on $\mathbf{Z}_p$.

Denote the $\mathbf{Z}$-module $\mathbf{Z}/p^n\mathbf{Z}$ by X_n and the canonical map from X_{n+1} to X_n by π_{n+1}, so $\pi_{n+1} : X_{n+1} \to X_n$ is defined by

$$x \bmod p^{n+1}\mathbf{Z} \longmapsto x \bmod p^n\mathbf{Z}.$$

The system of pairs (X_n, π_n) gives a projective system and we have the projective limit $\varprojlim X_n$:

$$\varprojlim X_n = \left\{(x_n) \in \prod_{n\geq 1} X_n \mid \pi_{n+1}(x_{n+1}) = x_n\right\}.$$

The ring of p-adic integers $\mathbf{Z}_p$ is identified with this projective limit $\varprojlim X_n$.

Definition 11.2 (Measure on $\mathbf{Z}_p$). A set of functions $\mu = \{\mu_n\}_{n=1}^{\infty}$ is called an $\mathcal{O}_p$-valued measure on $\mathbf{Z}_p$ if the following two conditions are satisfied:

(i) Each μ_n is an $\mathcal{O}_p$-valued function on X_n, $\mu_n : X_n \longrightarrow \mathcal{O}_p$.
(ii) For any $n \in \mathbf{N}$ and $x \in X_n$, the distribution property

$$\mu_n(x) = \sum_{\substack{y\in X_{n+1}\\ \pi_{n+1}(y)=x}} \mu_{n+1}(y)$$

holds.

The set of $\mathcal{O}_p$-valued measures on $\mathbf{Z}_p$ is denoted by $\mathcal{M}(\mathbf{Z}_p, \mathcal{O}_p)$. This has an $\mathcal{O}_p$-module structure. Further, the norm of $\mu = \{\mu_n\} \in \mathcal{M}(\mathbf{Z}_p, \mathcal{O}_p)$ is defined as

$$\|\mu\| = \sup_{n\in\mathbf{N},\ x\in X_n} |\mu_n(x)|.$$

Also, the $\mathcal{O}_p$-module of continuous $\mathcal{O}_p$-valued functions on $\mathbf{Z}_p$ is denoted by $C(\mathbf{Z}_p, \mathcal{O}_p)$, and the norm $\|\varphi\|$ of an element $\varphi \in C(\mathbf{Z}_p, \mathcal{O}_p)$ is defined by

$$\|\varphi\| = \sup_{x\in\mathbf{Z}_p} |\varphi(x)|.$$

For $\varphi \in C(\mathbf{Z}_p, \mathcal{O}_p)$ and $\mu = \{\mu_n\} \in \mathcal{M}(\mathbf{Z}_p, \mathcal{O}_p)$, the integral on $\mathbf{Z}_p$ is defined by

$$\int_{\mathbf{Z}_p} \varphi(x)d\mu(x) = \lim_{n\to\infty} \sum_{r=0}^{p^n-1} \varphi(r)\mu_n(r).$$

(We use the abbreviated notation $\mu_n(r)$ for $\mu_n(r \bmod p^n)$. A similar abbreviation will be used in the following.) The convergence of the limit on the right-hand side is guaranteed by the following estimate: when $n < m$, we have

$$\begin{aligned}
&\Big| \sum_{r=0}^{p^n-1} \varphi(r)\mu_n(r) - \sum_{l=0}^{p^m-1} \varphi(l)\mu_m(l) \Big| \\
&= \Big| \sum_{r=0}^{p^n-1} \Big(\varphi(r)\mu_n(r) - \sum_{q=0}^{p^{m-n}-1} \varphi(r+p^n q)\mu_m(r+p^n q) \Big) \Big| \\
&= \Big| \sum_{r=0}^{p^n-1} \left(\sum_{q=0}^{p^{m-n}-1} \left(\varphi(r) - \varphi(r+p^n q)\right) \mu_m(r+p^n q) \right) \Big| \\
&\le \max_{r,\,q} |\varphi(r) - \varphi(r+p^n q)| \, \|\mu\|.
\end{aligned}$$

For each natural number k, the binomial polynomial

$$\binom{t}{k} = \frac{t(t-1)\cdots(t-k+1)}{k!}$$

in t is a continuous function on $\mathbf{Z}_p$.

To $\mu = \{\mu_n\} \in \mathcal{M}(\mathbf{Z}_p, \mathcal{O}_p)$ we associate $f \in \mathcal{O}_p[[X]]$ in the following manner. Set $\Lambda = \mathcal{O}_p[[X]]$, $\Lambda_n = ((1+X)^{p^n} - 1)\Lambda$ and consider the projective system $\{(\Lambda/\Lambda_n, \varpi_n)\}$ by the natural map $\varpi_n : \Lambda/\Lambda_n \longrightarrow \Lambda/\Lambda_{n-1}$. Define $f_n(X) \in \Lambda/\Lambda_n$ by

$$f_n(X) = \sum_{r=0}^{p^n-1} \mu_n(r)(1+X)^r = \sum_{r=0}^{p^n-1} \sum_{k=0}^{r} \mu_n(r) \binom{r}{k} X^k = \sum_{k=0}^{p^n-1} c_{n,k} X^k.$$

Here we understand that the equalities are mod Λ_n and put

$$c_{n,k} = \sum_{r=0}^{p^n-1} \mu_n(r) \binom{r}{k}.$$

Since we have

$$(\varpi_n f_n)(X) = \varpi_n \left(\sum_{r=0}^{p^n-1} \mu_n(r)(1+X)^r \right)$$

$$= \varpi_n \left(\sum_{r'=0}^{p^{n-1}-1} \sum_{l=0}^{p-1} \mu_n(r' + p^{n-1}l)(1+X)^{r'}(1+X)^{p^{n-1}l} \right)$$

$$= \sum_{r'=0}^{p^{n-1}-1} \mu_{n-1}(r')(1+X)^{r'}$$

$$= f_{n-1}(X),$$

the system (f_n) is an element in the projective limit $\varprojlim \Lambda/\Lambda_n$. Now we have the isomorphism

$$\Lambda \cong \varprojlim \Lambda/\Lambda_n, \quad \Lambda \ni g \longmapsto (g_n) \in \varprojlim \Lambda/\Lambda_n,$$

where, for $g \in \Lambda$, the system (g_n) is given by $g_n = g \bmod \Lambda_n$. Through this isomorphism, the above $\{f_n\}$ corresponds to $f \in \Lambda$ by

$$f(X) = \sum_{m=0}^{\infty} c_m X^m,$$

where

$$c_m = \lim_{n\to\infty} \sum_{r=0}^{p^n-1} \mu_n(r) \binom{r}{m}$$

$$= \int_{\mathbf{Z}_p} \binom{x}{m} d\mu(x).$$

We therefore have obtained a map from $\mathcal{M}(\mathbf{Z}_p, \mathcal{O}_p)$ to $\mathcal{O}_p[[X]]$. An important fact is that this map gives a natural *isomorphism* between $\mathcal{M}(\mathbf{Z}_p, \mathcal{O}_p)$ and the ring of formal power series $\mathcal{O}_p[[X]]$, often referred to as the Iwasawa isomorphism. The way to associate a measure to an element in $\mathcal{O}_p[[X]]$ is described as follows.

For $f = \sum_{m=0}^{\infty} c_m X^m \in \mathcal{O}_p[[X]]$, define $\mu = \{\mu_n\}$ by

$$\mu_n(r) = \frac{1}{p^n} \sum_{\zeta^{p^n}=1} \zeta^{-r} f(\zeta - 1) \qquad (r \in X_n), \tag{11.1}$$

the sum running over all p^n-th roots ζ of 1. Since $|\zeta - 1| < 1$, $f(\zeta-1)$ converges. For each $m \geq 0$, we have

$$\frac{1}{p^n} \sum_{\zeta^{p^n}=1} \zeta^{-r}(\zeta-1)^m = \frac{1}{p^n} \sum_{\zeta^{p^n}=1} \sum_{j=0}^{m} \zeta^{-r} \binom{m}{j} (-1)^{m-j} \zeta^j$$

$$= \sum_{\substack{0 \leq j \leq m \\ j \equiv r \bmod p^n}} \binom{m}{j} (-1)^{m-j}.$$

So this is contained in $\mathcal{O}_p$. In particular, if $p^n > r > m$, then this is zero. When ζ is a primitive p^ν-th root of 1 ($\nu \geq 1$), the equality

$$|\zeta - 1|^{\varphi(p^\nu)} = |p| \qquad (\varphi \text{ is the Euler function})$$

holds and hence

$$|(\zeta - 1)^m| = |p^{m/\varphi(p^\nu)}|.$$

From this, we conclude that p^e divides the quantity

$$\sum_{\substack{0 \leq j \leq m \\ j \equiv r \bmod p^n}} \binom{m}{j} (-1)^{m-j}$$

for $e = m/\phi(p^n) - n$. Therefore,

$$\mu_n(r) = \sum_{m=0}^{\infty} c_m \left(\frac{1}{p^n} \sum_{\zeta^{p^n}=1} \zeta^{-r} (\zeta - 1)^m \right)$$

is convergent and the value is in $\mathcal{O}_p$. To check the distribution property (ii) of the measure, we need to calculate the following value:

$$\begin{aligned} \sum_{y \in X_{n+1},\ \pi_{n+1}(y)=x} \mu_{n+1}(y) &= \sum_{a \bmod p} \mu_{n+1}(x + p^n a) \\ &= \frac{1}{p^{n+1}} \sum_{\zeta^{p^{n+1}}=1} \left(\sum_{a \bmod p} \zeta^{-(x+p^n a)} \right) f(\zeta - 1). \end{aligned}$$

Using the identity

$$\sum_{a \bmod p} \zeta^{-p^n a} = \begin{cases} 0 & \text{if } \zeta^{p^n} \neq 1, \\ p & \text{if } \zeta^{p^n} = 1 \end{cases}$$

for a p^{n+1}-th root ζ of 1, we have

$$\sum_{\substack{a \bmod p \\ \zeta^{p^{n+1}}=1}} \zeta^{-x-p^n a} = p \sum_{\zeta^{p^n}=1} \zeta^{-x},$$

so we have

$$\sum_{\substack{y \in X_{n+1} \\ \pi_{n+1}(y)=x}} \mu_{n+1}(y) = \mu_n(x)$$

which is to be proved. If we define the formal power series $\tilde{f} \in \mathcal{O}_p[[X]]$ corresponding to this measure defined as before, then the coefficients c'_k of X^k of this series are given by

$$c'_k = \lim_{n\to\infty} \sum_{r=0}^{p^n-1} \mu_n(r)\binom{r}{k}$$
$$= \lim_{n\to\infty} \sum_{m=0}^{\infty} c_m \sum_{r=0}^{p^n-1} \binom{r}{k} \sum_{\substack{0\le j\le m \\ j\equiv r \bmod p^n}} \binom{m}{j}(-1)^{m-j}.$$

We fix k. To calculate the coefficient of c_m in the expression of c'_k in the right-hand side above, we fix m. We have $\binom{r}{k} = 0$ for $k > r$ so we may assume that $k \le r$. Taking n big enough, we assume that $m < p^n$. Then, if $j \equiv r \bmod p^n$ for some j with $0 \le j \le m$, we have $j = r$ since we also have $0 \le r \le p^n - 1$ by definition. So we may assume that $k \le r = j \le m$. So the coefficient of c_m is given by

$$\sum_{r=k}^{m} \binom{r}{k}\binom{m}{r}(-1)^{m-r} = \sum_{i=0}^{m-k} \binom{m-k}{i}\binom{m}{k}(-1)^{m-k-i} = \begin{cases} 1 & \text{if } m = k, \\ 0 & \text{if } m \ne k. \end{cases}$$

Hence we have $c'_k = c_k$. So we have $\tilde{f} = f$ and two mappings are inverse with each other and we see that the set $\mathcal{M}(\mathbf{Z}_p, \mathcal{O}_p)$ of $\mathcal{O}_p$-valued measures and the space of formal power series $\mathcal{O}_p[[X]]$ are bijective.

More precisely, we can introduce a product for both spaces and show that these are isomorphic as $\mathcal{O}_p$ algebras, as given in the following theorem whose complete proof is omitted (see e.g. Lang [66, Ch.4]).

For two measures $\mu,\ \nu \in \mathcal{M}(\mathbf{Z}_p, \mathcal{O}_p)$, we define an $\mathcal{O}_p$-valued function $(\mu * \nu)_n$ on X_n by

$$(\mu * \nu)_n(x) = \sum_{y=0}^{p^n-1} \mu_n(y)\nu_n(x-y) \qquad (x \in X_n). \tag{11.2}$$

Then $\mu * \nu = \{(\mu * \nu)_n\}$ becomes an element of $\mathcal{M}(\mathbf{Z}_p, \mathcal{O}_p)$. We call this a convolution product of μ and ν. The set $\mathcal{M}(\mathbf{Z}_p, \mathcal{O}_p)$ becomes an $\mathcal{O}_p$ algebra by this product $\mu * \nu$.

Theorem 11.3 (Iwasawa isomorphism). *Between the space $\mathcal{M}(\mathbf{Z}_p, \mathcal{O}_p)$ of $\mathcal{O}_p$-valued measures and the ring of formal power series $\mathcal{O}_p[[X]]$, there is an $\mathcal{O}_p$ algebra isomorphism $P : \mathcal{M}(\mathbf{Z}_p, \mathcal{O}_p) \longrightarrow \mathcal{O}_p[[X]]$ given by*

$$\mathcal{M}(\mathbf{Z}_p, \mathcal{O}_p) \ni \mu = \{\mu_n\} \overset{P}{\longmapsto} f(X) = \sum_{m=0}^{\infty} c_m X^m \in \mathcal{O}_p[[X]].$$

Here, c_m is determined by μ:

$$c_m = \int_{\mathbf{Z}_p} \binom{x}{m} d\mu(x),$$

and conversely μ_n is determined by f:

$$\mu_n(x) = \frac{1}{p^n} \sum_{\zeta^{p^n}=1} \zeta^{-x} f(\zeta - 1).$$

For convenience of the description below, we recall Mahler's[1] theorem giving the necessary and sufficient condition for an $\mathcal{O}_p$-valued function on $\mathbf{Z}_p$ to be continuous.

Theorem 11.4. *The function $\varphi : \mathbf{Z}_p \longrightarrow \mathcal{O}_p$ is continuous if and only if it can be written as*

$$\varphi(x) = \sum_{n=0}^{\infty} a_n \binom{x}{n}, \qquad a_n \in \mathcal{O}_p, \quad |a_n| \longrightarrow 0.$$

If this is the case, the coefficients a_n are uniquely determined by φ and given by

$$a_n = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} \varphi(k).$$

We omit the proof (cf. Lang [66, §4.1]).

If we use Theorem 11.4, we can understand a part of Theorem 11.3 more intuitively as follows. Fix $x_0 \in \mathbf{Z}$. Denote by φ the characteristic polynomial of $x_0 + p^n\mathbf{Z}_p$. Then by the definition of the p-adic measure, we see easily that

$$\int_{\mathbf{Z}_p} \varphi(x) d\mu(x) = \mu_n(x_0).$$

So if we replace $\varphi(x)$ by the expansion $\varphi(x) = \sum_{m=0}^{\infty} a_m \binom{x}{m}$ in Theorem 11.4, we have

$$\mu_n(x_0) = \sum_{m=0}^{\infty} a_m c_m = \sum_{m=0}^{\infty} c_m \sum_{k=0}^{m} (-1)^{m-k} \binom{m}{k} \varphi(k).$$

[1] Kurt Mahler (born on July 26, 1903 in Krefeld, Prussian Rhineland—died on February 25, 1988 in Canberra, Australia).

Now, for any ζ with $\zeta^{p^n} = 1$, we have

$$\sum_{m=0}^{\infty} c_m(\zeta - 1)^m = \sum_{m=0}^{\infty} c_m \sum_{k=0}^{m} \binom{m}{k} (-1)^{m-k} \zeta^k.$$

Since $\varphi(k) = 1$ if $k \equiv x_0 \bmod p^n$ and $\varphi(k) = 0$ otherwise, we have

$$\frac{1}{p^n} \sum_{\zeta^{p^n}=1} \zeta^{-x_0} \sum_{m=0}^{\infty} c_m(\zeta - 1)^m = \sum_{m=0}^{\infty} c_m \sum_{k=0}^{m} \binom{m}{k} (-1)^{m-k} \varphi(k).$$

So we get the expression of $\mu(x)$ by f in Theorem 11.3.

We describe here several useful properties of the correspondence P in Theorem 11.3 between measures and formal power series. Let the maximal ideal of $\mathcal{O}_p$ be

$$\mathcal{P} = \{z \in \mathcal{O}_p \mid |z| < 1\}.$$

For $z \in \mathcal{P}$, define the function $(1+z)^x$ in x by

$$(1+z)^x := \sum_{n=0}^{\infty} \binom{x}{n} z^n.$$

By Mahler's theorem, $(1+z)^x$ is a continuous function of $x \in \mathbf{Z}_p$. When x is a non-negative integer, this definition of $(1+z)^x$ coincides with the usual binomial expansion. We have the relation

$$(1+z)^x (1+z)^{x'} = (1+z)^{x+x'} \qquad (x,\ x' \in \mathbf{Z}_p). \tag{11.3}$$

This is obvious for $x,\ x' \in \mathbf{N}$, and the general case for $x,\ x' \in \mathbf{Z}_p$ follows from the fact that the set $\mathbf{N}$ of natural numbers is dense in $\mathbf{Z}_p$.

In the following, we list several properties of measures and corresponding power series, which will be used later.

Property (1). Let $z \in \mathcal{P}$. If μ corresponds to f (i.e. $P\mu = f$), then

$$f(z) = \int_{\mathbf{Z}_p} (1+z)^x \, d\mu(x).$$

In particular, by putting $z = 0$,

$$f(0) = \int_{\mathbf{Z}_p} d\mu(x).$$

Proof. Writing $f(X) = \sum_{n=0}^{\infty} c_n X^n$, we have by Theorem 11.3

$$\int_{\mathbf{Z}_p} (1+z)^x \, d\mu(x) = \int_{\mathbf{Z}_p} \sum_{n=0}^{\infty} \binom{x}{n} z^n \, d\mu(x)$$
$$= \sum_{n=0}^{\infty} z^n \int_{\mathbf{Z}_p} \binom{x}{n} d\mu(x)$$
$$= \sum_{n=0}^{\infty} c_n z^n = f(z).$$

□

We call the map λ from $C(\mathbf{Z}_p, \mathcal{O}_p)$ to $\mathcal{O}_p$ a bounded linear functional on $C(\mathbf{Z}_p, \mathcal{O}_p)$ if the following conditions (i), (ii) are satisfied:

(i) For any $\varphi,\ \varphi' \in C(\mathbf{Z}_p, \mathcal{O}_p)$ and any $a,\ b \in \mathcal{O}_p$,

$$\lambda(a\varphi + b\varphi') = a\lambda(\varphi) + b\lambda(\varphi').$$

(ii) There exists a positive constant $M > 0$ such that for any $\varphi \in C(\mathbf{Z}_p, \mathcal{O}_p)$,

$$|\lambda(\varphi)| \leq M\|\varphi\|.$$

The norm of λ is defined by

$$\|\lambda\| = \sup_{\substack{\varphi \in C(\mathbf{Z}_p, \mathcal{O}_p) \\ \varphi \neq 0}} \frac{|\lambda(\varphi)|}{\|\varphi\|}.$$

Let λ be a bounded linear functional on $C(\mathbf{Z}_p, \mathcal{O}_p)$. For $x \in X_n = \mathbf{Z}/p^n\mathbf{Z}$, write the characteristic function of $x + p^n\mathbf{Z}_p$ as $\varphi_{x,n}$. If we put

$$\mu_n(x) = \lambda(\varphi_{x,n}),$$

then $\mu = \{\mu_n\}$ is an $\mathcal{O}_p$-valued measure on $\mathbf{Z}_p$ (i.e. $\mu \in \mathcal{M}(\mathbf{Z}_p, \mathcal{O}_p)$). Conversely, given $\mu = \{\mu_n\} \in \mathcal{M}(\mathbf{Z}_p, \mathcal{O}_p)$, if we put

$$\lambda(\varphi) = \int_{\mathbf{Z}_p} \varphi(x) \, d\mu(x),$$

then λ is a bounded linear functional on $C(\mathbf{Z}_p, \mathcal{O}_p)$. This correspondence between λ and μ is easily seen to be one to one.

Moreover, for $h \in C(\mathbf{Z}_p, \mathcal{O}_p)$ and $\mu \in \mathcal{M}(\mathbf{Z}_p, \mathcal{O}_p)$, the map

$$\varphi \longmapsto \int_{\mathbf{Z}_p} \varphi(x)h(x)\, d\mu(x), \qquad (\varphi \in C(\mathbf{Z}_p, \mathcal{O}_p))$$

is a bounded linear functional on $C(\mathbf{Z}_p, \mathcal{O}_p)$. Let $h\mu$ be the corresponding measure. It is an interesting problem to compute the formal power series corresponding to the measure $h\mu$ when μ corresponds to $f = P\mu \in \mathcal{O}_p[[X]]$. Properties (2) and (3) below give examples of this correspondence.

For $f \in \mathcal{O}_p[[X]]$, put

$$(\mathbb{U}f)(X) = f(X) - \frac{1}{p}\sum_{\zeta^p=1} f(\zeta(1+X)-1). \tag{11.4}$$

Since

$$\frac{1}{p}\sum_{\zeta^p=1} (\zeta(1+X)-1)^l \in \mathbf{Z}_p[X]$$

for non-negative integers l, we have $\mathbb{U}f \in \mathcal{O}_p[[X]]$.

Property (2). Let $f \in \mathcal{O}_p[[X]]$ and μ_f be the corresponding measure. Also, let ψ be the characteristic function of $\mathbf{Z}_p^\times$. Then the formal power series corresponding to the measure $\psi\mu_f$ is $\mathbb{U}f$, i.e., $\psi\mu_f = \mu_{\mathbb{U}f}$. More precisely, we have for any $\varphi \in C(\mathbf{Z}_p, \mathcal{O}_p)$

$$\int_{\mathbf{Z}_p} \varphi(x)\psi(x)\, d\mu_f(x) = \int_{\mathbf{Z}_p} \varphi(x)\, d\mu_{\mathbb{U}f}(x).$$

This can also be written as

$$\int_{\mathbf{Z}_p^\times} \varphi(x)\, d\mu_f(x) = \int_{\mathbf{Z}_p} \varphi(x)\, d\mu_{\mathbb{U}f}(x).$$

Proof. Write the power series corresponding to the measure $\psi\mu_f$ as g. When $z \in \mathcal{P}$, by Property (1) we have

$$g(z) = \int_{\mathbf{Z}_p} (1+z)^x \psi(x)\, d\mu_f(x).$$

Let ζ be a pth root of 1. Regarding ψ also as a function on $\mathbf{Z}/p\mathbf{Z}$ via $\psi(a \bmod p) = \psi(a + p\mathbf{Z}_p)$, and putting

$$\hat{\psi}(\zeta) = \frac{1}{p} \sum_{a \in \mathbf{Z}/p\mathbf{Z}} \psi(a)\zeta^{-a},$$

(Fourier transform on $\mathbf{Z}/p\mathbf{Z}$) we have

$$\psi(a) = \sum_{\zeta^p=1} \hat{\psi}(\zeta)\zeta^a$$

by a simple calculation (inverse Fourier transform). Since

$$\hat{\psi}(\zeta) = \begin{cases} -\frac{1}{p} & \text{if } \zeta \neq 1, \\ \frac{p-1}{p} & \text{if } \zeta = 1, \end{cases}$$

by the definition of ψ, we obtain

$$\begin{aligned} g(z) &= \int_{\mathbf{Z}_p} (1+z)^x \psi(x)\, d\mu_f(x) \\ &= \int_{\mathbf{Z}_p} (1+z)^x \sum_{\zeta^p=1} \hat{\psi}(\zeta)\zeta^x\, d\mu_f(x) \\ &= \sum_{\zeta^p=1} \hat{\psi}(\zeta) \int_{\mathbf{Z}_p} (1+z)^x \zeta^x\, d\mu_f(x) \\ &= \sum_{\zeta^p=1} \hat{\psi}(\zeta) \int_{\mathbf{Z}_p} \Big(1 + (\zeta(1+z)-1)\Big)^x d\mu_f(x) \\ &= \sum_{\zeta^p=1} \hat{\psi}(\zeta) f(\zeta(1+z)-1) = f(z) - \frac{1}{p} \sum_{\zeta^p=1} f(\zeta(1+z)-1). \end{aligned}$$

This shows $g = \mathbb{U}f$. (Here we define the power ζ^x for $x \in \mathbf{Z}_p$ by

$$\zeta^x = (1+\zeta-1)^x = \sum_{n=0}^{\infty} \binom{x}{n} (\zeta-1)^n.$$

If we choose $a \in \mathbf{Z}$ so that $x - a \in p\mathbf{Z}_p$, we have $\zeta^x = \zeta^a$.) □

Define the differential operator D on the ring of formal power series $\mathcal{O}_p[[X]]$ by

$$D = (1+X)D_X, \qquad \text{where} \quad D_X = \frac{d}{dX}.$$

Property (3). For $f \in \mathcal{O}_p[[X]]$, the power series corresponding to the measure $x\mu_f$ is Df. Hence the power series corresponding to the measure $x^k\mu_f$ (k natural number) is $D^k f$ and the equalities

$$\int_{\mathbf{Z}_p} x^k \, d\mu_f(x) = \int_{\mathbf{Z}_p} d\mu_{D^k f}(x) = (D^k f)(0)$$

hold.

Proof. It is enough to show this when $k = 1$. Let $g \in \mathcal{O}_p[[X]]$ be the power series corresponding to the measure $x\mu_f$. By Property (1), we have for $z \in \mathcal{P}$

$$g(z) = \int_{\mathbf{Z}_p} x(1+z)^x \, d\mu_f(x).$$

Put $f(X) = \sum_{n=0}^{\infty} a_n X^n$, $g(X) = \sum_{n=0}^{\infty} b_n X^n$. Using

$$X\binom{X}{n} = (n+1)\binom{X}{n+1} + n\binom{X}{n}$$

and Theorem 11.3, we have

$$\begin{aligned} b_n &= \int_{\mathbf{Z}_p} \binom{x}{n} d\mu_g(x) = \int_{\mathbf{Z}_p} \binom{x}{n} x \, d\mu_f(x) \\ &= (n+1)\int_{\mathbf{Z}_p} \binom{x}{n+1} d\mu_f(x) + n\int_{\mathbf{Z}_p} \binom{x}{n} d\mu_f(x) \\ &= (n+1)a_{n+1} + na_n. \end{aligned}$$

On the other hand, Df is computed as

$$\begin{aligned} (Df)(X) &= ((1+X)D_X f)(X) \\ &= (1+X)(a_1 + 2a_2 X + \cdots + na_n X^{n-1} + \cdots) \\ &= \sum_{n=0}^{\infty} ((n+1)a_{n+1} + na_n)X^n. \end{aligned}$$

This gives $g = Df$. □

In general, for a power series $f(X)$, we define a new power series $f^*(Z)$ in Z by setting $X = e^Z - 1$:

$$f^*(Z) = f(e^Z - 1). \tag{11.5}$$

For example, when

$$f(X) = (1 + X)^a = \sum_{n=0}^{\infty} \binom{a}{n} X^n,$$

we have

$$f^*(Z) = e^{aZ} = \sum_{n=0}^{\infty} \frac{a^n Z^n}{n!}.$$

Note the identity

$$(D_Z^k f^*)(0) = (D^k f)(0) \tag{11.6}$$

since

$$D_Z f^*(Z) = (1 + X) D_X f(X) = Df(X).$$

The next property is the basis of the fact that the isomorphism P in Theorem 11.3 is an $\mathcal{O}_p$ algebra isomorphism.

Property (4). Let the measures $\mu,\ \nu$ correspond respectively to the power series $f,\ g \in \mathcal{O}_p[[X]]$ (i.e., $\mu = \mu_f,\ \nu = \mu_g$). Then the power series corresponding to the convolution $\mu * \nu$ is fg:

$$\mu_f * \mu_g = \mu_{fg}.$$

Proof. By Eq. (11.1), we have

$$\mu_n(r) = \frac{1}{p^n} \sum_{\zeta^{p^n}=1} \zeta^{-r} f(\zeta - 1),$$

$$\nu_n(k - r) = \frac{1}{p^n} \sum_{\zeta^{p^n}=1} \zeta^{-k+r} g(\zeta - 1).$$

Substituting this into the right-hand side of (11.2), we obtain

$$(\mu * \nu)_n(k) = \sum_{r=0}^{p^n-1} \frac{1}{p^n} \sum_{\zeta^{p^n}=1} \zeta^{-r} f(\zeta - 1) \frac{1}{p^n} \sum_{\xi^{p^n}=1} \xi^{-k+r} g(\xi - 1)$$

$$= \frac{1}{p^n} \sum_{\zeta} \sum_{\xi} f(\zeta - 1) g(\xi - 1) \xi^{-k} \cdot \frac{1}{p^n} \sum_{r=0}^{p^n-1} (\xi/\zeta)^r$$

$$= \frac{1}{p^n} \sum_{\zeta} f(\zeta - 1) g(\zeta - 1) \zeta^{-k}$$
$$= \mu_{fg,n}(k).$$

Here ζ and ξ run through all p^n-th roots of 1. From this, Property (4) follows. □

11.2 Bernoulli Measure

We define a specific measure called the Bernoulli measure. Recall that the first Bernoulli polynomial is by definition equal to

$$B_1(x) = x - \frac{1}{2}.$$

In the following, p denotes an *odd* prime. For each natural number n and $x \in X_n = \mathbf{Z}/p^n\mathbf{Z}$, set

$$E_n(x) = B_1\left(\left\{\frac{x}{p^n}\right\}\right),$$

where in the right-hand side, we regard x as an integer representing $x \bmod p^n$, and for $w \in \mathbf{R}$, $\{w\}$ is the real number satisfying $0 \le \{w\} < 1$ and $w - \{w\} \in \mathbf{Z}$ (the fractional part of w). Then $E = \{E_n\}$ is a measure on $\mathbf{Z}_p$ but is not $\mathcal{O}_p$-valued. We modify this as follows in order to have an $\mathcal{O}_p$-valued measure. Take an invertible element c in $\mathbf{Z}_p$ (i.e. $c \in \mathbf{Z}_p^\times$), and for $x \in X_n = \mathbf{Z}/p^n\mathbf{Z}$, let

$$E_{c,n}(x) = E_n(x) - cE_n(c^{-1}x).$$

We understand $c^{-1}x$ as an element in $X_n = \mathbf{Z}/p^n\mathbf{Z}$. It is easy to see that $E_c = \{E_{c,n}\}$ is an $\mathcal{O}_p$-valued measure. We call this the Bernoulli measure.

Proposition 11.5. (1) *The formal power series corresponding to the Bernoulli measure E_c is given by*

$$f_c(X) = \frac{1}{X} - \frac{c}{(1+X)^c - 1}.$$

(2) *Let k be a natural number. For $c \in \mathbf{Z}_p^\times$ with $c^k \neq 1$, we have*

$$\frac{B_k}{k} = \frac{(-1)^k}{1-c^k} \int_{\mathbf{Z}_p} x^{k-1}\, dE_c.$$

In particular, if $p - 1 \nmid k$, then $B_k/k \in \mathbf{Z}_{(p)}$.

Proof. (1) Since $c \in \mathbf{Z}_p^\times$, we see $f_c \in \mathbf{Z}_p[[X]]$, the first two terms of $f_c(X)$ being

$$f_c(X) = \frac{c-1}{2} + \frac{1-c^2}{12}X + \cdots .$$

Let $\mu = \{\mu_n\}$ be the measure on $\mathbf{Z}_p$ corresponding to f_c by Theorem 11.3. For $r \in X_n = \mathbf{Z}/p^n\mathbf{Z}$ we have

$$\begin{aligned}\mu_n(r) &= \frac{1}{p^n} \sum_{\zeta^{p^n}=1} \zeta^{-r} f_c(\zeta - 1) \\ &= \frac{1}{p^n} f_c(0) + \frac{1}{p^n} \sum_{\zeta^{p^n}=1,\, \zeta\neq 1} \zeta^{-r} \left(\frac{1}{\zeta - 1} - \frac{c}{\zeta^c - 1} \right).\end{aligned}$$

Now we use Lemma 8.5 on p. 110. For $\zeta^{p^n} = 1,\ \zeta \neq 1$ and $f = p^n$, the lemma gives

$$\frac{1}{\zeta^c - 1} = \frac{1}{f} \sum_{j=1}^{f-1} j\zeta^{cj}$$

since $(c, p) = 1$. By this, if we choose l so that $cl \equiv k \bmod p^n,\ 0 \leq l < p^n$, we obtain

$$\begin{aligned}\frac{1}{f} \sum_{\zeta^{p^n}=1,\, \zeta\neq 1} \zeta^{-k} \frac{c}{\zeta^c - 1} &= \frac{c}{f^2} \sum_{\zeta^{p^n}=1} \zeta^{-k} \sum_{j=1}^{f-1} j\zeta^{cj} - \frac{c(f-1)}{2f} \\ &= \frac{cl}{f} - \frac{c(f-1)}{2f} \\ &= c\left\{ \frac{c^{-1}k}{p^n} \right\} - \frac{c}{2} + \frac{c}{2f}\end{aligned}$$

and by substituting this into the formula for $\mu_n(r)$ above and noting that $f_c(0) = (c-1)/2$, we have

$$\begin{aligned}\mu_n(r) &= \frac{c-1}{2f} + \left(\left\{ \frac{r}{p^n} \right\} - \frac{1}{2} + \frac{1}{2f} - c\left\{ \frac{c^{-1}r}{p^n} \right\} + \frac{c}{2} - \frac{c}{2f} \right) \\ &= \left(\left\{ \frac{r}{p^n} \right\} - \frac{1}{2} \right) - c\left(\left\{ \frac{c^{-1}r}{p^n} \right\} - \frac{1}{2} \right).\end{aligned}$$

By the definition of the Bernoulli measure, we conclude $\mu_n(r) = E_{c,n}(r)$, i.e., $\mu = E_c$ and the power series corresponding to E_c is f_c.

The proof of (2) goes as follows. By Property (3) and Eq. (11.6) we have

$$\int_{\mathbf{Z}_p} x^{k-1}\, dE_c = (D^{k-1} f_c)(0) = (D_Z^{k-1} f_c^*)(0).$$

Here by definition (11.5), we have

$$\begin{aligned} f_c^*(Z) = f_c(e^Z - 1) &= \frac{1}{e^Z - 1} - \frac{c}{e^{cZ} - 1} \\ &= \sum_{n=1}^{\infty} (1 - c^n)(-1)^n B_n \frac{Z^{n-1}}{n!}, \end{aligned}$$

so we have

$$(D_Z^{k-1} f_c^*)(0) = (1 - c^k)(-1)^k \frac{B_k}{k}$$

and thus

$$\int_{\mathbf{Z}_p} x^{k-1}\, dE_c = (1 - c^k)(-1)^k \frac{B_k}{k}.$$

This gives (2). □

11.3 Kummer's Congruence Revisited

The "right" formulation of Kummer's congruence is the following.

Theorem 11.6. *Suppose p is an odd prime.*

(1) *Assume that m is a positive even integer such that $p - 1 \nmid m$. Then $B_m/m \in \mathbf{Z}_{(p)}$.*
(2) *Let a be a positive integer, and m and n positive even integers satisfying $m \equiv n \bmod (p-1)p^{a-1}$ and $m \not\equiv 0 \bmod (p-1)$. Then we have*

$$(1 - p^{m-1})\frac{B_m}{m} \equiv (1 - p^{n-1})\frac{B_n}{n} \mod p^a.$$

To prove this, we need the following integral expression of the Bernoulli number, a refined version of Proposition 11.5 (2).

Proposition 11.7. *Let k be a positive even integer and take $c \in \mathbf{Z}_p^\times$. Then we have*

$$(1 - c^k)(1 - p^{k-1})\frac{B_k}{k} = \int_{\mathbf{Z}_p^\times} x^{k-1}\, dE_c.$$

Proof. The power series that corresponds to the Bernoulli measure E_c is f_c in Proposition 11.5. As in (11.4), define from f_c a new power series g by

$$g(X) = \mathbb{U} f_c(X) = f_c(X) - \frac{1}{p} \sum_{\zeta^p=1} f_c(\zeta(1+X)-1).$$

We have $g \in \mathcal{O}_p[[X]]$ and so we let $\mu = \mu_g$ be the measure on $\mathcal{O}_p$ obtained from g. By Property (2) on p. 192 we have

$$\int_{\mathbf{Z}_p^\times} x^{k-1}\, dE_c = \int_{\mathbf{Z}_p} x^{k-1}\, d\mu.$$

Further, using Property (3) on p. 194 and (11.6) one sees

$$\int_{\mathbf{Z}_p} x^{k-1}\, d\mu = (D^{k-1} g)(0) = (D_Z^{k-1} g^*)(0).$$

We compute the value $(D_Z^{k-1} g^*)(0)$. First,

$$g^*(Z) = \frac{1}{e^Z-1} - \frac{c}{e^{cZ}-1} - \frac{1}{p}\sum_{\zeta^p=1}\left(\frac{1}{\zeta e^Z-1} - \frac{c}{\zeta^c e^{cZ}-1}\right).$$

Here, since

$$\frac{1}{p}\sum_{\zeta^p=1} \frac{1}{\zeta X-1} = \frac{1}{X^p-1},$$

we get

$$\begin{aligned}
g^*(Z) &= \frac{1}{e^Z-1} - \frac{c}{e^{cZ}-1} - \left(\frac{1}{e^{pZ}-1} - \frac{c}{e^{cpZ}-1}\right) \\
&= \sum_{k=0}^{\infty} (1-c^k)(-1)^k \frac{B_k}{k!} Z^{k-1} - \sum_{k=0}^{\infty} (1-c^k)(-1)^k \frac{B_k}{k!} (pZ)^{k-1} \\
&= \sum_{k=1}^{\infty} (1-c^k)(1-p^{k-1})(-1)^k \frac{B_k}{k!} Z^{k-1}.
\end{aligned}$$

Hence if k is even we have

$$(D_Z^{k-1} g^*)(0) = (1-c^k)(1-p^{k-1})\frac{B_k}{k},$$

and the proposition is established. $\square$

Proof of Theorem 11.6. The first assertion is already given in Theorem 3.2, but we give here an alternative proof for that too. Since we assumed $m \not\equiv 0 \bmod p-1$, we can take $c \in \mathbf{Z}$ such that $(c, p) = 1$ and $c^m \not\equiv 1 \bmod p$. For instance one may take a primitive root mod p. From the proposition above, we have

$$(1-c^n)(1-p^{n-1})\frac{B_n}{n} = \int_{\mathbf{Z}_p^\times} x^{n-1}\, dE_c$$

and

$$(1-c^m)(1-p^{m-1})\frac{B_m}{m} = \int_{\mathbf{Z}_p^\times} x^{m-1}\, dE_c.$$

The assumption $m \equiv n \bmod (p-1)p^{a-1}$ gives $c^{n-m} \equiv 1 \bmod p^a$, and since we assumed $(1-c^m, p) = 1$, we have also $(1-c^n, p) = 1$. Since E_c is an $\mathcal{O}_p$ measure, the above integral values are in $\mathcal{O}_p$ and we see that B_n/n and $B_m/m \in \mathbf{Z}_{(p)}$. Since $x^{m-1} \equiv x^{n-1} \bmod p^a$ if $x \in \mathbf{Z}_p^\times$, and since E_c is an $\mathcal{O}_p$-valued measure, we have

$$(1-c^n)\left((1-p^{n-1})\frac{B_n}{n} - (1-p^{m-1})\frac{B_m}{m}\right) \in p^a\mathcal{O}_p.$$

The left-hand side being contained in $\mathbf{Z}_p$, we conclude

$$(1-p^{n-1})\frac{B_n}{n} - (1-p^{m-1})\frac{B_m}{m} \in p^a\mathbf{Z}_p.$$

This proves the theorem. □

Theorem 3.2 is a corollary of Theorem 11.6. Indeed, if $a < m \le n$, then by Theorem 11.6, we have

$$\begin{aligned}
&(1-p^{m-1})\frac{B_m}{m} - (1-p^{n-1})\frac{B_n}{n} \\
&= (1-p^{m-1})\left(\frac{B_m}{m} - \frac{B_n}{n}\right) + \frac{B_n}{n}(p^{n-m}-1)p^{m-1} \\
&\equiv 0 \bmod p^a.
\end{aligned}$$

Since $p-1 \nmid n$, we have $B_n/n \in \mathbf{Z}_{(p)}$ by Theorem 11.6. Since $a \le m-1$, we have $p^{m-1}B_n/n \in p^a\mathbf{Z}_{(p)}$. Hence we have

$$\frac{B_m}{m} - \frac{B_n}{n} \equiv 0 \bmod p^a.$$

Exercise 11.8. Give an example of an odd prime p and integers $2 \le a = m < n$ such that the congruence in Theorem 3.2 does not hold. Check that for the same choice of a, n, m and p, the congruence of Theorem 11.6 surely holds.
Hint: For example, put $p = 5$, $a = m = 2$ and $n = 22$ and use the following values:

$$B_2 = \frac{1}{6}, \qquad B_{22} = \frac{854513}{138}.$$

Exercise 11.9. Show that the Bernoulli number B_n is given by the limit (p-adic limit in $\mathbf{Q}_p$)

$$\lim_{m\to\infty} \frac{1}{p^m} \sum_{i=0}^{p^m-1} i^n.$$

(For a function $f : \mathbf{Z}_p \to \mathbf{Q}_p$ with a suitable condition, the limit

$$\lim_{m\to\infty} \frac{1}{p^m} \sum_{i=0}^{p^m-1} f(i)$$

is sometimes referred to as the Volkenborn integral of f over $\mathbf{Z}_p$. See [94, 95] for details.)