p-Adic Measures and Bernoulli Numbers

Adam Bowers[1]

Introduction

The constants B_k in the Taylor series expansion

$$\frac{t}{e^t - 1} = \sum_{k=0}^{\infty} B_k \frac{t^k}{k!}$$

are known as the Bernoulli numbers. The first few are

$$1,\ -\frac{1}{2},\ \frac{1}{6},\ 0, -\frac{1}{30},\ 0,\ \frac{1}{42}, \cdots.$$

These numbers play an important role in number theory. For example, the Reimann zeta-function essentially equals a Bernoulli number at negative integers:

$$\zeta(1-k) = -\frac{B_k}{k}$$

for $k \geq 2$. A few of the interesting classical results about Bernoulli numbers are given in the following theorem.

Theorem. Let $k \in \mathbb{Z}^+$ and p be a prime. Then

1. If $a \in \mathbb{Z}$, then
$$a(a^k - 1)B_k \in \mathbb{Z}.$$
2. If $a \in \mathbb{Z}$, then
$$a^k(a^k - 1)\frac{B_k}{k} \in \mathbb{Z}.$$

[1]This paper was written as an assignment in a course taught by Keith Conrad during Fall Semester 2004 at the University of Connecticut. Anything correct is only so due to Professor Conrad's diligent revision.

3. If $k \not\equiv 0 \bmod p-1$, then
$$\frac{B_k}{k} \in \mathbb{Z}_p.$$
4. For k_1 and k_2 even, if $k_1 \equiv k_2 \not\equiv 0 \bmod p-1$, then
$$\frac{B_{k_1}}{k_1} \equiv \frac{B_{k_2}}{k_2} \bmod p.$$
5. For k even or $k = 1$,
$$B_k + \sum_{p-1|k} \frac{1}{p} \in \mathbb{Z}$$
.

This paper will develop the ideas needed to prove these claims bt p-adic methods and in the process show the intimate relationship between Bernoulli numbers and p-adic measures.

p-Adic distributions

Let X be any compact-open subset of $\mathbb{Q}_p$, such as $\mathbb{Z}_p$ or $\mathbb{Z}_p^\times$. A **p-adic distribution** μ on X is defined to be an additive map from the collection of compact-open sets in X to $\mathbb{Q}_p$. Additivity means
$$\mu\Big(\bigcup_{k=1}^{n} U_k\Big) = \sum_{k=1}^{n} \mu(U_k),$$
where $n \geq 1$ and $\{U_1, \ldots, U_n\}$ is any collection of pair-wise disjoint compact-open sets in X.

Just from the definition, it is not clear how to construct a p-adic distribution. Fortunately, $\mathbb{Q}_p$ has some forgiving topological properties. The set $\mathbb{Q}_p$ has a topological basis of compact-open sets of the form $a + p^n\mathbb{Z}_p$, where $a \in \mathbb{Q}_p$ and $n \in \mathbb{Z}$ (these are the closed balls in $\mathbb{Q}_p$). Consequently, if U is any compact-open subset of $\mathbb{Q}_p$, it can be written as a finite disjoint union of sets
$$U = \bigcup_{j=1}^{k} \Big(a_j + p^N\,\mathbb{Z}_p\Big)$$

for some $N \in \mathbb{Z}$ and $a_1, \ldots, a_k \in \mathbb{Q}_p$. There are many such representations. In fact, each "p-adic ball" $a + p^n\mathbb{Z}_p$ can be represented as the union of "smaller" balls,

$$a + p^n\mathbb{Z}_p = \bigcup_{b=0}^{p-1} \Big(a + bp^n + p^{n+1}\,\mathbb{Z}_p \Big).$$

This follows from the fact that these balls are closed under intersection, so that they intersect if and only if one is contained in the other.

The ability to decompose compact-open subsets of $\mathbb{Q}_p$ into sets of the form $a + p^N\mathbb{Z}_p$ allows one to reformulate the additivity condition into a more practical condition.

Proposition. Every map μ from the collection of compact-open sets in X to $\mathbb{Q}_p$ for which

$$\mu\Big(a + p^n\,\mathbb{Z}_p \Big) = \sum_{b=0}^{p-1} \mu\Big(a + bp^n + p^{n+1}\,\mathbb{Z}_p \Big) \tag{1}$$

holds whenever $a + p^n\mathbb{Z}_p \in X$, extends to a p-adic distribution on X.

Equation 1 is called a **distribution relation**. The proof follows from the additivity of μ and the topological properties described above. For more details, see [2], page 32.

The proposition is quite useful. Any compact-open set in X can be written as a disjoint union of balls $a + p^n\mathbb{Z}_p$, so one can check whether or not a set function on these balls satisfies Equation 1 and then extend it to a distribution on X. As a simple example, consider the Haar distribution μ_{Haar} defined by

$$\mu_{Haar}\Big(a + p^n\,\mathbb{Z}_p \Big) = \frac{1}{p^n}$$

for $a \in \mathbb{Z}_p$ and $n \in \mathbb{N}$. This extends to a distribution on $\mathbb{Z}_p$ since it satisfies the distribution relation:

$$\sum_{b=0}^{p-1} \mu_{Haar}\Big(a + bp^n + p^{n+1}\,\mathbb{Z}_p \Big) = \sum_{b=0}^{p-1} \frac{1}{p^{n+1}} = \frac{1}{p^n} = \mu_{Haar}\Big(a + p^n\,\mathbb{Z}_p \Big).$$

How does one construct distributions on $\mathbb{Z}_p$? Can they be constructed from, say, polynomials? Suppose f_k is a polynomial of degree k. Define a map μ_k on the balls in $\mathbb{Z}_p$ as follows:

$$\mu_k\Big(a + p^n\,\mathbb{Z}_p\Big) = p^{n(k-1)} f_k\left(\frac{\{a\}_n}{p^n}\right),$$

where $\{a\}_n$ is the unique number in the set $\{0, 1, \ldots, p^n - 1\}$ such that $\{a\}_n \equiv a \bmod p^n$. What could f_k look like? If μ_k is a distribution, it must satisfy the distribution relation in (1), so taking a to be from the set $\{0, 1, \ldots, p^n - 1\}$,

$$p^{n(k-1)} f_k\left(\frac{a}{p^n}\right) = \sum_{b=0}^{p-1} \mu_k\Big(a + bp^n + p^{n+1}\,\mathbb{Z}_p\Big) = \sum_{b=0}^{p-1} p^{(n+1)(k-1)} f_k\left(\frac{a + bp^n}{p^{n+1}}\right).$$

Thus, in order to be a distribution,

$$f_k\left(\frac{a}{p^n}\right) = p^{k-1} \sum_{b=0}^{p-1} f_k\left(\frac{\frac{a}{p^n} + b}{p}\right).$$

This is to hold for all $n \geq 1$ and every $a \in \{0, 1, \ldots, p^n - 1\}$, so μ_k is a distribution on $\mathbb{Z}_p$ if and only if f_k satisfies the identity

$$f_k(x) = p^{k-1} \sum_{b=0}^{p-1} f_k\left(\frac{x + b}{p}\right).$$

As it turns out, for each $k \in \mathbb{N}$ the only (monic) polynomial of degree k that satisfies the above equation is $\mathbb{B}_k(x)$, the k^{th} Bernoulli polynomial (see below). In fact, the k^{th} Bernoulli polynomial satisfies the stronger condition: for any $M \in \mathbb{N}$,

$$\mathbb{B}_k(x) = M^{k-1} \sum_{b=0}^{M-1} \mathbb{B}_k\left(\frac{x + b}{M}\right). \tag{2}$$

What are the Bernoulli polynomials? Recall the definition of the Bernoulli numbers given in the introduction. They were defined by the following Taylor series expansion:

$$\frac{t}{e^t - 1} = \sum_{k=0}^{\infty} B_k \frac{t^k}{k!}.$$

In the above series, B_k is the k^{th} Bernoulli number. The first few are

$$B_0 = 1,\ B_1 = -\frac{1}{2},\ B_2 = \frac{1}{6},\ B_3 = 0, B_4 = -\frac{1}{30},\ B_5 = 0,\ B_6 = \frac{1}{42}, \cdots.$$

It can be shown that $B_k = 0$ for all odd $k > 1$.

For each $k \in \mathbb{N}$, define the k^{th} **Bernoulli polynomial**, denoted $\mathbb{B}_k(x)$, by the following formula:

$$\mathbb{B}_k(x) = \sum_{j=0}^{k} \left(\begin{array}{c} k \\ j \end{array} \right) B_{k-j} x^j.$$

So for each $k \geq 0$,

$$\mathbb{B}_k(x) = B_0 x^k + k B_1 x^{k-1} + \cdots = x^k - \frac{k}{2} x^{k-1} + \cdots.$$

The first few Bernoulli polynomials are:

$$\begin{aligned}
\mathbb{B}_0(x) &= 1 \\
\mathbb{B}_1(x) &= x - \frac{1}{2} \\
\mathbb{B}_2(x) &= x^2 - x + \frac{1}{6} \\
\mathbb{B}_3(x) &= x^3 - \frac{3}{2}x^2 + \frac{1}{2}x \\
\mathbb{B}_4(x) &= x^4 - 2x^3 + x^2 - \frac{1}{30} \\
\mathbb{B}_5(x) &= x^5 - \frac{5}{2}x^4 + \frac{5}{3}x^3 - \frac{1}{6}x \\
\mathbb{B}_6(x) &= x^6 - 3x^5 + \frac{5}{2}x^4 - \frac{1}{2}x^2 + \frac{1}{42} \\
\mathbb{B}_7(x) &= x^7 - \frac{7}{2}x^6 + \frac{7}{2}x^5 - \frac{7}{6}x^3 + \frac{1}{6}x
\end{aligned}$$

Note that for each $k \in \mathbb{N}$,

$$\mathbb{B}_k(0) = B_k$$

and

$$\mathbb{B}_k'(x) = k\mathbb{B}_{k-1}(x)$$

for all $x \in \mathbb{Q}_p$.

The Bernoulli polynomials extend the notion of Bernoulli numbers in that they satisfy the formal identity

$$\frac{te^{xt}}{e^t - 1} = \sum_{k=0}^{\infty} \mathbb{B}_k(x) \frac{t^k}{k!}.$$

Returning to the topic of p-adic distributions, it can now be seen that μ_k as defined by

$$\mu_k\Big(a + p^n\, \mathbb{Z}_p\Big) = p^{n(k-1)} \mathbb{B}_k\left(\frac{\{a\}_n}{p^n}\right)$$

for $a \in \mathbb{Z}_p$ is in fact a distribution on $\mathbb{Z}_p$, because the Bernoulli polynomials satisfy Equation 2. What are some of these **Bernoulli distributions**? Consider the cases $k = 0, 1, 2$. To simplify the following calculations, a will be taken from the set $\{0, 1, \ldots, p^n - 1\}$.

When $k = 0$, the distribution is a familiar one,

$$\mu_0\Big(a + p^n\, \mathbb{Z}_p\Big) = p^{n(0-1)} \mathbb{B}_0\left(\frac{a}{p^n}\right) = \frac{1}{p^n}.$$

This is just the Haar distribution, which was introduced above. When $k = 1$,

$$\mu_1\Big(a + p^n\, \mathbb{Z}_p\Big) = p^{n(1-1)} \mathbb{B}_1\left(\frac{a}{p^n}\right) = \frac{a}{p^n} - \frac{1}{2}.$$

This is known as the Mazur distribution and is denoted μ_{Mazur}. A similar calculation reveals that

$$\mu_2\Big(a + p^n\, \mathbb{Z}_p\Big) = p^{n(2-1)} \mathbb{B}_2\left(\frac{a}{p^n}\right) = \frac{a^2}{p^n} - a + \frac{p^n}{6}.$$

In general,

$$\mu_k\Big(a + p^n\, \mathbb{Z}_p\Big) = \frac{a^k}{p^n} + \Big(\text{term in } \frac{1}{d_k}\, \mathbb{Z}_p\Big),$$

where d_k is the least common multiple of the denominators of $B_0, B_1, \ldots, B_k$. [Note that d_k is independent of a and n.]

Regardless of the choice of k, when $a \in \mathbb{Z}_p^\times$ (e.g., $a = 1$)

$$\left|\mu_k\Big(a + p^n\,\mathbb{Z}_p\Big)\right|_p = p^n,$$

which tends to infinity as $n \to \infty$. Thus the "small" balls $1 + p^n\mathbb{Z}_p$ have large μ_k-values.

p-Adic measures

Again, let X be any compact-open subset of $\mathbb{Q}_p$, such as $\mathbb{Z}_p$ or $\mathbb{Z}_p^\times$. A p-adic distribution μ on X is called a **p-adic measure** on X if its values on compact-open sets $U \subset X$ are bounded; i.e., there exists some $B \in \mathbb{R}$ such that

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

for all compact-open sets $U \subset X$. The least bound is denoted $||\mu||$.

The Dirac distribution μ_α on $\mathbb{Z}_p$, concentrated at $\alpha \in \mathbb{Z}_p$, is defined by

$$\mu_\alpha(U) = \begin{cases} 1 & \text{if } \alpha \in U, \\ 0 & \text{otherwise.} \end{cases}$$

This is a measure. The proof is simple and, as is all-too common with simple proofs, uninteresting.

The Bernoulli distributions are much more interesting, but not bounded (as was shown above), so they are not p-adic measures. Is there any way to "fix" this problem? For all $\alpha \in \mathbb{Z}_p^\times$ and each $k \in \mathbb{N}$, define the k^{th} **regularized Bernoulli distributions** on $\mathbb{Z}_p$ by

$$\mu_{k,\alpha}(U) = \mu_k(U) - \alpha^k \mu_k(\alpha^{-1}U).$$

This adjustment to the k^{th} Bernoulli distribution removes the divergent term, making the k^{th} regularized Bernoulli distribution bounded, so actually a measure. The proof of this claim is involved and given below.

The case when $k = 0$ is quite simple: for any $n \in \mathbb{N}$ and $0 \leq a \leq p^n - 1$,

$$\begin{aligned} \mu_{0,\alpha}\Big(a + p^n\,\mathbb{Z}_p\Big) &= \mu_0\Big(a + p^n\,\mathbb{Z}_p\Big) - \alpha^0\mu_0\Big(\alpha^{-1}a + p^n\,\mathbb{Z}_p\Big) \\ &= \frac{1}{p^n} - 1 \cdot \frac{1}{p^n} = 0. \end{aligned}$$

Thus $\mu_{0,\alpha}$ is identically zero, so is a measure, albeit not a very interesting one. What about the case when $k = 1$? It will be shown that

$$\Big|\mu_{1,\alpha}\Big(a + p^n\,\mathbb{Z}_p\Big)\Big|_p \leq 1.$$

Again let $n \in \mathbb{N}$ and $0 \leq a \leq p^n - 1$. Then

$$\begin{aligned} \mu_{1,\alpha}\Big(a + p^n\,\mathbb{Z}_p\Big) &= \mu_1\Big(a + p^n\,\mathbb{Z}_p\Big) - \alpha\mu_1\Big(\alpha^{-1}a + p^n\,\mathbb{Z}_p\Big) \\ &= \frac{a}{p^n} - \frac{1}{2} - \alpha\Big(\frac{\{\alpha^{-1}a\}_n}{p^n} - \frac{1}{2}\Big) \\ &= \frac{a - \alpha\{\alpha^{-1}a\}_n}{p^n} + \frac{\alpha - 1}{2}. \end{aligned}$$

In the above calculation, $\{\alpha^{-1}a\}_n$ is defined to be the coset representative of $\alpha^{-1}a + p^n\mathbb{Z}_p$ which is contained in $\{0, 1, 2, \ldots, p^n - 1\}$; that is

$$\{\alpha^{-1}a\}_n \equiv \alpha^{-1}a \bmod p^n$$

and $0 \leq \alpha^{-1}a \leq p^n - 1$.

So why is this bounded by 1? Consider the second term first:

$$\frac{\alpha - 1}{2} = (\alpha - 1)\left(\frac{1}{2}\right).$$

If $p \neq 2$ then $\frac{1}{2} \in \mathbb{Z}_p$ and $\alpha - 1 \in \mathbb{Z}_p$. If $p = 2$, then since $\alpha \in \mathbb{Z}_p^\times$, it follows that $\alpha - 1 \equiv 0 \bmod 2$, i.e. $\alpha - 1$ is a multiple of 2. Either way, $\frac{\alpha-1}{2} \in \mathbb{Z}_p$, so

$$\Big|\frac{\alpha - 1}{2}\Big|_p \leq 1.$$

Now consider the first term:

$$\frac{a - \alpha\{\alpha^{-1}a\}_n}{p^n}.$$

By definition

$$\{\alpha^{-1}a\}_n \equiv \alpha^{-1}a \bmod p^n,$$

so

$$\{\alpha^{-1}a\}_n = \alpha^{-1}a + Ap^n,$$

for some $A \in \mathbb{Z}_p$. Thus (solving for A)

$$A = \frac{\alpha^{-1}a}{p^n} - \frac{\{\alpha^{-1}a\}_n}{p^n}$$

or

$$\alpha A = \frac{\alpha\alpha^{-1}a}{p^n} - \frac{\alpha\{\alpha^{-1}a\}_n}{p^n} = \frac{a - \alpha\{\alpha^{-1}a\}_n}{p^n}.$$

Hence

$$\left|\frac{a - \alpha\{\alpha^{-1}a\}_n}{p^n}\right|_p = |\alpha A|_p \leq 1,$$

where this inequality follows from both α and A sitting inside $\mathbb{Z}_p$. Therefore

$$\left|\mu_{1,\alpha}\Big(a + p^n\,\mathbb{Z}_p\Big)\right|_p \leq 1,$$

as required. It remains to show that the $\mu_{k,\alpha}$ are bounded for $k > 1$. This will follow from the next theorem.

Theorem. Let d_k be the least common denominator of the coefficients of $\mathbb{B}_k(x)$ (as before). Then

$$d_k\mu_{k,\alpha}\Big(a + p^n\,\mathbb{Z}_p\Big) \equiv d_k k a^{k-1}\mu_{1,\alpha}\Big(a + p^n\,\mathbb{Z}_p\Big) \bmod p^n, \tag{3}$$

where both sides lie in $\mathbb{Z}_p$.

Before beginning the proof, a remark: Note d_k is independent of a and n. So, as n gets large, (3) says that $\mu_{k,\alpha}\Big(a+p^n\mathbb{Z}_p\Big)$ is very close to $ka^{k-1}\mu_{1,\alpha}\Big(a+p^n\,\mathbb{Z}_p\Big)$.

Proof. By definition,

$$d_k\mu_{k,\alpha}\Big(a + p^n\,\mathbb{Z}_p\Big) = d_k\Big[\mu_k\Big(a + p^n\,\mathbb{Z}_p\Big) - \alpha^k\mu_k\Big(\alpha^{-1}a + p^n\,\mathbb{Z}_p\Big)\Big]$$

$$= d_k\Big[p^{n(k-1)}\mathbb{B}_k\left(\frac{a}{p^n}\right) - \alpha^k p^{n(k-1)}\mathbb{B}_k\left(\frac{\{\alpha^{-1}a\}_n}{p^n}\right)\Big].$$

When these polynomials are expanded out by a few terms, the result is an unfriendly looking expression:

$$d_k p^{n(k-1)}\Bigg(\left[\left(\frac{a}{p^n}\right)^k - \frac{k}{2}\left(\frac{a}{p^n}\right)^{k-1} + \cdots\right] \\ -\alpha^k\left[\left(\frac{\{\alpha^{-1}a\}_n}{p^n}\right)^k - \frac{k}{2}\left(\frac{\{\alpha^{-1}a\}_n}{p^n}\right)^{k-1} + \cdots\right]\Bigg).$$

The terms which are so conveniently concealed by $\cdots$ have as denominators $\{p^{n(k-2)}, p^{n(k-1)}, \ldots p^n, 1\}$ (respectively), since the polynomial $d_k\mathbb{B}_k(x)$ has integral coefficients by the construction of d_k. So when these terms are multiplied by the leading $p^{n(k-1)}$, the denominators will cancel, leaving a factor of p^n or greater; hence the hidden terms are congruent to zero (mod p^n). This means the unfriendly expression above differs by an element of $p^n\mathbb{Z}_p$ from the slightly more friendly expression below:

$$d_k p^{n(k-1)}\left[\left(\frac{a}{p^n}\right)^k - \frac{k}{2}\left(\frac{a}{p^n}\right)^{k-1} - \alpha^k\left(\frac{\{\alpha^{-1}a\}_n}{p^n}\right)^k + \alpha^k\frac{k}{2}\left(\frac{\{\alpha^{-1}a\}_n}{p^n}\right)^{k-1}\right],$$

which, if nothing else, at least fits on one line. Simplifying this a bit gives something even better:

$$d_k\mu_{k,\alpha}\Big(a + p^n\,\mathbb{Z}_p\Big) + \Big(\text{term in } p^n\,\mathbb{Z}_p\Big)$$

$$= d_k\left[\frac{a^k}{p^n} - \frac{k}{2}a^{k-1} - \frac{\alpha^k\{\alpha^{-1}a\}_n^k}{p^n} + \frac{k}{2}\alpha^k\{\alpha^{-1}a\}_n^{k-1}\right]$$

$$= d_k\left[\frac{a^k - \alpha^k\{\alpha^{-1}a\}_n^k}{p^n} - \frac{k}{2}\Big(a^{k-1} - \alpha^k\{\alpha^{-1}a\}_n^{k-1}\Big)\right].$$

By definition of $\{\alpha^{-1}a\}_n$, the second term is congruent (mod p^n) to

$$\frac{k}{2}\Big(a^{k-1} - \alpha^k(\alpha^{-1}a)^{k-1}\Big) = \frac{k}{2}a^{k-1}\Big(1-\alpha\Big),$$

keeping in mind that the second term in fact has no denominator, despite the presence of the $\frac{1}{2}$, because d_k contains a factor of 2, by construction.

The first term may have a denominator, namely p^n. Recall that

$$\{\alpha^{-1}a\}_n = \alpha^{-1}a - Ap^n,$$

for some $A \in \mathbb{Z}_p$. Then

$$\{\alpha^{-1}a\}_n^k = (\alpha^{-1}a - Ap^n)^k = \sum_{j=0}^{k} \left(\begin{array}{c} k \\ j \end{array} \right) (\alpha^{-1}a)^{k-j}(-Ap^n)^j$$

by the binomial theorem. Thus

$$\begin{aligned} \frac{\{\alpha^{-1}a\}_n^k}{p^n} &= \sum_{j=0}^{k} \left(\begin{array}{c} k \\ j \end{array} \right) (\alpha^{-1}a)^{k-j}(-A)^j(p^n)^{j-1} \\ &= \frac{(\alpha^{-1}a)^k}{p^n} + k(\alpha^{-1}a)^{k-1}(-A) + \cdots \\ &\equiv \frac{(\alpha^{-1}a)^k}{p^n} - k(\alpha^{-1}a)^{k-1}A \mod p^n. \end{aligned}$$

Then, since $\alpha \in \mathbb{Z}_p$,

$$\begin{aligned} \alpha^k \cdot \frac{\{\alpha^{-1}a\}_n^k}{p^n} &\equiv \frac{\alpha^k(\alpha^{-1}a)^k}{p^n} - k\alpha^k(\alpha^{-1}a)^{k-1}A \mod p^n \\ &= \frac{a^k}{p^n} - k\alpha a^{k-1}A. \end{aligned}$$

Therefore,

$$\frac{a^k - \alpha^k\{\alpha^{-1}a\}_n^k}{p^n} = \frac{a^k}{p^n} - \frac{\alpha^k\{\alpha^{-1}a\}_n^k}{p^n}$$

$$\begin{aligned} &\equiv \frac{a^k}{p^n} - \left(\frac{a^k}{p^n} - ka^{k-1}\alpha A\right) \mod p^n \\ &= ka^{k-1}\alpha A \\ &= ka^{k-1}\alpha\left(\frac{\alpha^{-1}a - \{\alpha^{-1}a\}_n}{p^n}\right) \\ &= ka^{k-1}\left(\frac{a - \alpha\{\alpha^{-1}a\}_n}{p^n}\right). \end{aligned}$$

Putting all of these calculations together,

$$\begin{aligned} &d_k\mu_{k,\alpha}\Big(a + p^n\,\mathbb{Z}_p\Big) + \Big(\text{term in } p^n\,\mathbb{Z}_p\Big) \\ &\quad = d_k\left[ka^{k-1}\left(\frac{a - \alpha\{\alpha^{-1}a\}_n}{p^n}\right) - \frac{k}{2}a^{k-1}\Big(1-\alpha\Big)\right] \\ &\quad = d_k ka^{k-1}\left[\frac{a - \alpha\{\alpha^{-1}a\}_n}{p^n} + \frac{\alpha - 1}{2}\right] \\ &\quad = d_k ka^{k-1}\mu_{1,\alpha}\Big(a + p^n\,\mathbb{Z}_p\Big). \end{aligned}$$

This proves the theorem. Note that it is now known that everything is in $\mathbb{Z}_p$, so the congruence in the statement of the theorem makes sense. $\diamond$

Corollary. For each $k > 1$ and $\alpha \in \mathbb{Z}_p^\times$, the Bernoulli distribution $\mu_{k,\alpha}$ is bounded, hence a p-adic measure.

Proof. Let U be a compact-open set in X. Without loss of generality, assume $U = a + p^n\mathbb{Z}_p$ for some $n \in \mathbb{N}$ and $0 \le a \le p^n - 1$. By the theorem,

$$d_k\mu_{k,\alpha}(U) = d_k\mu_{k,\alpha}\Big(a + p^n\,\mathbb{Z}_p\Big) = d_k ka^{k-1}\mu_{1,\alpha}\Big(a + p^n\,\mathbb{Z}_p\Big) + Ap^n,$$

for some $A \in \mathbb{Z}_p$. Thus

$$|\mu_{k,\alpha}(U)|_p \;\le\; \max\left\{\left|ka^{k-1}\mu_{1,\alpha}\Big(a + p^n\,\mathbb{Z}_p\Big)\right|_p, \left|A\cdot\frac{p^n}{d_k}\right|_p\right\}$$

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

For n sufficiently large, $\left|\frac{p^n}{d_k}\right|_p < 1$, so $|\mu_{k,\alpha}(U)|_p \leq 1$ by the non-archimedean inequality. It also follows from the non-archimedean inequality that $|\mu_{k,\alpha}(U)|_p \leq 1$ for all compact-open U because any such set can be written as the disjoint union of p-adic balls for large enough n.

p-Adic integration

The main purpose for constructing p-adic measures is to integrate functions. The development parallels the classic treatment, beginning with the idea of Riemann sums. Suppose μ is a p-adic measure on some compact-open subset X of $\mathbb{Q}_p$, say $\mathbb{Z}_p$ or $\mathbb{Z}_p^\times$. Suppose also that f is a continuous K-valued map, where K is a finite extension of $\mathbb{Q}_p$ (or possibly $\mathbb{Q}_p$ itself). Let $N \in \mathbb{N}$ be fixed. Choose from each $a + p^N\mathbb{Z}_p$ contained in X a representative, say $x_{a,N}$. Then the N^{th} **Riemann sum** over $\{x_{a,N}\}$ is defined to be

$$S_{N,\{x_{a,N}\}} = \sum_{a+p^N\mathbb{Z}_p \subset X} f(x_{a,N})\mu(a+p^N\mathbb{Z}_p).$$

Theorem. Let μ, X and f be as above. If $f : X \to K$ is a continuous function, then the Riemann sums (as defined above) converge to a limit in K which does not depend on the choice of $\{x_{a,N}\}$. This unique limit will be denoted

$$\int_X f(x)d\mu(x)$$

or simply $\int_X f d\mu$.

Proof. By definition, the p-adic measure μ on X is bounded, so there is some $B > 0$ such that $\mu(U) \leq B$ for every compact-open set $U \subset X$.

First, convergence will be shown for a particular Riemann sum. For any given $n \in \mathbb{N}$,

$$\mathbb{Z}_p = \bigcup_{0 \le a \le p^n - 1} \Big(a + p^n \, \mathbb{Z}_p \Big)$$

(where the balls are pairwise disjoint), so for each $a \in \{0, 1, \ldots, p^n - 1\}$, select the representative in $a + p^n \mathbb{Z}_p$ to be $x_{a,n} = a$. It suffices to show the sequence $\{S_{N,\{a\}}\}$ is a Cauchy sequence. Let $\epsilon > 0$ be given. The set X is compact, so f is not only continuous, but uniformly continuous. Thus, there exists some $N_0 \in \mathbb{N}$ such that $|f(x) - f(y)|_p < \frac{\epsilon}{B}$ whenever $x \equiv y \mod p^N$, for all $N \ge N_0$.

Now choose $N \ge N_0$ large enough that every ball $a + p^N \mathbb{Z}_p$ is either contained in X or disjoint from it. Let $M > N$. Two p-adic balls intersect if and only if one is contained in the other, so for each a,

$$a + p^N \mathbb{Z}_p = \bigcup_{\substack{0 \le \hat{a} \le p^M - 1 \\ \hat{a} \equiv a \mod p^N}} \Big(\hat{a} + p^M \, \mathbb{Z}_p \Big).$$

Then by finite additivity of μ,

$$\mu\Big(a + p^N \, \mathbb{Z}_p \Big) = \sum_{\substack{0 \le \hat{a} \le p^M - 1 \\ \hat{a} \equiv a \mod p^N}} \mu\Big(\hat{a} + p^M \, \mathbb{Z}_p \Big).$$

Thus

$$S_{N,\{a\}} = \sum_{a + p^N \mathbb{Z}_p \subset X} f(a) \mu\Big(a + p^N \, \mathbb{Z}_p \Big) = \sum_{\hat{a} + p^M \mathbb{Z}_p \subset X} f(a) \mu\Big(\hat{a} + p^M \, \mathbb{Z}_p \Big),$$

where a is in the set $\{0, 1, \ldots, p^N - 1\}$ and $a \equiv \hat{a} \mod p^N$.

By construction, for each $\hat{a} \in \{0, 1, \ldots, p^M - 1\}$, the representative in the corresponding Riemann sum was $x_{\hat{a},M} = \hat{a}$. Thus

$$S_{M,\{\hat{a}\}} = \sum_{\hat{a}+p^M\mathbb{Z}_p \subset X} f(\hat{a})\mu\Big(\hat{a} + p^M\,\mathbb{Z}_p\,\Big).$$

Consequently,

$$\begin{aligned}
\Big|S_{N,\{a\}} - S_{M,\{\hat{a}\}}\Big|_p &= \left|\sum_{\hat{a}+p^M\mathbb{Z}_p \subset X} \Big(f(a) - f(\hat{a})\Big)\mu\Big(\hat{a} + p^M\,\mathbb{Z}_p\,\Big)\right|_p \\
&\leq \max\left\{\Big|f(a) - f(\hat{a})\Big|_p \cdot \left|\mu\Big(\hat{a} + p^M\,\mathbb{Z}_p\,\Big)\right|_p\right\}.
\end{aligned}$$

But $a \equiv \hat{a} \bmod p^N$, hence $\Big|f(a) - f(\hat{a})\Big|_p < \frac{\epsilon}{B}$. Therefore $\Big|S_{N,\{a\}} - S_{M,\{\hat{a}\}}\Big|_p < \epsilon$, as required.

It remains to show that the choice of representative does not matter. Suppose for each $a + p^n\mathbb{Z}_p$, the number $x'_{N,a}$ is some other representative. Then

$$\begin{aligned}
\Big|S_{N,\{a\}} - S_{M,\{x'_{N,a}\}}\Big|_p &= \left|\sum_{a+p^N\mathbb{Z}_p \subset X} \Big(f(a) - f(x'_{N,a})\Big)\mu\Big(a + p^N\,\mathbb{Z}_p\,\Big)\right|_p \\
&\leq \max\left\{\Big|f(a) - f(x'_{N,a})\Big|_p \cdot \left|\mu\Big(a + p^N\,\mathbb{Z}_p\,\Big)\right|_p\right\}.
\end{aligned}$$

As before, $a \equiv x'_{N,a} \bmod p^N$, so for an appropriately large N,

$$\left| f(a) - f(x'_{N,a}) \right|_p < \frac{\epsilon}{B},$$

hence the result. $\diamond$

The following corollary follows directly from the theorem, so the proof is omitted.

Corollary. If $f : X \to K$ is a continuous function such that $|f(x)|_p \leq A$ for all $x \in X$, and if $|\mu(U)|_p \leq B$ for all compact-open $U \subset X$, then

$$\left| \int_X f(x)\, d\mu(x) \right|_p \leq A \cdot B.$$

In particular, if $||f||_\infty \leq A$, then

$$\left| \int_X f(x)\, d\mu_{k,\alpha}(x) \right|_p \leq A.$$

In p-adic integration, the measure $\mu_{1,\alpha}$ has a special role. In some sense it can be thought of as the p-adic analog to Lebesgue measure in classical analysis (see [2], page 37). This role is made more precise in the following theorem.

Theorem. If $f : \mathbb{Z}_p \to K$ is a continuous function, then

$$\int_{\mathbb{Z}_p} f(x) d\mu_{k,\alpha}(x) = \int_{\mathbb{Z}_p} f(x) \cdot k x^{k-1} d\mu_{1,\alpha}(x). \tag{4}$$

Proof. The characteristic functions on p-adic balls are dense in in $C(\mathbb{Z}_p, K)$ (see [1]), so without loss of generality suppose $f = \chi_{c+p^n\mathbb{Z}_p}$ for some $n \in \mathbb{N}$ and $0 \leq c \leq p^n - 1$. Then

$$\int_{\mathbb{Z}_p} f(x) d\mu_{k,\alpha}(x) = \lim_{N\to\infty} \sum_{a=0}^{p^N-1} f(a) \mu_{k,\alpha}(a + p^N\mathbb{Z}_p).$$

By Equation 3, for each N and $a \in \{0, 1, \ldots, p^N - 1\}$,

$$d_k \mu_{k,\alpha}\Big(a + p^N \mathbb{Z}_p\Big) = d_k k a^{k-1} \mu_{1,\alpha}\Big(a + p^N \mathbb{Z}_p\Big) + p^N A_{N,a},$$

for some $A_{N,a} \in \mathbb{Z}_p$. Thus

$$d_k \sum_{a=0}^{p^N-1} f(a)\mu_{k,\alpha}(a + p^N\mathbb{Z}_p) = \sum_{a=0}^{p^N-1} f(a)\Big[d_k k a^{k-1} \mu_{1,\alpha}\Big(a + p^N \mathbb{Z}_p\Big) + p^N A_{N,a}\Big]$$

$$= d_k k \sum_{a=0}^{p^N-1} f(a) a^{k-1} \mu_{1,\alpha}\Big(a + p^N \mathbb{Z}_p\Big) + p^N \sum_{a=0}^{p^N-1} f(a) A_{N,a}.$$

Observe, for any $N \in \mathbb{N}$, the second term is in $p^N\mathbb{Z}_p$ since $|f| \leq 1$ and $A_{N,a} \in \mathbb{Z}_p$. Thus

$$\lim_{N\to\infty} p^N \sum_{a=0}^{p^N-1} f(a) A_{N,a} = 0.$$

Therefore,

$$\lim_{N\to\infty} d_k \sum_{a=0}^{p^N-1} f(a)\mu_{k,\alpha}(a + p^N\mathbb{Z}_p) = \lim_{N\to\infty} d_k k \sum_{a=0}^{p^N-1} f(a) a^{k-1} \mu_{1,\alpha}\Big(a + p^N \mathbb{Z}_p\Big),$$

hence

$$d_k \int_{\mathbb{Z}_p} f(x) d\mu_{k,\alpha}(x) = d_k k \int_{\mathbb{Z}_p} f(x)\ x^{k-1} d\mu_{1,\alpha}(x),$$

as required. $\diamond$

Corollary. For each $k \in \mathbb{N}$ and each $\alpha \in \mathbb{Z}_p^\times$ not a root of unity,

$$B_k = \frac{k}{1-\alpha^k} \int_{\mathbb{Z}_p} x^{k-1}\, d\mu_{1,\alpha}(x).$$

Before beginning the proof, a remark: Note the right hand side in the above expression is independent of α, simply because the left hand side does not depend on α.

PROOF. Begin by observing that for any k and any α,

$$\begin{aligned} \mu_{k,\alpha}(\mathbb{Z}_p) &= \mu_k(\mathbb{Z}_p) - \alpha^k \mu(\mathbb{Z}_p) \\ &= (1-\alpha^k)\mathbb{B}_k(0) \\ &= (1-\alpha^k)B_k. \end{aligned}$$

This follows from the definitions of μ_k and $\mu_{k,\alpha}$ with $a = 0$ and $n = 0$. By the previous theorem,

$$\int_{\mathbb{Z}_p} 1\, d\mu_{k,\alpha} = \int_{\mathbb{Z}_p} 1 \cdot kx^{k-1}\, d\mu_{1,\alpha}(x),$$

but

$$\int_{\mathbb{Z}_p} 1\, d\mu_{k,\alpha} = \lim_{N\to\infty} \sum_{a=0}^{p^N-1} 1\, \mu_{k,\alpha}\Big(a + p^N\, \mathbb{Z}_p\Big) = \mu_{k,\alpha}(\mathbb{Z}_p).$$

Thus

$$\int_{\mathbb{Z}_p} kx^{k-1}\, d\mu_{1,\alpha}(x) = (1-\alpha^k)B_k,$$

from which the result follows.

Why boundedness is important

In the theory of p-adic integration, does it matter that the distributions be bounded? To show that it does, consider a very simple case: let $\mu = \mu_{Haar}$ and let $f(x) = x$ for all $x \in \mathbb{Z}_p$. For each $N \in \mathbb{N}$,

$$\mathbb{Z}_p = \bigcup_{a=0}^{p^N-1} \Big(a + p^N \, \mathbb{Z}_p \Big),$$

so consider the sequence of partial sums

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

where $x_{a,N}$ is a representative of the ball $a + p^N \mathbb{Z}_p$. For the integral to exist (as defined above), the limit of this sum should not depend on the choice of $x_{a,N} \in a + p^N \mathbb{Z}_p$.

First suppose each $x_{a,N} = a$. This makes sense since $a \in a + p^N \mathbb{Z}_p$ for each $a \in \{0, 1, \ldots, p^N - 1\}$. Then

$$\sum_{a=0}^{p^N-1} x_{a,N} \frac{1}{p^N} = \frac{1}{p^N} \sum_{a=0}^{p^N-1} a = \frac{1}{p^N} \frac{(p^N - 1)(p^N)}{2} = \frac{p^N - 1}{2}.$$

In $\mathbb{Q}_p$,

$$\lim_{N \to \infty} \frac{p^N - 1}{2} = -\frac{1}{2}.$$

Now, for each N, choose exactly one $x_{a,N}$ to be $a + a_0 p^N$ for a fixed $a_0 \in \mathbb{Z}_p$, leaving all the others as a. Then

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

In $\mathbb{Q}_p$,

$$\lim_{N \to \infty} \left(\frac{p^N - 1}{2} + a_0 \right) = a_0 - \frac{1}{2}.$$

This limit is not independent of the choice of representative picked in each ball, so one cannot integrate $f(x) = x$ against μ (as defined here). While one

might be willing to accept a measure that does not allow certain functions to be integrable, $f(x) = x$ is not usually one of those functions. As was shown, this problem does not arise for a continuous function when using a bounded p-adic distribution. This objection could be dealt with by insisting on taking the representative $x_{a,N}$ from the set $\{0, 1, \ldots, p^N - 1\}$. For further information on this development, see Volkenborn integral in [3].

Theorems about Bernoulli numbers

In the introduction, several claims were made about Bernoulli numbers. The theory has been developed enough that these can be proved. The proofs rely mainly on one of the corollaries given above:

Corollary. For each $k \in \mathbb{N}$ and each $\alpha \in \mathbb{Z}_p^\times$ not a root of unity,

$$B_k = \frac{k}{1 - \alpha^k} \int_{\mathbb{Z}_p} x^{k-1} \, d\mu_{1,\alpha}(x).$$

An important observation is that the value of this expression does not depend on α in any way, nor does it depend on choice of k. Keeping this in mind, recall the theorems from the introduction.

Theorem. Let $k \in \mathbb{Z}^+$ and p be a prime. Then

1. If $a \in \mathbb{Z}$, then $a(a^k - 1)B_k \in \mathbb{Z}$.
2. (Sylvester-Lipschitz) If $a \in \mathbb{Z}$, then $a^k(a^k - 1)\dfrac{B_k}{k} \in \mathbb{Z}$.
3. (Adams) If $k \not\equiv 0 \bmod p - 1$, then $\dfrac{B_k}{k} \in \mathbb{Z}_p$.
4. (Kummer) For k_1 and k_2 even, if $k_1 \equiv k_2 \not\equiv 0 \bmod p - 1$, then

$$\frac{B_{k_1}}{k_1} \equiv \frac{B_{k_2}}{k_2} \bmod p.$$

5. (Clausen - von Staudt) For k even or $k = 1$,

$$B_k + \sum_{p-1|k} \frac{1}{p} \in \mathbb{Z}.$$

Proof of Claim (1). If $k = 1$, then one of a or $a - 1$ must be even. Thus

$$a(a-1)B_1 = a(a-1)(-\frac{1}{2}) \in \mathbb{Z}.$$

Suppose $k > 1$. Whenever $k > 1$ is odd, $B_k = 0$ and the result is trivial, so assume k is even. Consider the following lemma, given without proof (see [1]).

Lemma. If $A \in \mathbb{Z}_p$ for every prime p, then $A \in \mathbb{Z}$.

Given this lemma, it suffices to show that $a(a^k - 1)B_k \in \mathbb{Z}_p$ for every prime p. Fix a prime p. Then

$$a(a^k - 1)B_k = \frac{a(a^k-1)k}{1-\alpha^k} \int_{\mathbb{Z}_p} x^{k-1}\, d\mu_{1,\alpha}(x),$$

where $\alpha \in \mathbb{Z}_p^\times$ is not a root of unity. For any k and α,

$$\left| \int_{\mathbb{Z}_p} x^{k-1}\, d\mu_{1,\alpha}(x) \right|_p \;\leq\; \max_{x \in \mathbb{Z}_p} \left\{ |x^{k-1}|_p \right\} \cdot ||\mu|| \;\leq\; 1,$$

so it only remains to show

$$\frac{a(a^k-1)k}{1-\alpha^k} \in \mathbb{Z}_p. \tag{5}$$

But the choice of α is arbitrary, so it suffices to find *some* α such that (5) is satisfied.

If p does not divide a, then $a \in \mathbb{Z}_p^\times$, so choose $\alpha = a$. Then

$$\frac{a(a^k-1)k}{1-\alpha^k} = \frac{a(a^k-1)k}{1-a^k} = -ak,$$

which is in $\mathbb{Z}_p$, as required.

If p does divide a, then $|a|_p \leq \frac{1}{p}$, so $a \notin \mathbb{Z}_p^\times$. It follows that α cannot be a, so some other choice must be made. In this case, let $\alpha = 1 + p$. The proof that this choice of α works relys on the following lemma, again given without proof (see [1]).

Lemma. Suppose $m, n \in \mathbb{Z}$. If $p \neq 2$ and $x \in 1 + p\mathbb{Z}_p$, then $|x^m - x^n|_p = |x-1|_p|m-n|_p$. If $p = 2$ and $x \in 1+4\mathbb{Z}_2$, then $|x^m - x^n|_2 = |x-1|_2|m-n|_2$.

First suppose $p \neq 2$. Let $\alpha = 1 + p \in \mathbb{Z}_p^\times$. Then by the lemma,

$$|1 - \alpha^k|_p = |1 - \alpha|_p| - k|_p = \frac{1}{p}|k|_p.$$

Thus

$$\left|\frac{ak}{1-\alpha^k}\right|_p = \frac{|a|_p|k|_p}{\frac{1}{p}|k|_p} = p|a|_p.$$

But $a \in p\mathbb{Z}_p$, so $p|a|_p \leq 1$. It follows that

$$\frac{ak}{1-\alpha^k} \in \mathbb{Z}_p.$$

Since $a^k - 1 \in \mathbb{Z}_p$ (by the non-archimedean inequality), (5) follows.

Now suppose $p = 2$. Let $\alpha = 1 + 2 = 3$. When $p = 2$, the lemma only applies if $\alpha \equiv 1 \bmod 4\mathbb{Z}_2$, but $3 \not\equiv 1 \bmod 4\mathbb{Z}_2$. However $3^k = 9^{k/2}$, and 9 is congruent to 1 mod 4. Since k was assumed to be even,

$$|1 - \alpha^k|_p = |1 - 3^k|_2 = |1 - 9^{k/2}|_2 = |1 - 9|_2|k/2|_2 = \frac{1}{4}|k|_2.$$

Therefore

$$\left|\frac{ak}{1-\alpha^k}\right|_2 = \frac{|a|_2|k|_2}{\frac{1}{4}|k|_2} = 4|a|_2.$$

As before, $a^k - 1 \in \mathbb{Z}_2$ and $a \in 2\mathbb{Z}_2$, so

$$\left|\frac{ak(a^k-1)}{1-\alpha^k}\right|_p \leq 2,$$

but this bound is insufficient to show (5).

Recall the goal is to show

$$a(a^k-1)B_k = \frac{ak(a^k-1)}{1-\alpha^k}\int_{\mathbb{Z}_2} x^{k-1}\, d\mu_{1,\alpha}(x) \in \mathbb{Z}_2.$$

Given the bound on the first term in the product, it will suffice to show

$$\left|\int_{\mathbb{Z}_2} x^{k-1}\, d\mu_{1,\alpha}(x)\right|_2 \leq \frac{1}{2}.$$

For $x \in \mathbb{Z}_2$, $x^{k-1} \equiv x \bmod 2\mathbb{Z}_2$, so

$$\int_{\mathbb{Z}_2} x^{k-1}\, d\mu_{1,3}(x) \equiv \int_{\mathbb{Z}_2} x\, d\mu_{1,3}(x) \bmod 2\,\mathbb{Z}_2\,.$$

By (4), with $k=2$ and $\alpha = 3$,

$$\int_{\mathbb{Z}_2} x\, d\mu_{1,3}(x) = \frac{1}{2}\int_{\mathbb{Z}_2} d\mu_{2,3}(x) = \frac{1}{2}\mu_{2,3}(\mathbb{Z}_2).$$

To calculate this last expression, return to the definition of the Bernoulli distributions:

$$\mu_k\Big(a + p^n\,\mathbb{Z}_p\Big) = p^{n(k-1)}\mathbb{B}_k\left(\frac{\{a\}_n}{p^n}\right)$$

for $a \in \mathbb{Z}_p$. Thus

$$\mu_k(\mathbb{Z}_p) = \mathbb{B}_k(0) = B_k.$$

Therefore

$$\mu_{k,\alpha}(\mathbb{Z}_p) = \mu_k(\mathbb{Z}_p) - \alpha^k\mu_k(\mathbb{Z}_p) = (1-\alpha^k)B_k.$$

In this particular case, $k=2$ and $\alpha = 3$, so

$$\frac{1}{2}\mu_{2,3}(\mathbb{Z}_2) = \frac{1}{2}(1-3^2)B_2 = \Big(\frac{1}{2}\Big)\Big(-8\Big)\Big(\frac{1}{6}\Big) = -\frac{2}{3}.$$

However, $2\left(-\dfrac{1}{3}\right) \equiv 0 \bmod 2\mathbb{Z}_2$. Thus

$$\int_{\mathbb{Z}_2} x^{k-1}\, d\mu_{1,3}(x) \equiv 0 \bmod 2\mathbb{Z}_2,$$

so

$$\left|\int_{\mathbb{Z}_2} x^{k-1}\, d\mu_{1,3}(x)\right|_2 \leq \frac{1}{2},$$

as required. It follows that

$$\left|a(a^k-1)B_k\right|_2 \leq 2 \cdot \frac{1}{2} = 1,$$

which proves the first claim of the theorem.

Proof of Claim (2). By the lemma given in the proof of (1), it suffices to show that

$$a^k(a^k-1)\frac{B_k}{k} = \frac{a^k(a^k-1)}{1-\alpha^k}\int_{\mathbb{Z}_p} x^{k-1}\, d\mu_{1,\alpha}(x) \in \mathbb{Z}_p$$

for every prime p. As before,

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

so it only remains to show

$$\left|\frac{a^k(a^k-1)}{1-\alpha^k}\right|_p \leq 1. \tag{6}$$

If p does not divide a, then $|a|_p = 1$, so $a \in \mathbb{Z}_p^\times$. In this case, let $\alpha = a$. Then

$$\left|\frac{a^k(a^k-1)}{1-\alpha^k}\right|_p = \left|a^k\right|_p \left|\frac{a^k-1}{1-a^k}\right|_p \leq 1.$$

If p does divide a, then let $\alpha = 1+p$, as before. Since $p|a$, there exists some $e \in \mathbb{N}$ and a' such that $(p, a') = 1$ and $a = p^e a'$. Then

$$\left|a^k\right|_p = \left|(p^e a')^k\right|_p = \left|p^{ek}\,(a')^k\right|_p = \frac{1}{p^{ek}}.$$

Furthermore, since $\alpha \in \mathbb{Z}_p^\times$,

$$|1-\alpha^k|_p = |1-\alpha|_p|k|_p = |p|_p|k|_p = \frac{1}{p}|k|_p.$$

Observe that $k = p^f k'$ for some $k' \in \mathbb{Z}_p^\times$ and $f \in \mathbb{Z}^+$ (possibly zero). Thus

$$\left|\frac{a^k(a^k-1)}{1-\alpha^k}\right|_p = \frac{|a^k|_p|a^k-1|_p}{\frac{1}{p}|k|_p} \leq \frac{1}{p^{ek}}\frac{p}{|p^f|_p} = p^{1+f-ek}.$$

If $p^{1+f-ek} \leq 1$, then (6) will be verified.

By construction, $k = p^f k'$, so $k > f$. Because $e \geq 1$, it follows that $ek \geq k > f$. Therefore,

$$ek - 1 \geq k - 1 \geq f.$$

It follows that $1 + f - ek \leq 0$, so that $p^{1+f-ek} \leq 1$, as required.

Having verified (6) for all values of p, the second claim in the theorem is proven.

Proof of Claim (3). Begin by observing that $p > 2$. The multiplicative group of nonzero residue classes of $\mathbb{Z}$ mod p is cyclic of order $p-1$ (see [2]), so choose α in $\{2, 3, \ldots, p-1\}$ so that α^{p-1} is the lowest positive power of α which is congruent to 1 mod p. Since $k \not\equiv 0 \bmod p-1$, k is not a multiple of $p-1$. Thus $\alpha^k \not\equiv 1 \bmod p$. Therefore $\dfrac{1}{1-\alpha^k} \in \mathbb{Z}_p$. Thus

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

This proves the third claim.

Proof of Claim (4). To show $\dfrac{B_{k_1}}{k_1} \equiv \dfrac{B_{k_2}}{k_2} \bmod p$, it must be shown that

$$\frac{1}{1-\alpha^{k_1}} \int_{\mathbb{Z}_p} x^{k_1-1}\, d\mu_{1,\alpha}(x) \equiv \frac{1}{1-\alpha^{k_2}} \int_{\mathbb{Z}_p} x^{k_2-1}\, d\mu_{1,\alpha}(x) \bmod p.$$

As before, α may be chosen from $\{2, 3, \ldots, p-1\}$ so that α^{p-1} is the lowest positive power of α which is congruent to 1 mod p. It will be shown that

$$\frac{1}{1-\alpha^{k_1}} \equiv \frac{1}{1-\alpha^{k_2}} \bmod p$$

and

$$\int_{\mathbb{Z}_p} x^{k_1-1}\, d\mu_{1,\alpha}(x) \equiv \int_{\mathbb{Z}_p} x^{k_2-1}\, d\mu_{1,\alpha}(x) \bmod p.$$

From this it follows that the products are congruent mod p as well.

To show the first of these two, observe that $k_2 = k_1 + c(p-1)$ for some $c \in \mathbb{Z}^+$, by assumption. Thus

$$\alpha^{k_2} = \alpha^{k_1+c(p-1)} = \alpha^{k_1}(\alpha^{p-1})^c \equiv \alpha^{k_1} \bmod p.$$

Now observe

$$\frac{1}{1-\alpha^{k_1}} - \frac{1}{1-\alpha^{k_2}} = \frac{(1-\alpha^{k_2}) - (1-\alpha^{k_1})}{(1-\alpha^{k_1})(1-\alpha^{k_2})} = \frac{\alpha^{k_1} - \alpha^{k_2}}{(1-\alpha^{k_1})(1-\alpha^{k_2})}.$$

By choice of α, since $k_1, k_2 \not\equiv 0 \bmod (p-1)$, the same argument as above shows

$$\frac{1}{1-\alpha^{k_1}}, \frac{1}{1-\alpha^{k_2}} \in \mathbb{Z}_p^\times,$$

hence so is the product of the two. Thus

$$\left|\frac{1}{1-\alpha^{k_1}} - \frac{1}{1-\alpha^{k_2}}\right|_p = \left|\frac{\alpha^{k_1} - \alpha^{k_2}}{(1-\alpha^{k_1})(1-\alpha^{k_2})}\right|_p = \left|\alpha^{k_1} - \alpha^{k_2}\right|_p \leq \frac{1}{p}.$$

This gives the first congruence.

Now let $x \in \mathbb{Z}_p$ and $\{x\}_1$ be the element from $\{0, 1, \ldots, p-1\}$ that is congruent to x mod p. Then

$$x^{k_2} \equiv \{x\}_1^{k_2} = \{x\}_1^{k_1+c(p-1)} = \{x\}_1^{k_1}\{x\}_1^{c(p-1)} \equiv \{x\}_1^{k_1} \equiv x^{k_1} \bmod p.$$

From this it follows that $x^{k_1-1} \equiv x^{k_2-1} \bmod p$. Finally,

$$\left| \int_{\mathbb{Z}_p} x^{k_1-1}\, d\mu_{1,\alpha}(x) - \int_{\mathbb{Z}_p} x^{k_2-1}\, d\mu_{1,\alpha}(x) \right|_p$$

$$= \left| \int_{\mathbb{Z}_p} (x^{k_1-1} - x^{k_2-1})\, d\mu_{1,\alpha}(x) \right|_p \leq \sup_{x\in\mathbb{Z}_p} \left| x^{k_1-1} - x^{k_2-1} \right|_p \leq \frac{1}{p}.$$

This provides the second congruence, hence completes the proof of the fourth claim.

Proof of Claim (5). This claim, which is attributed to Clausen and von Staudt, states: For k even or $k = 1$,

$$B_k + \sum_{p-1|k} \frac{1}{p} \in \mathbb{Z}.$$

For each k it will be shown that

$$B_k + \sum_{p-1|k} \frac{1}{p} \in \mathbb{Z}_q$$

for every prime q. This will give the required result, by the lemma above.

First consider $k = 1$. The prime $p = 2$ is the only prime such that $(p-1)|1$, so the sum is simply

$$B_1 + \frac{1}{2} = -\frac{1}{2} + \frac{1}{2} = 0.$$

Clearly this is in $\mathbb{Z}_q$ for every prime q.

Now let k be an even integer and fix a prime q. If $q-1$ does not divide k, then the sum will be over primes not q; but for any $p \neq q$, $\frac{1}{p} \in \mathbb{Z}_q$. Thus

$$\sum_{p-1|k} \frac{1}{p} \in \mathbb{Z}_q.$$

Furthermore, if $q-1$ does not divide k, then $k \not\equiv 0 \bmod q-1$, so by the theorem of Adams (see above) $\dfrac{B_k}{k} \in \mathbb{Z}_q$. Since $k \in \mathbb{Z}$, it follows that

$$B_k = \frac{B_k}{k} \times k \in \mathbb{Z}_q,$$

hence

$$B_k + \sum_{p-1|k} \frac{1}{p} \in \mathbb{Z}_q.$$

Now suppose that $q-1$ does divide k. Then

$$B_k + \sum_{p-1|k} \frac{1}{p} = B_k + \frac{1}{q} + \sum_{\substack{p-1|k \\ p \neq q}} \frac{1}{p}.$$

As before,

$$\sum_{\substack{p-1|k \\ p \neq q}} \frac{1}{p} \in \mathbb{Z}_q,$$

so it only remains to show that

$$B_k + \frac{1}{q} \in \mathbb{Z}_q.$$

It will suffice to show

$$qB_k \equiv -1 \bmod q\mathbb{Z}_q,$$

for then $qB_k = -1 + qA$ for some $A \in \mathbb{Z}_q$ and

$$B_k + \frac{1}{q} = \frac{qB_k + 1}{q} = \frac{-1 + qA + 1}{q} = A \in \mathbb{Z}_q.$$

The proof of this congruence, which is called the Clausen - von Staudt congruence, is given below. Having shown

$$B_k + \frac{1}{q} \in \mathbb{Z}_q$$

if $q-1|k$, it follows that

$$B_k + \sum_{p-1|k} \frac{1}{p} \in \mathbb{Z}_q$$

for every prime q. Thus

$$B_k + \sum_{p-1|k} \frac{1}{p} \in \mathbb{Z},$$

as required. $\diamond$

This paper concludes by proving the congruence which is at the heart of the theorem of Clausen and von Staudt.

Lemma. (The Clausen - von Staudt congruence.) If $p-1|k$ for some prime $p \neq 2$, or $p = 2$ and k is even or $k = 1$, then

$$pB_k \equiv -1 \bmod p\mathbb{Z}_p, \tag{7}$$

Proof. Begin by recalling that

$$pB_k = \frac{kp}{1-\alpha^k} \int_{\mathbb{Z}_p} x^{k-1}\, d\mu_{1,\alpha}(x),$$

where α is any element of $\mathbb{Z}_p^\times$ other than a root of unity. The proof is in two parts; when $p = 2$ and when $p \neq 2$. First suppose $p \neq 2$. The choice of α is arbitrary, so let $\alpha = \dfrac{1}{1+p}$. Then

$$1 - \alpha^k = 1 - (1+p)^{-k} \equiv kp \bmod p^{\mathrm{ord}_p(k)+2},$$

whence

$$\frac{kp}{1-\alpha^k} \equiv 1 \bmod p.$$

Thus

$$pB_k \equiv \int_{\mathbb{Z}_p} x^{k-1}\, d\mu_{1,\alpha}(x) \bmod p.$$

Since $\mathbb{Z}_p = \mathbb{Z}_p^\times \cup p\mathbb{Z}_p$ is a disjoint union, and $k > 1$,

$$\int_{\mathbb{Z}_p} x^{k-1}\, d\mu_{1,\alpha}(x) = \int_{\mathbb{Z}_p^\times} x^{k-1}\, d\mu_{1,\alpha}(x) + \int_{p\mathbb{Z}_p} x^{k-1}\, d\mu_{1,\alpha}(x)$$

$$\equiv \int_{\mathbb{Z}_p^\times} x^{k-1}\, d\mu_{1,\alpha}(x) \bmod p,$$

By assumption $p-1|k$, so $x^k \equiv 1 \bmod p$ (as has been seen before). Thus

$$x^{k-1} \equiv x^{-1} \bmod p$$

for all $x \in \mathbb{Z}_p^\times$. Therefore,

$$\int_{\mathbb{Z}_p^\times} x^{k-1}\, d\mu_{1,\alpha}(x) \equiv \int_{\mathbb{Z}_p^\times} x^{-1}\, d\mu_{1,\alpha}(x) \bmod p.$$

Define $g(x) = \{x\}_1^{-1}$ for $x \in \mathbb{Z}_p^\times$. Then $x^{-1} \equiv g(x) \bmod p$ for all $x \in \mathbb{Z}_p^\times$. Thus

$$\int_{\mathbb{Z}_p^\times} x^{-1}\, d\mu_{1,\alpha}(x) \equiv \int_{\mathbb{Z}_p^\times} \{x\}_1^{-1}\, d\mu_{1,\alpha}(x) \bmod p.$$

The function g is a step function, and this last integral can be evaluated directly:

$$\begin{aligned}
\int_{\mathbb{Z}_p^\times} \frac{1}{\{x\}_1}\, d\mu_{1,\alpha}(x) &= \sum_{a=1}^{p-1} \frac{1}{a} \mu_{1,\alpha}(a + p\mathbb{Z}_p) \\
&= \sum_{a=1}^{p-1} \frac{1}{a} \left(\mu_1(a + p\mathbb{Z}_p) - \alpha\mu_1(\alpha^{-1}a + p\mathbb{Z}_p)\right) \\
&= \sum_{a=1}^{p-1} \frac{1}{a} \left(\left(\frac{a}{p} - \frac{1}{2}\right) - \alpha\left(\frac{\{\alpha^{-1}a\}_1}{p} - \frac{1}{2}\right)\right).
\end{aligned}$$

Recall that α was chosen to be $\dfrac{1}{1+p}$. Thus

$$\begin{aligned}
\int_{\mathbb{Z}_p^\times} \frac{1}{\{x\}_1}\, d\mu_{1,\alpha}(x) &= \sum_{a=1}^{p-1} \frac{1}{a}\left(\frac{a}{p} - \frac{1}{2} - \frac{1}{1+p}\Big(\frac{\{(1+p)a\}_1}{p} - \frac{1}{2}\Big)\right) \\
&= \sum_{a=1}^{p-1} \frac{1}{a}\left(\frac{a}{p} - \frac{1}{2} - \frac{a}{(1+p)p} + \frac{1}{2(1+p)}\right) \\
&= \sum_{a=1}^{p-1} \frac{2a(1+p) - p(1+p) - 2a + p}{2ap(1+p)} \\
&= \sum_{a=1}^{p-1} \frac{2a-p}{2a(1+p)}.
\end{aligned}$$

Now observe

$$\begin{aligned}
\sum_{a=1}^{p-1} \frac{2a-p}{2a(1+p)} &\equiv \sum_{a=1}^{p-1} \frac{2a}{2a(1+p)} \bmod p\,\mathbb{Z}_p \\
&= \sum_{a=1}^{p-1} \frac{1}{1+p} \\
&= \frac{p-1}{1+p} \\
&\equiv \frac{p^2+p-1}{1+p} \bmod p\,\mathbb{Z}_p \\
&\equiv p-1 \bmod p\,\mathbb{Z}_p
\end{aligned}$$

Therefore

$$pB_k \equiv p-1 \equiv -1 \bmod p\mathbb{Z}_p,$$

as required. The congruence has now been proven for all $p \neq 2$.

Now suppose $p = 2$. As before,

$$2B_k = \frac{2k}{1-\alpha^k} \int_{\mathbb{Z}_2} x^{k-1}\, d\mu_{1,\alpha}(x).$$

Choose $\alpha = \frac{1}{5} \in \mathbb{Z}_2^\times$.

Claim 1: $\left|\dfrac{2k}{1-\alpha^k}\right|_2 = 2.$

Notice that $\dfrac{1}{5} + 4\left(\dfrac{1}{5}\right) = 1$. Thus $\dfrac{1}{5} \equiv 1 \bmod 4\mathbb{Z}_2$, so, by the lemma on page 22,

$$\left|1 - \frac{1}{5}^k\right|_2 = \left|1 - \frac{1}{5}\right|_2 |k|_2 = \left|\frac{4}{5}\right|_2 |k|_2 = \frac{|k|_2}{4}.$$

Therefore,

$$\left|\frac{2k}{1-\alpha^k}\right|_2 = \frac{|k|_2/2}{|k|_2/4} = 2.$$

Claim 2: $\left|\displaystyle\int_{\mathbb{Z}_2} x^{k-1}\, d\mu_{1,\alpha}(x)\right|_2 = \frac{1}{2}.$

By the same argument used for $p \neq 2$,

$$\int_{\mathbb{Z}_2} x^{k-1}\, d\mu_{1,\alpha}(x) \equiv \int_{\mathbb{Z}_2^\times} \frac{1}{x}\, d\mu_{1,\alpha}(x) \bmod 2.$$

Define $g(x) = \{x\}_2^{-1}$ for $x \in \mathbb{Z}_p^\times$, where $\{x\}_2$ is the element in $\{0,1,2,3\}$ congruent to x mod 4. Then

$$\int_{\mathbb{Z}_2^\times} \frac{1}{x}\, d\mu_{1,\alpha}(x) \equiv \int_{\mathbb{Z}_2^\times} g(x)\, d\mu_{1,\alpha}(x) \bmod 4.$$

This integral can be evaluated directly:

$$\begin{aligned}\int_{\mathbb{Z}_2^\times} \frac{1}{\{x\}_2}\, d\mu_{1,\alpha}(x) &= \sum_{a=1}^{3} \frac{1}{a}\mu_{1,\alpha}(a+4\mathbb{Z}_2) \\ &= \sum_{a=1}^{3} \frac{1}{a}\left(\mu_1(a+4\mathbb{Z}_2) - \frac{1}{5}\mu_1(5a+4\mathbb{Z}_2)\right) \\ &= \sum_{a=1}^{3} \frac{1}{a}\left(\left(\frac{a}{4}-\frac{1}{2}\right) - \frac{1}{5}\left(\frac{\{5a\}_2}{4}-\frac{1}{2}\right)\right).\end{aligned}$$

Noting that $\{5\}_2 = 1$, $\{10\}_2 = 2$, and $\{15\}_2 = 3$, this can be simplified:

$$\sum_{a=1}^{3} \frac{1}{a}\left(\left(\frac{a}{4}-\frac{1}{2}\right) - \frac{1}{5}\left(\frac{\{5a\}_2}{4}-\frac{1}{2}\right)\right)$$

$$= \left(-\frac{1}{4}+\frac{1}{20}\right) + \frac{1}{3}\left(\frac{1}{4}-\frac{1}{20}\right) = -\frac{2}{15}.$$

Observe that $-\frac{2}{15} + 4\left(\frac{8}{15}\right) = 2$. Thus

$$\int_{\mathbb{Z}_2^\times} \frac{1}{x}\, d\mu_{1,\alpha}(x) \equiv 2 \bmod 4\,\mathbb{Z}_2\,.$$

This term is congruent to 0 mod 2, but not 0 mod 4, so it follows that

$$\left|\int_{\mathbb{Z}_2^\times} \frac{1}{x}\, d\mu_{1,\alpha}(x)\right|_2 = \frac{1}{2}.$$

It has been shown that

$$\int_{\mathbb{Z}_2} x^{k-1}\, d\mu_{1,\alpha}(x) = \int_{\mathbb{Z}_2^\times} x^{-1}\, d\mu_{1,\alpha}(x) + 2C,$$

for some term $C \in \mathbb{Z}_p$. Therefore,

$$\left| \int_{\mathbb{Z}_2} x^{k-1} \, d\mu_{1,\alpha}(x) \right|_2 = \max \left\{ \left| \int_{\mathbb{Z}_2^\times} x^{-1} \, d\mu_{1,\alpha}(x) \right|_2 , |2C|_2 \right\} = \frac{1}{2}.$$

This proves the second claim.

Finally,

$$\left| 2B_k \right|_2 = \left| \frac{2k}{1-\alpha^k} \right|_2 \left| \int_{\mathbb{Z}_2} x^{k-1} \, d\mu_{1,\alpha}(x) \right|_2 = 2 \times \frac{1}{2} = 1.$$

Therefore $2B_k \in \mathbb{Z}_2^\times$, hence (since $p = 2$),

$$2B_k \equiv 1 \equiv -1 \bmod 2\,\mathbb{Z}_2 \, .$$

This concludes the proof. $\diamond$

References

[1] K. Conrad, *Introduction to local fields*, in The Lectures of Keith Conrad (as recorded by A. Bowers), Fall Semester 2004.

[2] N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Springer-Verlag New York, second ed., 1984.

[3] A. Robert, *A Course in p-adic Analysis*, Springer-Verlag, 2000.