Combinatorial Congruences and $\psi$-Operators

Daqing Wan*
dwan@math.uci.edu
Department of Mathematics
University of California, Irvine
CA 92697-3875

March 29, 2022

Abstract

The $\psi$-operator for $(\phi, \Gamma)$-modules plays an important role in the study of Iwasawa theory via Fontaine’s big rings. In this note, we prove several sharp estimates for the $\psi$-operator in the cyclotomic case. These estimates immediately imply a number of sharp $p$-adic combinatorial congruences, one of which extends the classical congruences of Fleck (1913) and Weisman (1977).

1 Combinatorial Congruences

Let $p$ be a prime, $n \in \mathbb{Z}_{>0}$. Throughout this paper, let $[x]$ denote the integer part of $x$ if $x \geq 0$ and $[x] = 0$ if $x < 0$. In the author’s course lectures [4] on Fontaine’s theory and $p$-adic L-functions given at UC Irvine (spring 2005) and at the Morningside Center of Mathematics (summer 2005), the following two congruences were discovered.

**Theorem 1.1.** For integers $r \in \mathbb{Z}$, $j \geq 0$, we have

$$
\sum_{k \equiv r (\text{mod} \ p)} (-1)^{n-k} \binom{n}{k} \binom{k-r}{p-j} \equiv 0 \pmod{p^{\left\lfloor \frac{p-1}{p^2} \right\rfloor}}.
$$

We shall see that the theorem comes from a simple estimate of $\psi(\pi^n)$ for the cyclotomic $\varphi$-module.

*Partially supported by NSF. The author thanks Z.W. Sun for helpful discussions on combinatorial congruences.*
Theorem 1.2. For integer $j \geq 0$, we have

$$\sum_{i_0 + \cdots + i_{p-1} = n \atop i_1 + 2i_2 + \cdots \equiv r \pmod{p}} \left( \begin{array}{c} n \\ i_0i_1 \cdots i_{p-1} \end{array} \right) \left( \frac{i_1 + 2i_2 + \cdots - r}{p} \right) \equiv 0 \pmod{\left\lfloor \frac{2(p-1)-1}{p-1} \right\rfloor}.$$  

As we shall see, this theorem comes from a simple estimate of $\psi(\pi^{-n})$ for the cyclotomic $\varphi$-module. Note that when $p = 2$, Theorem 1.2 is equivalent to Theorem 1.1.

The above two congruences can be extended from $p$ to $q = p^a$, where $a$ is a positive integer. To do so, it suffices to estimate the $a$-th iterate $\psi^a(\pi^n)$. This can be done by induction. The estimate of $\psi^a(\pi^n)$ for $n > 0$ leads to

Theorem 1.3. For integers $r \in \mathbb{Z}$, $j \geq 0$ and $a > 0$, we have

$$\sum_{k \equiv r \pmod{p^a}} (-1)^{n-k} \binom{n}{k} \left( \frac{k-r}{p^a} \right) \equiv 0 \pmod{\left\lfloor \frac{a(p-1)-1}{p-1} \right\rfloor}.$$  

The estimate of $\psi^a(\pi^n)$ for $n < 0$ leads to

Theorem 1.4. Let

$$S_j(n, r, p^a) = \sum_{i_0 + \cdots + i_{p^a-1} = n \atop i_1 + 2i_2 + \cdots \equiv r \pmod{p^a}} \left( \begin{array}{c} n \\ i_0 \cdots i_{p^a-1} \end{array} \right) \left( \frac{i_1 + 2i_2 + \cdots - r}{p^a} \right) \left( \frac{(i_1 + 2i_2 + \cdots - r)/p^a}{j} \right).$$

Then for integer $j \geq 0$, we have

$$S_j(n, r, p^a) \equiv 0 \pmod{\left\lfloor \frac{(an-a+1)(p-1)-j(ap-a+1)-1}{p-1} \right\rfloor}.$$  

As Z.W. Sun informed me, the special case $j = 0$ of Theorem 1.1.1 was first proved by Fleck [1] in 1913, and the special case of Theorem 1.1.3 for $j = 0$ was first proved by Weisman [5] in 1977. A different extension of Theorem 1.1.1 and Weisman’s congruence has been obtained by Z.W. Sun [2] using different combinatorial arguments. Motivated by applications in algebraic topology, Sun-Davis [3] proved yet another extension:

$$\sum_{k \equiv r \pmod{p^a}} (-1)^{n-k} \binom{n}{k} \left( \frac{k-r}{p^a} \right) \equiv 0 \pmod{\operatorname{ord}_p((n/p^a-1)!)-j-\operatorname{ord}_p(j!)}. $$
2 The operator \( \psi \)

Let \( p \) be a fixed prime. Let \( \pi \) be a formal variable. Let
\[
A^+ = \mathbb{Z}_p[[\pi]]
\]
be the formal power series ring over the ring of \( p \)-adic integers. Let \( A \) be the \( p \)-adic completion of \( A^+[\frac{1}{\pi}] \), and let \( B = A[\frac{1}{p}] \) be the fraction field of \( A \). The rings \( A^+ \), \( A \) and \( B \) correspond to \( A^+_Q_p \), \( A_Q_p \) and \( B_Q_p \) in Fontaine's theory.

We shall not discuss the Galois action on \( A \), which is not needed for our present purpose. The Frobenius map \( \varphi \) acts on the above rings by
\[
\varphi(\pi) = (1 + \pi)^p - 1.
\]

If we let \([\varepsilon] = 1 + \pi\), then \( \varphi([\varepsilon]) = [\varepsilon]^p \). The map \( \varphi \) is injective of degree \( p \).

Proposition 2.1. \( \{1, \pi, \cdots, \pi^{p-1}\} \) (and \( \{1, [\varepsilon], \cdots, [\varepsilon]^{p-1}\} \)) is a basis of \( A \) over the subring \( \varphi(A) \).

Definition 2.2. The operator \( \psi : A \to A \) is defined by
\[
\psi(x) = \psi\left( \sum_{i=0}^{p-1} [\varepsilon]^i \varphi(x_i) \right) = x_0 = \frac{1}{p} \varphi^{-1}(\text{Tr}_{A/\varphi(A)}(x)),
\]
where \( x : A \to A \) denotes the multiplication by \( x \) as \( \varphi(A) \)-linear map.

Example 2.3.
\[
\psi([\varepsilon]^n) = \begin{cases} [\varepsilon]^{n/p}, & \text{if } p \mid n; \\ 0, & \text{if } p \nmid n. \end{cases}
\]

It is clear that \( \psi \) is \( \varphi^{-1} \)-linear:
\[
\psi(\varphi(a)x) = a\psi(x) \quad \forall \ a, x \in A.
\]

Example 2.4. Let \( a \) be a positive integer relatively prime to \( p \). Then
\[
\psi\left(\frac{1}{(1 + \pi)^a - 1}\right) = \frac{1}{(1 + \pi)^a - 1}.
\]

In fact,
\[
\psi\left(\frac{1}{[\varepsilon]^a - 1}\right) = \psi\left(\frac{1}{[\varepsilon]^{ap} - 1} \cdot \frac{[\varepsilon]^{ap} - 1}{[\varepsilon] - 1}\right)
\]
\[
= \frac{1}{[\varepsilon]^{a-1}} \psi\left(1 + [\varepsilon]^a + \cdots + [\varepsilon]^{(p-1)a}\right)
\]
\[
= \frac{1}{[\varepsilon]^{a-1}} = \frac{1}{(1 + \pi)^{a-1}}.
\]
By $p$-adic continuity, the above example holds for any $p$-adic unit $a \in \mathbb{Z}_p^*$. In the general theory of $(\varphi, \Gamma)$-modules, it is important to find the fix points of $\psi$ for applications to $p$-adic $L$-functions and Iwasawa theory. In the simplest cyclotomic case, we have the following description for the fixed points (see [4]).

**Proposition 2.5.**

$$A^{\psi=1} = \frac{1}{\pi} \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \left\{ \sum_{k=0}^{\infty} \varphi^k(x) \left| x \in \bigoplus_{i=1}^{p-1} [\varepsilon]^i \varphi(\pi^i + \pi^n \mathbb{Z}_p[[\pi]]), \sum_{i=1}^{p-1} a_i = 0 \right\},$$

where $a_i \in \mathbb{Z}_p$.

For example, if $a$ is a positive integer relatively prime to $p$, then the element

$$\frac{a}{(1 + \pi)^a - 1} - \frac{1}{\pi} \in (A^+)^{\psi=1}$$

gives the cyclotomic units and the Euler system. This element is the Amice transform of a $p$-adic measure which produces the $p$-adic zeta function of $\mathbb{Q}$. This type of connections is conjectured to be a general phenomenon for $(\varphi, \Gamma)$-modules coming from global $p$-adic Galois representations.

### 3 Sharp estimates for $\psi$

The ring $A$ is a topological ring with respect to the $(p, \pi)$-topology. A basis of neighborhoods of 0 is the sets $p^k A + \pi^n A^+$, where $k \in \mathbb{Z}$ and $n \in \mathbb{N}$. The operator $\psi$ is uniformly continuous. This continuity will give rise to combinatorial congruences.

For $s \in A^+$, one checks that

$$\psi((\pi^p)^s) = \psi( ([\varepsilon] - 1)^p s)$$
$$= \psi( ([\varepsilon]^p - 1)s + pss_1)$$
$$= \pi \psi(s) + p \psi(s_1) \in (p, \pi) \psi(sA^+).$$

In particular,

$$\psi(\pi^p A^+) \subset (p, \pi) A^+. $$

Thus, by iteration, we get
Proposition 3.1 (Weak Estimate). Let $n \geq 0$. Then

$$
\psi(\pi^n A^+) \subset (p, \pi)^{[n/p]} A^+ = \sum_{j=0}^{[n/p]} \pi^j p^{[n/p] - j} A^+.
$$

Since the exponent $[(n - jp)/p]$ is decreasing in $j$, this proposition implies that for $x \in \pi^n A^+$, we have

$$
\psi(x) = \sum_{j=0}^{\infty} a_j \pi^j, \quad a_j \in \mathbb{Z}_p, \quad \text{ord}_p(a_j) \geq [(n - jp)/p].
$$

This already gives a non-trivial combinatorial congruence. Let $r$ be an integer. Let us calculate $\psi(\pi^n [\varepsilon]^{-r})$ in a different way.

Lemma 3.2.

$$
\psi(\pi^n [\varepsilon]^{-r}) = \sum_{j \geq 0} \pi^j \sum_{k \equiv r \pmod{p}} (-1)^{n-k} \binom{n}{k} \left(\frac{(k-r)/p}{j}\right).
$$

Proof. Since $\pi = [\varepsilon] - 1$ and $[\varepsilon] = 1 + \pi$, we have

$$
\psi(\pi^n [\varepsilon]^{-r}) = \psi((\varepsilon - 1)\pi^n [\varepsilon]^{-r})
$$

$$
= \psi \left( \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} \varepsilon^{k-r} \right)
$$

$$
= \sum_{k \equiv r \pmod{p}} (-1)^{n-k} \binom{n}{k} \varepsilon^{(k-r)/p} \pi^j
$$

$$
= \sum_{k \equiv r \pmod{p}} (-1)^{n-k} \binom{n}{k} \sum_{j \geq 0} \left(\frac{(k-r)/p}{j}\right) \pi^j
$$

$$
= \sum_{j \geq 0} \pi^j \sum_{k \equiv r \pmod{p}} (-1)^{n-k} \binom{n}{k} \left(\frac{(k-r)/p}{j}\right).
$$

Comparing the coefficients of $\pi^j$ in this equation and the weak estimate, we get

Corollary 3.3 (Weak Congruence). Let $n \geq 0$. We have

$$
\sum_{k \equiv r \pmod{p}} (-1)^{n-k} \binom{n}{k} \left(\frac{(k-r)/p}{j}\right) \equiv 0 \pmod{\lfloor (n-jp)/p \rfloor}.
$$
The above simple estimate is crude and certainly not optimal since we ignored a factor of $\pi$. We now improve on it.

**Theorem 3.4 (Sharp Estimate I).** For $n \geq 0$, we have

$$\psi(\pi^n A^+) \subseteq \sum_{j=0}^{[n/p]} \pi^j p^\left[\frac{n-1-jp}{p-1}\right] A^+.$$

**Proof.** We prove the theorem by induction. The theorem is trivial if $n \leq p - 1$. Write

$$\varphi(\pi) = (1 + \pi)^p - 1 = \pi^p - p\pi s_1, \ s_1 \in A^+.$$

Then,

$$\psi(\pi^p s) = \psi((\varphi(\pi) + p\pi s_1) s) = \pi\psi(s) + p\psi(\pi s_1 s).$$

This proves that the theorem is true for $n = p$. Let $n > p$. Assume the theorem holds for $\leq n - 1$. It follows that

$$\psi(\pi^n A^+) = \psi(\pi^p \pi^{n-p} A^+) \subseteq \pi\psi(\pi^{n-p} A^+) + p\psi(\pi^{n+1-p} A^+).$$

By the induction hypothesis, the right side is contained in

$$\pi \sum_{j=0}^{[(n-p)/p]} \pi^j p^\left[\frac{n-p-1-jp}{p-1}\right] A^+ + p \sum_{j=0}^{[(n+1-p)/p]} \pi^j p^\left[\frac{2-n-1-jp}{p-1}\right] A^+$$

$$= \sum_{j=1}^{[n/p]} \pi^j p^\left[\frac{n-1-jp}{p-1}\right] A^+ + \sum_{j=0}^{[(n+1-p)/p]} \pi^j p^\left[\frac{2-n-1-jp}{p-1}\right] A^+. $$

The function $\left[(n - 1 - jp)/(p - 1)\right]$ is decreasing in $j$ and vanishes for $j \geq [n/p]$. Comparing the coefficients of $\pi^j$ in the lemma and the above sharp estimate, we deduce

**Corollary 3.5 (Sharp Congruence I).** Let $r \in \mathbb{Z}$.

$$\sum_{k \equiv r \pmod{p}} (-1)^{n-k}\binom{n}{k}\binom{(k-r)/p}{j} \equiv 0 \pmod{p^\left[\frac{n-1-jp}{p-1}\right]},$$

where $j \geq 0$ is a non-negative integer.
Theorem 3.6 (Sharp Estimate II). For $n > 0$, we have

$$\psi \left( \frac{1}{\pi^n} A^+ \right) \subseteq \sum_{j=0}^\left\lfloor n(p-1)/p \right\rfloor \frac{1}{\pi^{n-j} p^\left\lfloor n(p-1) \cdot (p-1) \right\rfloor} A^+. $$

Proof. Note that

$$\varphi(\pi)/\pi = \pi^{p-1} + \left( \frac{p}{1} \right) \pi^{p-2} + \cdots + \left( \frac{p}{p-1} \right) \in (\pi^{p-1}, p),$$

so $\left( \frac{\varphi(\pi)}{\pi} \right)^n \in (\pi^{p-1}, p^n)$. Then

$$\psi \left( \frac{1}{\pi^n} A^+ \right) = \psi \left( \frac{1}{\varphi(\pi)} \left( \frac{\varphi(\pi)}{\pi} \right)^n A^+ \right) = \frac{1}{\pi^n} \psi \left( \left( \frac{\varphi(\pi)}{\pi} \right)^n A^+ \right) \subseteq \frac{1}{\pi^n} \sum_{i=0}^n p^{n-i} \psi (\pi^i A^+).$$

By Sharp Estimate I, we have

$$\psi (\pi^i A^+) \subseteq \sum_{j=0}^\left\lfloor i(p-1)/p \right\rfloor \frac{1}{\pi^j p^\left\lfloor (p-1) \cdot (p-1) \right\rfloor} A^+. $$

Then,

$$\psi \left( \frac{1}{\pi^n} A^+ \right) \subseteq \sum_{j=0}^\left\lfloor n(p-1)/p \right\rfloor \frac{1}{\pi^{n-j}} \sum_{\left\lfloor j(p-1) \right\rfloor \leq i \leq n} p^{n-i+\left\lfloor (p-1) \cdot (p-1) \right\rfloor} A^+ \subseteq \sum_{j=0}^\left\lfloor n(p-1)/p \right\rfloor \frac{1}{\pi^{n-j} p^\left\lfloor n(p-1) \cdot (p-1) \right\rfloor} A^+. $$

\[\square\]

Corollary 3.7 (Sharp Congruence II). Let

$$S_j(n, r, p) = \sum_{i_0 + \cdots + i_{p-1} = n \atop i_1 + 2i_2 + \cdots \equiv r \pmod{p}} \binom{n}{i_0 \cdots i_{p-1}} \binom{n}{i_1 + 2i_2 + \cdots - r}/j.$$  

Then integer $j \geq 0$, we have

$$S_j(n, r, p) \equiv 0 \pmod{\left\lfloor n(p-1) \cdot (p-1) \right\rfloor}.$$
Proof.

\[
\psi \left( \frac{1}{\pi^n} \varepsilon^{-r} \right) = \frac{1}{\pi^n} \psi \left( \left( \frac{[\varepsilon]^p - 1}{[\varepsilon] - 1} \right)^n \varepsilon^{-r} \right) = \frac{1}{\pi^n} \psi((1 + \varepsilon + \cdots + [\varepsilon]^{p-1})^n \cdot [\varepsilon]^{-r}) = \frac{1}{\pi^n} \sum_{i_0 + \cdots + i_{p-1} = n} \frac{[\varepsilon]^{(i_1 + 2i_2 + \cdots - r)/p}}{i_0 \cdots i_{p-1}} \left( \begin{array}{c} n \\ i_0 \cdots i_{p-1} \end{array} \right)
\]

The function \([(n(p - 1) - jp - 1)/(p - 1)]\) is decreasing in \(j\) and vanishes for \(j \geq [n(p - 1)/p]\). Comparing the coefficients of \(\frac{1}{\pi^n}\), the congruence follows.

\[\square\]

4 Sharp estimates for \(\psi^a\)

Let \(a\) be a positive integer. In this section, we extend the sharp estimates for \(\psi\) to \(\psi^a\).

**Theorem 4.1 (Sharp Estimate I).** For \(n \geq 0\), we have

\[
\psi^a(\pi^n A^+) \subseteq \sum_{j=0}^{[n/p^a]} \pi^{j/p^a} \left( \frac{n-p^{a-1}-p^a}{p^{a-1}(p-1)} \right) A^+.
\]

**Proof.** We prove the theorem by induction on \(a\). The theorem is true if \(a = 1\). Assume now \(a \geq 2\) and assume that the theorem holds for \(a - 1\).
Then,

\[
\psi^a(n^A) = \psi(\psi^{a-1}n^A) \\
\subseteq \psi(\sum_{i=0}^{[n/p^{a-1}]} \pi^i p^{[n^{a-2} - (i+1)p^{a-1}]} A^+) \\
\subseteq \sum_{i=0}^{[n/p^{a-1}]} \sum_{j=0}^{[n/p^{a-2}]} \pi^j A^{[n/p^{a-1}]} + [i-1-p] A^+ \\
\subseteq \sum_{j=0}^{[n/p^{a}]} \pi^j \sum_{pj \leq i \leq [n/p^{a-1}]} p^{[n^{a-3} - (i-1)p^{a-1}]} + [i-1-p] A^+.
\]

The exponent of \( p \) for a fixed \( j \) is decreasing in \( i \) and hence the minimum exponent of \( p \) is attained when \( i = [n/p^{a-1}] \). The minimum exponent is computed to be

\[
\frac{n - p^{a-2} - [n/p^{a-1}]p^{a-1}}{p^{a-1} - p^{a-2}} + \frac{[n/p^{a-1}] - 1 - j p^a}{p - 1} = \frac{n - p^{a-1} - j p^a}{p^{a-1}(p - 1)}.
\]

The proof of the lemma gives more general

**Lemma 4.2.**

\[
\psi^a(n^n [\varepsilon]^{-r}) = \sum_{j \geq 0} \pi^j \sum_{k \equiv r \mod p^a} (-1)^{n-k} \binom{n}{k} \left( (k - r)/p^a \right).
\]

Comparing the coefficients of \( \pi^j \) in the lemma and the sharp estimate for \( \psi^a \), we get

**Corollary 4.3 (Sharp Congruence I).** Let \( r \in \mathbb{Z} \). Then

\[
\sum_{k \equiv r \mod p^a} (-1)^{n-k} \binom{n}{k} \left( (k - r)/p^a \right) \equiv 0 \mod \left( \frac{n - p^{a-1} - j p^a}{p^{a-1}(p - 1)} \right),
\]

where \( j \geq 0 \) is a non-negative integer.

**Theorem 4.4 (Sharp Estimate II).** For \( n > 0 \) and \( a > 0 \), we have

\[
\psi^a \left( \frac{1}{\pi^n A^+} \right) \subseteq \sum_{j=0}^{[\binom{an-a+1}{ap-a+1}]_p} \frac{1}{\pi^{n-j} p^{[\binom{an-a+1}{ap-a+1}]_p} A^+}.
\]
Proof. The theorem is true for \( a = 1 \). Assume now that \( a > 1 \) and assume that the theorem is true for \( a - 1 \). Then

\[
\psi^a \left( \frac{1}{\pi^n} A^+ \right) = \psi \left( \psi^{a-1} \left( \frac{1}{\pi^n} A^+ \right) \right)
\]

\[
\subseteq \psi \left( \sum_{j=0}^{\frac{(a-1)n-a+2}{(a-1)p-a+2}} \frac{1}{\pi^{n-j}} \left[ \frac{(a-1)n-a+2}{(a-1)p-a+2} \right]^{(p-1)\left(\frac{1}{p-1}\right)-j((a-1)p-a+2)-1} A^+ \right)
\]

\[
\subseteq \sum_{j} \sum_{i} \frac{1}{\pi^{n-j-1}} \left[ \frac{(a-1)n-a+2}{(a-1)p-a+2} \right]^{(p-1)\left(\frac{1}{p-1}\right)-j((a-1)p-a+2)-1} A^+,
\]

where the indices \( i \) and \( j \) satisfy

\[
0 \leq j \leq \left\lfloor \frac{(a-1)n-a+2}{(a-1)p-a+2} \right\rfloor, \quad 0 \leq i \leq [(n-j)(p-1)/p].
\]

For fixed \( i + j = k \), the exponent of \( p \) is decreasing in \( j \) and the minimum value is attained when \( j = k \) and \( i = 0 \). It follows that

\[
\psi^a \left( \frac{1}{\pi^n} A^+ \right) \subseteq \sum_{k \geq 0} \frac{1}{\pi^{n-k}} \left[ \frac{(a-1)n-a+2}{(a-1)p-a+2} \right]^{(p-1)\left(\frac{1}{p-1}\right)-k((a-1)p-a+2)-1+(n-k-1)A^+}
\]

\[
\subseteq \sum_{k=0}^{\left\lfloor \frac{(an-a+1)(p-1)}{ap-a+1} \right\rfloor} \frac{1}{\pi^{n-k}} \left[ \frac{(an-a+1)(p-1)}{ap-a+1} \right]^{-k((ap-a+1)-1)} A^+,
\]

where we stop at \( k = \left\lfloor \frac{(an-a+1)(p-1)}{ap-a+1} \right\rfloor \) in the summation as the exponent of \( p \) is zero if \( k \geq \left\lfloor \frac{(an-a+1)(p-1)}{ap-a+1} \right\rfloor \).

Corollary 4.5 (Sharp Congruence II). Let

\[
S_j(n, r, p^a) = \sum_{i_0 + \cdots + i_j p^a - 1 = n \atop i_1 + 2i_2 + \cdots \equiv r (\text{mod} p^a)} \binom{n}{i_0 \cdots i_j} \left( \frac{i_0 + 2i_2 + \cdots - r}{p^a} \right)_{\frac{n}{j}}.
\]

Then for integer \( j \geq 0 \), we have

\[
S_j(n, r, p^a) \equiv 0(\text{mod} p^{\left\lfloor \frac{(an-a+1)(p-1)-j((ap-a+1)-1)}{p-1} \right\rfloor}).
\]
References

[1] L.E. Dickson, History of the Theory of Numbers, Vol. I, AMS Chelsea Publ., 1999, Chapter XI, pp. 270-275.

[2] Z.W. Sun, Polynomial extension of Fleck’s congruence, preprint, 2005, arXiv:math.NT/0507008.

[3] Z.W. Sun and D.M. Davis, A combinatorial congruence for polynomials, arXiv:math.NT/0508087.

[4] D. Wan, Fontaine’s Rings and $p$-Adic L-Functions, Lecture Notes at the Morningside Center of Mathematics, 2005.

[5] C.S. Weisman, Some congruences for binomial coefficients, Michigan Math. J., 24(1977), 141-151.