GENERALIZATIONS OF WOLSTENHOLME'S THEOREM VIA THE P-ADIC LOGARITHM

Peter Lombaers [1]
Dep. de Mathemática, Centro de Mathemática, Universidade do Porto, Porto, Portugal
p.lombaers@gmail.com

Received:4/8/19, Revised: 2/17/20, Accepted: 5/10/20, Published: 5/26/20

Abstract

We use the p-adic logarithm to express the binomial coefficient $\binom{2p-1}{p-1}$ in terms of harmonic sums, where p is an odd prime. We use the same logarithmic method on norms of cyclotomic integers to obtain several congruences. For example, we show:

$$\sum_{k=1}^{p-1}(-1)^{k-1}\frac{1}{k}\binom{2k}{k} \equiv \frac{(1-L_p^2)(L_p^2-3)}{2p} \mod p^2,$$

where L_p is a the p-th Lucas number.

1. Introduction

In 1862, Joseph Wolstenholme [10] proved the following theorem:

Theorem 1. *For any prime $p \geq 5$ we have:*

$$\binom{2p-1}{p-1} \equiv 1 \mod p^3, \tag{1}$$

$$\sum_{k=1}^{p-1}\frac{1}{k} \equiv 0 \mod p^2, \tag{2}$$

$$\sum_{k=1}^{p-1}\frac{1}{k^2} \equiv 0 \mod p. \tag{3}$$

Let us set $H_n^{(i)} = \sum_{k=1}^{n}\frac{1}{k^i}$ and $H_n = H_n^{(1)}$. So Wolstenholme's theorem says $H_{p-1} \equiv 0 \mod p^2$ and $H_{p-1}^{(2)} \equiv 0 \mod p$. Over the years many generalizations of

[1]The author was partially supported by CMUP (UID/MAT/00144/2013), which is funded by FCT (Portugal) with national (MEC) and European structural funds (FEDER), under the partnership agreement PT2020 and by FCT (Portugal) through the PhD grant PD/BD/128063/2016.

this theorem have been investigated. For a nice survey, see the article [3]. One generalization is to consider $\binom{2p-1}{p-1}$ modulo higher powers of p and express it in terms of harmonic sums $H_{p-1}^{(i)}$, see for example [8, 4]. This leads to statements such as ([3], p. 6):

$$\binom{2p-1}{p-1} \equiv 1 + 2pH_{p-1} + \frac{2}{3}p^3 H_{p-1}^{(3)} + 2p^2 \left(H_{p-1}\right)^2 + \frac{4}{3}p^4 H_{p-1}H_{p-1}^{(3)} + \frac{2}{5}p^5 H_{p-1}^{(5)} \mod p^9. \tag{4}$$

In the article [1], the author used the p-adic logarithm and exponential functions to study congruence conditions for binomial coefficients. In the present article we will show that many Wolstenholme type theorems such as (4) can be proven in a uniform manner by using the properties of the p-adic logarithm and the p-adic exponential function. Using this method we can extend identities such as (4) to arbitrary high powers of p. This leads to Theorem 2 below. As an application, in Corollary 1 we prove the following congruence:

$$\begin{aligned}\binom{2p-1}{p-1} \equiv 1 &+ 2pH_{p-1} + \frac{2}{3}p^3 H_{p-1}^{(3)} + \frac{2}{5}p^5 H_{p-1}^{(5)} + \frac{2}{7}p^7 H_{p-1}^{(7)} \\ &+ \frac{2}{9}p^9 H_{p-1}^{(9)} + 2p^2 \left(H_{p-1}\right)^2 + \frac{2}{9}p^6 \left(H_{p-1}^{(3)}\right)^2 \\ &+ \frac{4}{3}p^4 H_{p-1}H_{p-1}^{(3)} + \frac{4}{5}p^6 H_{p-1}H_{p-1}^{(5)} \\ &+ \frac{4}{3}p^3 \left(H_{p-1}\right)^3 + \frac{4}{3}p^5 \left(H_{p-1}\right)^2 H_{p-1}^{(3)} \mod p^{12}.\end{aligned}$$

Following the article [2], we call a prime p a Wolstenholme prime if it satisfies $\binom{2p-1}{p-1} \equiv 1 \mod p^4$. The author shows that the primes 16843 and 2124679 are the only two Wolstenholme primes smaller than 10^9. Moreover he conjectured there are infinitely many Wolstenholme primes. Using the p-adic logarithm, we obtain characterisations of Wolstenholme primes in terms of harmonic sums. This leads to a characterisation of Wolstenholme primes modulo p^{12} in Theorem 4. Thereby we confirm a conjecture from [3] (Remark 24), which says that a prime p is Wolstenholme if and only if it satisfies

$$\binom{2p-1}{p-1} \equiv 1 + 2pH_{p-1} + \frac{2}{3}p^3 H_{p-1} + \frac{2}{5}p^5 H_{p-1}^{(5)} \mod p^8.$$

In the second part of this article we apply the logarithmic method of the first part to norms of integers of cyclotomic fields. The analog of Lemma 2 is given by Theorem 5. As an application, in Proposition 1 we prove the congruence

$$\sum_{k=1}^{p-1} \frac{1}{k}\binom{2k}{k} \equiv 0 \mod p^2.$$

This is the weaker, modulo p^2 version of a result from [8]. Moreover, in Theorem 6, we get the congruence

$$\sum_{k=1}^{p-1}(-1)^{k-1}\frac{1}{k}\binom{2k}{k} \equiv \frac{(1-L_p^2)(L_p^2-3)}{2p} \mod p^2,$$

where L_p is the p-th Lucas number. This improves on a result in [7]. Finally we find a congruence involving the integers of the sequence A092765 of the OEIS.

2. Logarithms and Binomial Coefficients

2.1. Properties of the p-adic Logarithm and Exponential

First we will collect the properties of the p-adic logarithm that we need for our purpose. As a reference see for example [9], page 50. Let p be an odd prime, and let $\mathbb{Q}_p$ be the field of p-adic numbers. For $x \in \mathbb{Q}_p$ we denote by $\nu_p(x)$ the p-adic valuation of x. If $x \in \mathbb{Q}_p$ satisfies $x \equiv 1 \mod p$, i.e. $\nu_p(x-1) \geq 1$, then

$$\log_p(x) := -\sum_{i\geq 1}\frac{(1-x)^i}{i}.$$

The function $\log_p$ takes on values in $\mathbb{Q}_p$. In general the p-adic logarithm can be extended to the whole of $\mathbb{Q}_p$, but we will not need this. We will drop the subscript and just write log instead of $\log_p$ to ease the notation. Just like the normal logarithm, the p-adic logarithm satisfies

$$\log(xy) = \log(x) + \log(y)$$

when both x and y are congruent to 1 modulo p.

For $x \equiv 0 \mod p$, the p-adic exponential function is defined by

$$\exp_p(x) = \exp(x) := \sum_{i\geq 0}\frac{x^i}{i!}.$$

If both $\nu_p(x), \nu_p(y) \geq 1$ then we have $\exp(xy) = \exp(x) + \exp(y)$. Moreover, if $\nu_p(x) \geq 1$ then $\log(\exp x) = x$ and $\exp(\log(1+x)) = 1 + x$.

We will also need the following lemma.

Lemma 1. *Let $x \in \mathbb{Q}_p$ satisfy $x \equiv 1 \mod p$, and let $0 < k < p-2$. Then*

$$x \equiv \sum_{i=0}^{k}\frac{(\log(x))^i}{i!} \mod p^{r(k+1)}$$

if and only if $x \equiv 1 \mod p^r$.

Proof. We have $x \equiv 1 \mod p^r$ if and only if $\log(x) \equiv 0 \mod p^r$. Moreover, we have

$$x = \exp\log(x) = \sum_{i\geq 0} \frac{(\log(x))^i}{i!},$$

so it is enough to show that for any $y \equiv 1 \mod p$ we have

$$\sum_{i\geq k+1} \frac{y^i}{i!} \equiv 0 \mod p^{r(k+1)}$$

if and only if $y \equiv 1 \mod p^r$. This amounts to showing that $\nu_p\left(\frac{y^i}{i!}\right) > \nu_p\left(\frac{y^{k+1}}{(k+1)!}\right)$, because then we have $\nu_p\left(\sum_{i\geq k+1} \frac{y^i}{i!}\right) = \nu_p\left(\frac{y^{k+1}}{(k+1)!}\right)$. But $\nu_p\left(\frac{y^{k+2}}{(k+2)!}\right) > \nu_p\left(\frac{y^{k+1}}{(k+1)!}\right)$ follows from the fact that $k < p-2$, whilst for $i > k+2$ the claim is obvious. □

2.2. Wolstenholme-type Theorems

Our main tool will be the next lemma.

Lemma 2. *In $\mathbb{Q}_p$ we have the following three identities:*

$$\sum_{i=1}^{\infty} \frac{p^i}{i} H_{p-1}^{(i)} = 0, \tag{5}$$

$$\sum_{i=1}^{\infty} (-1)^{i-1} \frac{p^i}{i} H_{p-1}^{(i)} = \log\binom{2p-1}{p-1}, \tag{6}$$

$$2\sum_{i=1}^{\infty} \frac{p^{2i-1}}{(2i-1)} H_{p-1}^{(2i-1)} = \log\binom{2p-1}{p-1}. \tag{7}$$

Proof. Note that, since p is odd, $1 = \prod_{k=1}^{p-1} \frac{k-p}{k}$. Hence we get:

$$\begin{aligned} 0 = -\log_p(1) &= -\sum_{k=1}^{p-1} \log_p(1 - \frac{p}{k}) \\ &= \sum_{k=1}^{p-1}\sum_{i=1}^{\infty} \frac{p^i}{k^i i} = \sum_{i=1}^{\infty} \frac{p^i}{i} H_{p-1}^{(i)}. \end{aligned}$$

For the second identity, we note $\binom{2p-1}{p-1} = \prod_{k=1}^{p-1} \frac{p+k}{k} \equiv 1 \mod p$, which allows us to proceed in exactly the same manner as for the first identity. Finally, the third identity is obtained by adding the first two to each other. □

The following lemma is useful for simplifying some of the expressions we will obtain.

Lemma 3. *For any $i \in \mathbb{N}$ we have:*

$$H_{p-1}^{(i)} \equiv \begin{cases} 0 \mod p, & \text{if } p-1 \nmid i \\ -1 \mod p, & \text{if } p-1 \mid i. \end{cases}$$

If i is odd, then:

$$H_{p-1}^{(i)} \equiv \begin{cases} 0 \mod p^2, & \text{if } p-1 \nmid i+1 \\ \frac{ip}{2} \mod p^2, & \text{if } p-1 \mid i+1. \end{cases}$$

Proof. The first claim follows easily from the existence of a primitive root modulo p. For the second claim, note that we have

$$\begin{aligned} \sum_{k=1}^{p-1} \frac{1}{k^i} &= \sum_{k=1}^{(p-1)/2} \frac{k^i + (p-k)^i}{k^i(p-k)^i} \\ &\equiv \sum_{k=1}^{(p-1)/2} \frac{k^i + (-k)^i + ip(-k)^{i-1}}{k^i(p-k)^i} \mod p^2. \end{aligned}$$

So, if i is odd, we see that

$$H_{p-1}^{(i)} \equiv -ip \sum_{k=1}^{(p-1)/2} \frac{1}{k^{i+1}} \equiv -\frac{ip}{2} H_{p-1}^{(i+1)} \mod p^2.$$

□

Lemma 3 covers parts (2) and (3) of Wolstenholme's theorem 1. Note that the equivalence of (2) and (3) also follows from our Lemma 2 by looking at equation (5) modulo p^3, after knowing that $H_{p-1}^{(3)} \equiv 0 \mod p$. The equivalence between (1) and the other two parts of Wolstenholme's theorem follows by looking at (7) modulo p^3.

For $p = 3$ we have $\binom{5}{3} = 1 + 3^2$ and by Wolstenholme's theorem, for $p \geq 5$ we have $\binom{2p-1}{p-1} \equiv 1 \mod p^3$ for $p \geq 5$. Therefore, by the general properties of the p-adic logarithm and exponential we know that $\exp \log \binom{2p-1}{p-1} = \binom{2p-1}{p-1}$. Combined with Lemma 2, this allows us to express $\binom{2p-1}{p-1}$ in terms of harmonic sums.

Theorem 2. *Let p be an odd prime. In $\mathbb{Q}_p$ we have the identity:*

$$\binom{2p-1}{p-1} = \sum_{n \geq 0} \frac{1}{n!} \left(2 \sum_{i \geq 1} \frac{p^{2i-1}}{2i-1} H_{p-1}^{(2i-1)} \right)^n. \tag{8}$$

Proof. The proof follows immediately from the combination of Lemma 2 and the

definition of the exponential function:

$$\begin{aligned}\binom{2p-1}{p-1} &= \exp\log\binom{2p-1}{p-1} \\ &= \sum_{n\geq 0}\frac{1}{n!}\left(\log\binom{2p-1}{p-1}\right)^n \\ &= \sum_{n\geq 0}\frac{1}{n!}\left(2\sum_{i\geq 1}\frac{p^{2i-1}}{2i-1}H_{p-1}^{(2i-1)}\right)^n.\end{aligned}$$

□

By looking modulo a specific power p^k, and using Lemma 3 to eliminate the terms which are congruent to 0 modulo p^k, we can obtain previously known results, such as the following.

Corollary 1. *For any prime $p \geq 11$ we have the congruence:*

$$\begin{aligned}\binom{2p-1}{p-1} \equiv 1 &+ 2pH_{p-1} + \frac{2}{3}p^3H_{p-1}^{(3)} + \frac{2}{5}p^5H_{p-1}^{(5)} + \frac{2}{7}p^7H_{p-1}^{(7)} \\ &+ \frac{2}{9}p^9H_{p-1}^{(9)} + 2p^2\left(H_{p-1}\right)^2 + \frac{2}{9}p^6\left(H_{p-1}^{(3)}\right)^2 \\ &+ \frac{4}{3}p^4H_{p-1}H_{p-1}^{(3)} + \frac{4}{5}p^6H_{p-1}H_{p-1}^{(5)} \\ &+ \frac{4}{3}p^3\left(H_{p-1}\right)^3 + \frac{4}{3}p^5\left(H_{p-1}\right)^2H_{p-1}^{(3)} \mod p^{12}.\end{aligned}$$

Proof. By Lemma 3, $H_{p-1}^{(2i-1)} \equiv 0 \mod p$ for all odd primes p and $i \geq 1$. Also, for $p \geq 5$ we see that $pH_{p-1} \equiv 0 \mod p^3$. Hence, if we look at equation (8) modulo p^{12}, we only need to consider $n \leq 3$. So we find:

$$\begin{aligned}\binom{2p-1}{p-1} \equiv 1 &+ 2pH_{p-1} + \frac{2}{3}p^3H_{p-1}^{(3)} + \cdots + \frac{2}{9}p^9H_{p-1}^{(9)} \\ &+ \frac{1}{2}\left(2pH_{p-1} + \frac{2}{3}p^3H_{p-1}^{(3)} + \cdots + \frac{2}{9}p^9H_{p-1}^{(9)}\right)^2 \\ &+ \frac{1}{6}\left(2pH_{p-1} + \frac{2}{3}p^3H_{p-1}^{(3)} + \cdots + \frac{2}{9}p^9H_{p-1}^{(9)}\right)^3 \mod p^{12}.\end{aligned}$$

Expanding the square and the cube, and using Lemma 3 to eliminate the terms that are congruent to 0 modulo p^{12}, we end up with the statement of the corollary for primes $p \geq 11$. For smaller primes p, there will be some extra terms, but we will not give those formulas here. □

Remark 1. Looking modulo p^6 we obtain for all primes $p \geq 5$:

$$\binom{2p-1}{p-1} \equiv 1 + 2pH_{p-1} + \frac{2}{3}p^3 H_{p-1}^{(3)} \mod p^6.$$

This was originally proved in [8]. Looking modulo p^9 we get the congruence mentioned in the introduction, i.e., for all primes $p \geq 7$:

$$\binom{2p-1}{p-1} \equiv 1 + 2pH_{p-1} + \frac{2}{3}p^3 H_{p-1}^{(3)} + \frac{2}{5}p^5 H_{p-1}^{(5)} + 2p^2 \left(H_{p-1}\right)^2 + \frac{4}{3}p^4 H_{p-1} H_{p-1}^{(3)} \mod p^9.$$

2.3. Wolstenholme Primes

By using Lemma 2, one can quickly prove the following well-known fact.

Theorem 3. *For any prime p the following are equivalent:*

$$\binom{2p-1}{p-1} \equiv 1 \mod p^4, \tag{9}$$

$$H_{p-1} \equiv 0 \mod p^3, \tag{10}$$

$$H_{p-1}^{(2)} \equiv 0 \mod p^2. \tag{11}$$

Proof. From Lemma 1, we know that, for $p > 3$, $\binom{2p-1}{p-1} \equiv 1 \mod p^4$ if and only if $\log \binom{2p-1}{p-1} \equiv 0 \mod p^4$. Looking at (7) modulo p^4, we see that this happens if and only if $H_{p-1} \equiv 0 \mod p^3$. Finally, looking at (6) modulo p^4 we see that $H_{p-1} \equiv \frac{p}{2} H_{p-1}^{(2)} \mod p^3$, which proves the theorem. □

As in the article [2], we call a prime satisfying any of these conditions a *Wolstenholme prime*. The two known Wolstenholme primes are 16843 and 2124679. We can use the methods of the previous section to give characterisations of Wolstenholme primes in terms of harmonic sums.

Theorem 4. *A prime p is Wolstenholme if and only if:*

$$\binom{2p-1}{p-1} \equiv 1 + 2pH_{p-1} + \frac{2}{3}p^3 H_{p-1}^{(3)} + \frac{2}{5}p^5 H_{p-1}^{(5)} + \frac{2}{7}p^7 H_{p-1}^{(7)} + \frac{2}{9}p^9 H_{p-1}^{(9)} + 2p^2 H_{p-1}^2 + \frac{4}{3}p^4 H_{p-1} H_{p-1}^{(3)} + \frac{4}{5}p^6 H_{p-1} H_{p-1}^{(5)} + \frac{2}{9}p^6 \left(H_{p-1}^{(3)}\right)^2 \mod p^{12}.$$

Proof. By Lemma 1 we know that p is Wolstenholme if and only if

$$\binom{2p-1}{p-1} \equiv 1 + \log \binom{2p-1}{p-1} + \frac{1}{2}\left(\log \binom{2p-1}{p-1}\right)^2 \mod p^{12}.$$

Now we substitute the expression (7) we obtained for the logarithm. We obtain the result of the theorem after eliminating the terms which are 0 modulo p^{12} by using Lemma 3 and Theorem 3, exactly like we did in the proof of Corollary 1. Since the first primes are not Wolstenholme, we do not need to concern ourselves with a lower bound for p like we did in that corollary. □

Remark 2. By looking modulo p^8 we obtain that p is a Wolstenholme prime if and only if

$$\binom{2p-1}{p-1} \equiv 1 + 2pH_{p-1} + \frac{2}{3}p^3 H_{p-1} + \frac{2}{5}p^5 H_{p-1}^{(5)} \mod p^8.$$

This is congruence (49) of [3], which is also given in Proposition 1.1 of [5]. In Remark 24 of that article, the author asks whether this congruence characterizes Wolstenholme primes. The theorem above proves that this is indeed the case.

Of course, for prime p such that $\binom{2p-1}{p-1} \equiv 1 \mod p^5$ we could do the same procedure to obtain congruences that characterize these primes. However, in [2] the author conjectures that there are infinitely many Wolstenholme primes, but no primes p such that $\binom{2p-1}{p-1} \equiv 1 \mod p^5$. Therefore, we do not give the corresponding congruences in this article.

3. Logarithms and Cyclotomic Integers

Let p be an odd prime, $\zeta = \zeta_p$ a primitive p-th root of unity, $K = \mathbb{Q}(\zeta)$ the p-th cyclotomic field and $\mathcal{O}_K = \mathbb{Z}[\zeta]$ its ring of integers. The ideal (p) is totally ramified in $K/\mathbb{Q}$, in fact we have $p\mathcal{O}_K = \pi^{p-1}\mathcal{O}_K$ where $\pi = 1 - \zeta$. We denote the elements of $\mathrm{Gal}(K/\mathbb{Q})$ by σ_j, $j = 1, \ldots, p-1$, where σ_j is defined by $\sigma_j(\zeta) = \zeta^j$. Denote by $\mathrm{N}_{K/\mathbb{Q}} = \mathrm{N}$ the norm of K and by $\mathrm{Tr}_{K/Q} = \mathrm{Tr}$ the trace, so $\mathrm{N}(x) = \prod_{j=1}^{p-1} \sigma_j(x)$ and $\mathrm{Tr}(x) = \sum_{j=1}^{p-1} \sigma_j(x)$.

In exactly the same way as we did for binomial coefficients modulo p, we can use the p-adic logarithm to obtain congruence relations for norms of elements of $\mathcal{O}_K$. We need an extension of the p-adic logarithm to the field $\mathbb{Q}_p(\zeta)$. We will denote by ν_π the valuation with respect to the prime ideal $\pi\mathcal{O}_K$. For our purposes it is enough to know that if $\nu_\pi(x-1) \geq 1$, then

$$\log(x) = -\sum_{i \geq 1} \frac{(1-x)^i}{i},$$

and if $x \equiv y \equiv 1 \mod \pi$, then $\log(xy) = \log(x) + \log(y)$. The analog of Lemma 2 is given by the following theorem.

Theorem 5. *Let $\alpha \in \mathcal{O}_K$ be such that $\nu_\pi(\alpha) \geq 1$. Then we have, in $\mathbb{Q}_p$:*

$$\sum_{k=1}^{\infty} \frac{1}{k} \mathrm{Tr}(\alpha^k) = -\log \mathrm{N}(1-\alpha). \tag{12}$$

If moreover we know that $1-\alpha$ is a unit, then

$$\sum_{k=1}^{\infty} \frac{1}{k} \mathrm{Tr}(\alpha^k) = 0, \tag{13}$$

$$-2\sum_{k=1}^{\infty} \frac{\mathrm{Tr}(\alpha^{2k-1})}{2k-1} = \log \mathrm{N}(1+\alpha), \tag{14}$$

and in particular we get:

$$\sum_{k=1}^{p-1} \frac{1}{k} \mathrm{Tr}(\alpha^k) \equiv 0 \mod p^{\nu_\pi(\alpha)}. \tag{15}$$

Proof. Applying the p-adic logarithm to $\mathrm{N}(1-\alpha)$ we see:

$$\begin{aligned} \log(\mathrm{N}(1-\alpha)) &= \sum_{j=1}^{p-1} \log(1-\sigma_j(\alpha)) \\ &= -\sum_{j=1}^{p-1}\sum_{k=1}^{\infty} \frac{\sigma_j(\alpha^k)}{i} \\ &= -\sum_{k=1}^{\infty} \frac{1}{k} \mathrm{Tr}(\alpha^k), \end{aligned}$$

which gives the first identity. If $1-\alpha$ is a unit, then we have $\mathrm{N}(1-\alpha) = 1$ so $\log \mathrm{N}(1-\alpha) = 0$. For the third identity, note that we have

$$\log(\mathrm{N}(1+\alpha)) = \sum_{i \geq 1} \frac{(-1)^{i+1}}{i} \mathrm{Tr}(\alpha^i).$$

Adding this to the second we get

$$\log(\mathrm{N}(1+\alpha)) = \sum_{i \geq 1} \frac{(-1)+(-1)^{i+1}}{i} \mathrm{Tr}(\alpha^i) = -2\sum_{i \geq 1} \frac{\mathrm{Tr}(\alpha^{2k-1})}{2k-1}.$$

Now we investigate the p-adic valuation of $\frac{1}{k}\mathrm{Tr}(\alpha^k)$. We know that $\nu_\pi(\mathrm{Tr}(x)) \geq \nu_\pi(x)$ so we find:

$$\nu_\pi\left(\frac{1}{k}\mathrm{Tr}(\alpha^k)\right) \geq k\nu_\pi(\alpha) - \nu_\pi(k).$$

If $p \nmid k$, then of course $\nu_\pi\left(\frac{1}{k}\mathrm{Tr}(\alpha^k)\right) \geq k\nu_\pi(\alpha)$. When $\nu_p(k) = t \geq 1$, then, using Bernouilli's inequality, one gets

$$\begin{aligned} k\nu_\pi(\alpha) - \nu_\pi(k) &\geq p^t\nu_\pi(\alpha) - t(p-1) \\ &\geq (1 + t(p-1))\,\nu_\pi(\alpha) - t(p-1) \\ &\geq \nu_\pi(\alpha) + t(p-1)(\nu_\pi(\alpha) - 1). \end{aligned}$$

In particular, we see that for any $k \geq p$ one has

$$\nu_\pi\left(\frac{1}{k}\mathrm{Tr}(\alpha^k)\right) > (p-1)(\nu_\pi(\alpha) - 1),$$

and since $\frac{1}{k}\mathrm{Tr}(\alpha^k)$ is a rational number, this means that

$$\nu_p\left(\frac{1}{k}\mathrm{Tr}(\alpha^k)\right) \geq \nu_\pi(\alpha).$$

The congruence (15) then follows from equality (13). □

The discrete Fourier transform will be useful for calculating the trace of an element:

Lemma 4. *Let p be an odd prime and for $j = 0, p-1$, let f_j be a complex number. If $g_i = \sum_{j=0}^{p-1} f_j\zeta^{ij}$ then $f_j = \frac{1}{p}\sum_{i=0}^{p-1} g_i\zeta^{-ij}$.*

Proof. This is a simple calculation:

$$\sum_{i=0}^{p-1} g_i\zeta^{-ij} = \sum_{i=0}^{p-1}\left(\sum_{k=0}^{p-1} f_k\zeta^{ik}\right)\zeta^{-ij} = \sum_{k=0}^{p-1} f_k\left(\sum_{i=0}^{p-1}\zeta^{i(k-j)}\right) = pf_j.$$

□

We are now ready to apply this to specific units.

Proposition 1. *For any prime $p \geq 5$ we have*

$$\sum_{k=1}^{p-1}\frac{1}{k}\binom{2k}{k} \equiv 0 \mod p^2.$$

Proof. Consider the element $\zeta - 1 + \zeta^{-1} = 1 + \zeta^{-1}(1-\zeta)^2$, so that in this case we have $\alpha = -\zeta^{-1}(1-\zeta)^2$. Note that for $p > 3$ we have

$$\zeta(\zeta - 1 + \zeta^{-1})(\zeta + 1) = \zeta^3 + 1 = \frac{1-\zeta^6}{1-\zeta^3},$$

so $1-\alpha$ is indeed a unit. We will calculate the trace of α^k. We know

$$(1-\zeta^i)^{2k} = \sum_{r=-\infty}^{\infty} \binom{2k}{r}(-1)^r\zeta^{ir} = \sum_{j=0}^{p-1}\left(\sum_{r\equiv j \bmod p}(-1)^r\binom{2k}{r}\right)\zeta^{ij}.$$

Now we can apply Lemma 4 with $g_i = (1-\zeta^i)^{2k}$ to get

$$\sum_{r\equiv j \bmod p}(-1)^r\binom{2k}{r} = \frac{1}{p}\sum_{i=1}^{p-1}(1-\zeta^i)^{2k}\zeta^{-ij} = \frac{1}{p}\mathrm{Tr}(\zeta^{-j}(1-\zeta)^{2k}).$$

In particular we have

$$\mathrm{Tr}(\alpha^k) = p\sum_{r\equiv k \bmod p}(-1)^{k+r}\binom{2k}{r},$$

and for $0<k<p$ this means

$$\mathrm{Tr}(\alpha^k) = p\binom{2k}{k}.$$

Because $\nu_\pi(\alpha)=2$, (15) immediately gives us that

$$p\sum_{k=1}^{p-1}\frac{1}{k}\binom{2k}{k} = \sum_{k=1}^{p-1}\frac{1}{k}\mathrm{Tr}(\alpha^k) \equiv 0 \mod p^2.$$

We can easily get the result modulo p^2 by using the fact that, for $k>p$, one has $\nu_\pi(\frac{\alpha^k}{k}) \geq 2(p+1)$, and thus $\frac{1}{k}\mathrm{Tr}(\alpha^k) \equiv 0 \mod p^3$. This means that we have

$$\begin{aligned}\sum_{k=1}^{p-1}\frac{1}{k}\mathrm{Tr}(\alpha^k) &\equiv -\frac{1}{p}\mathrm{Tr}(\alpha^p) = -\sum_{r\equiv 0 \bmod p}(-1)^{p+r}\binom{2p}{r}\\ &= -\left(\binom{2p}{p}-2\right) \equiv 0 \mod p^3,\end{aligned}$$

by Wolstenholme's theorem. □

Remark 3. These trace calculations can be used to find some identities on their own. For example we can write $\alpha = -\zeta(1-\zeta)^2$ from Proposition 1 also as $\alpha = (1-\zeta)(1-\zeta^{-1})$. Doing the trace calculation in the second form we get

$$\mathrm{Tr}(\alpha^k) = p\sum_{r\equiv s \bmod p}(-1)^{r+s}\binom{k}{r}\binom{k}{s}.$$

If $k<p$ the only solution for $r\equiv s \mod p$ is $r=s$. Combining this with the expression we found for $\mathrm{Tr}(\alpha^k)$ in Proposition 1 we find

$$\binom{2k}{k} = \sum_{r=0}^{k}\binom{k}{r}^2$$

(which is also an easy consequence of Vandermonde's identity).

Remark 4. In [8] the author shows via a different method that in fact we have

$$\sum_{k=1}^{p-1} \frac{1}{k}\binom{2k}{k} \equiv -\frac{8}{3}H_{p-1} \equiv -\frac{2}{3}\left(\binom{2p}{p} - 2\right) \mod p^4.$$

So far we have been using the fact that the norm of a unit is equal to 1, so it was not necessary to calculate norms. If the element we are dealing with is not a unit, we can sometimes still calculate the norm in terms of recurrence sequences.

Lemma 5. *Let $a, b, c \in \mathbb{Q}$ such that $a(b+c+1) \neq 0$. Define a recurrence sequence $(G_k)_{k\in\mathbb{N}}$ by $G_0 = \frac{2}{b+c+1}, G_1 = \frac{-b}{b+c+1}$ and*

$$G_{k+2} = -\frac{b}{a}G_{k+1} - \frac{c}{a}G_k.$$

Then we have:

$$N(a\zeta^2 + b\zeta + c) = a^{p-1}(c^p + 1 - G_p).$$

Proof. We define $\omega = \frac{-b+\sqrt{b^2-4ac}}{2a}$ and $\overline{\omega} = \frac{-b-\sqrt{b^2-4ac}}{2a}$ so that we have $ax^2 + bx + c = a(x-\omega)(x-\overline{\omega})$, $\omega\overline{\omega} = c$ and $\omega + \overline{\omega} = -b$. Then we see:

$$\begin{aligned}
N(a\zeta^2 + b\zeta + c) &= \prod_{j=1}^{p-1} \left(a\zeta^{2j} + b\zeta^j + c\right) \\
&= a^{p-1} \prod_{j=1}^{p-1} (\zeta^j - \omega)(\zeta^j - \overline{\omega}) \\
&= a^{p-1} \frac{\omega^p - 1}{\omega - 1} \frac{\overline{\omega}^p - 1}{\overline{\omega} - 1} \\
&= a^{p-1} \frac{\omega^p\overline{\omega}^p - \omega^p - \overline{\omega}^p + 1}{\omega\overline{\omega} - \omega - \overline{\omega} + 1} \\
&= a^{p-1} \frac{c^p + 1 - (\omega^p + \overline{\omega}^p)}{c + b + 1}.
\end{aligned}$$

Finally notice that the numbers $\frac{\omega^p+\overline{\omega}^p}{c+b+1}$ give exactly the recurrence sequence we defined. □

As an application of this we have the following theorem.

Theorem 6. *Let p be an odd prime and let L_p be the p-th Lucas number, i.e. $L_0 = 2, L_1 = 1$ and $L_{k+2} = L_{k+1} + L_k$. Then we have:*

$$\sum_{k=1}^{p-1} (-1)^{k-1} \frac{1}{k}\binom{2k}{k} \equiv \frac{(1 - L_p^2)(L_p^2 - 3)}{2p} \mod p^2.$$

Proof. Again let $\alpha = -\zeta^{-1}(1-\zeta)^2$ as in the previous proposition. Then $1+\alpha = 3-\zeta-\zeta^{-1}$. Note that we have

$$(\zeta^2-\zeta-1)(\zeta^{-2}-\zeta^{-1}-1) = 3-\zeta^2-\zeta^{-2}$$

and therefore $N(1+\alpha) = N(\zeta^2-\zeta-1)^2$. By using Lemma 5 we see that $N(\zeta^2-\zeta-1) = L_p$. So $N(1+\alpha) = L_p^2$ and we can use this to calculate $\log(N(1+\alpha))$. We find:

$$\begin{aligned}\log(N(1+\alpha)) &\equiv N(1+\alpha) - 1 - \frac{1}{2}\left(N(1+\alpha)-1\right)^2 \\ &\equiv L_p^2 - 1 - \frac{1}{2}\left(L_p^2-1\right)^2 \\ &\equiv \frac{(1-L_p^2)(L_p^2-3)}{2} \mod p^3.\end{aligned}$$

On the other hand, in the previous proposition we saw that $\mathrm{Tr}(\alpha)^k \equiv 0 \mod p^3$ for $k \geq p$, and thus (12) tells us that

$$\log(N(1+\alpha)) \equiv \sum_{k=1}^{p-1}(-1)^{k-1}\frac{1}{k}\mathrm{Tr}(\alpha^k) \equiv p\sum_{k=1}^{p-1}(-1)^{k-1}\frac{1}{k}\binom{2k}{k} \mod p^3.$$

Together these give the desired result. □

Remark 5. In the article [7], the authors show that

$$\sum_{k=1}^{p-1}(-1)^{k-1}\frac{1}{k}\binom{2k}{k} \equiv 5\frac{F_{p-\left(\frac{p}{5}\right)}}{p} \mod p.$$

Here F_k is the k-th Fibonacci number. Using the fact $F_{p-\left(\frac{p}{5}\right)} \equiv L_p^2 - 1 \mod p$ it is easy to see that Theorem 6 reduces to this result modulo p.

A prime p for which $F_{p-\left(\frac{p}{5}\right)} \equiv 0 \mod p^2$ is called a Wall-Sun-Sun prime. It has been shown that if the first case of Fermat's last theorem fails, then p must be a Wall-Sun-Sun prime. It is interesting to compare this with the case of Wolstenholme primes. It has been shown that if the first case of Fermat's last theorem fails, then p must divide the Bernoulli number B_{p-3} which happens if and only if $\binom{2p-1}{p-1} \equiv 1 \mod p^4$.

Now we apply our results to a different element α. The result we obtain is concerned with the following sequence. For $k \geq 0$, define

$$a_k := \sum_{s=0}^{k}\binom{k}{s}\binom{k}{2k-3s}.$$

This is sequence A092765 of the OEIS [6], starting with

$$1, 0, 4, 6, 36, 100, 430, 1470, 5796, \ldots$$

Proposition 2. *For a prime $p \geq 7$ we have*

$$\sum_{k=1}^{(p-1)/2} (-1)^k \frac{a_k}{k} \equiv 0 \mod p.$$

Proof. Consider the element $\alpha = -\zeta^2 + \zeta + \zeta^{-1} - \zeta^{-2} = -\zeta^{-2}(1-\zeta)(1-\zeta^3)$. Then

$$1 - \alpha = \zeta^2 - \zeta + 1 - \zeta^{-1} + \zeta^{-2} = \zeta^{-2}\frac{1+\zeta^5}{1+\zeta}$$

is indeed a unit. To calculate the trace we use the same trick as in the previous example:

$$\begin{aligned}(1-\zeta^i)^k(1-\zeta^{3i})^k &= \left(\sum_{r=-\infty}^{\infty}\binom{k}{r}(-1)^r\zeta^{ir}\right)\left(\sum_{s=-\infty}^{\infty}\binom{k}{s}(-1)^s\zeta^{3is}\right)\\ &= \sum_{r,s=-\infty}^{\infty}(-1)^{r+s}\binom{k}{r}\binom{k}{s}\zeta^{i(3s+r)}\\ &= \sum_{j=0}^{p-1}\left(\sum_{3s+r\equiv j \bmod p}(-1)^{r+s}\binom{k}{r}\binom{k}{s}\right)\zeta^{ij}.\end{aligned}$$

By Lemma 4 we get

$$\begin{aligned}\sum_{3s+r\equiv j \bmod p}(-1)^{r+s}\binom{k}{r}\binom{k}{s} &= \frac{1}{p}\sum_{i=1}^{p-1}(1-\zeta^i)^k(1-\zeta^{3i})^k\zeta^{-ij}\\ &= \frac{1}{p}\mathrm{Tr}(\zeta^{-j}(1-\zeta)^k(1-\zeta^3)^k).\end{aligned}$$

Because $\nu_\pi(\alpha) = 2$ we know that $\nu_\pi\left(\frac{1}{k}\mathrm{Tr}(\alpha^k)\right) > p-1$ for $k > \frac{p-1}{2}$, and thus $\nu_\pi\left(\frac{1}{k}\mathrm{Tr}(\alpha^k)\right) > 1$. Now Theorem 5 tells us that

$$\sum_{k=1}^{(p-1)/2}\frac{1}{k}\mathrm{Tr}(\alpha^k) \equiv 0 \mod p^2.$$

For $0 \leq k \leq \frac{p-1}{2}$ and $0 \leq r, s \leq k$, the only solution to $3s + r \equiv 2k \mod p$ is $r = 2k - 3s$. Thus we find

$$\begin{aligned}0 \equiv \sum_{k=1}^{(p-1)/2}\frac{1}{k}\mathrm{Tr}(\alpha^k) &\equiv p\sum_{k=1}^{(p-1)/2}\frac{1}{k}\left(\sum_{3s+r\equiv 2k \bmod p}(-1)^{k+r+s}\binom{k}{r}\binom{k}{s}\right)\\ &\equiv p\sum_{k=1}^{(p-1)/2}\frac{(-1)^k}{k}\left(\sum_{s=0}^{k}\binom{k}{s}\binom{k}{2k-3s}\right) \mod p^2.\end{aligned}$$

□

The previous results were all obtained by starting with an element of the cyclotomic field, calculating its norm and trace, and then using the logarithm to obtain a congruence. Clearly one can get many more results in this way. However, a more interesting problem is the inverse problem. Suppose there is a congruence one would like to prove, is there a corresponding cyclotomic element that does the trick? Also it would be interesting to see if there are other, known identities that can be proved or improved using the logarithmic method.

References

[1] A. Granville, Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers, *Organic Mathematics (CMS Conf. Proc.)* **20** (1997), 253-276.

[2] R. J. McIntosh, On the converse of Wolstenholme's theorem, *Acta Arith.* **71**(4) (1995), 381-389.

[3] R. Meštrović, Wolstenholme's theorem: Its generalizations and extensions in the last hundred and fifty years (1862–2012), *arXiv:1111.3057* (2011).

[4] R. Meštrović, On the $\bmod p^7$ determination of $\binom{2p-1}{p-1}$, *Rocky Mountain J. Math.* **44(2)** (2014), 633-648.

[5] R. Meštrović, Congruences for Wolstenholme primes, *Czechoslovak Math. J.* **65(1)** (2015), 237-253.

[6] N. J. A. Sloane, The On-Line Encyclopedia of Integer Sequences, *Published electronically at* `https://oeis.org`, *Sequence A092765.*

[7] Z. Sun and R. Tauraso, New congruences for central binomial coefficients, *Adv. in Appl. Math.* **45**(1) (2010), 125-148.

[8] R. Tauraso, More congruences for central binomial coefficients, *J. Number Theory* **130**(12) (2010), 2639-2649.

[9] L. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag, New York, 1997.

[10] J. Wolstenholme, On certain properties of prime numbers, *Quart. J. Pure Appl. Math.* **5** (1862), 35-39.