Acta Arith. **127**(2007), no. 4, 337–363.

ON FLECK QUOTIENTS

Zhi-Wei Sun[1] (Nanjing) and Daqing Wan[2] (Irvine, CA)

[1]Department of Mathematics, Nanjing University
Nanjing 210093, People's Republic of China
zwsun@nju.edu.cn
`http://math.nju.edu.cn/~zwsun`

[2]Department of Mathematics, University of California
Irvine, CA 92697-3875, USA
dwan@math.uci.edu
`http://www.math.uci.edu/~dwan`

Abstract. Let p be a prime, and let $n \geqslant 1$ and r be integers. In this paper we study Fleck's quotient

$$F_p(n,r) = (-p)^{-\lfloor (n-1)/(p-1) \rfloor} \sum_{k \equiv r \pmod{p}} \binom{n}{k}(-1)^k \in \mathbb{Z}.$$

We determine $F_p(n,r) \bmod p$ completely by certain number-theoretic and combinatorial methods; consequently, if $2 \leqslant n \leqslant p$ then

$$\sum_{k=1}^{n} (-1)^{pk-1} \binom{pn-1}{pk-1} \equiv (n-1)! B_{p-n} p^n \pmod{p^{n+1}},$$

where $B_0, B_1, \ldots$ are Bernoulli numbers. We also establish the Kummer-type congruence $F_p(n+p^a(p-1), r) \equiv F_p(n,r) \pmod{p^a}$ for $a = 1, 2, 3, \ldots$, and reveal some connections between Fleck's quotients and class numbers of the quadratic fields $\mathbb{Q}(\sqrt{\pm p})$ and the p-th cyclotomic field $\mathbb{Q}(\zeta_p)$. In addition, generalized Fleck quotients are also studied in this paper.

2000 *Mathematics Subject Classification.* Primary 11B65; Secondary 05A10, 11A07, 11B68, 11B73, 11L05, 11S99.

The first author is supported by the National Science Fund for Distinguished Young Scholars (No. 10425103) in China. The second author is partially supported by NSF.

1. Introduction and main results

Let $m \in \mathbb{Z}^+ = \{1, 2, \dots\}$, $n \in \mathbb{N} = \{0, 1, \dots\}$ and $r \in \mathbb{Z}$, and define

$$C_m(n, r) = \sum_{k \equiv r \ (\mathrm{mod}\ m)} \binom{n}{k} (-1)^k. \tag{1.0}$$

This sum has been studied by various authors and many applications have been found (cf. [S02] and its references). The following well-known observation is fundamental:

$$mC_m(n, r) = \sum_{k=0}^{n} \binom{n}{k} (-1)^k \sum_{\gamma^m = 1} \gamma^{k-r} = \sum_{\gamma^m = 1} \gamma^{-r}(1 - \gamma)^n.$$

Note that

$$C_m(n + 1, r) = C_m(n, r) - C_m(n, r - 1)$$

since $x^{-r}(1 - x)^{n+1} = x^{-r}(1 - x)^n - x^{-r+1}(1 - x)^n$.

Let p be a prime, and let $n \in \mathbb{N}$ and $r \in \mathbb{Z}$. In 1913 A. Fleck (cf. [D, p. 274]) showed that

$$\mathrm{ord}_p(C_p(n, r)) \geqslant \left\lfloor \frac{n - 1}{p - 1} \right\rfloor,$$

where $\mathrm{ord}_p(\alpha)$ denotes the p-adic order of a p-adic number α, and $\lfloor \cdot \rfloor$ is the well-known floor function. Fleck's result is fundamental in the recent investigation of the ψ-operator related to Fontaine's theory, Iwasawa's theory, and p-adic Langlands correspondence (cf. [Co], [SW] and [W]); it also plays an indispensable role in Davis and Sun's study of homotopy exponents of special unitary groups (cf. [DS] and [SD]). In this paper we are interested in the *Fleck quotient*

$$F_p(n, r) := (-p)^{-\lfloor (n-1)/(p-1) \rfloor} C_p(n, r) + [\![n = 0]\!]. \tag{1.1}$$

(Throughout this paper, for an assertion A we let $[\![A]\!]$ take 1 or 0 according as A holds or not.)

For $a \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, we use $\{a\}_m$ to denote the least nonnegative residue of a mod m (thus $\{a\}_m/m$ is the fractional part $\{a/m\}$ of a/m). For a prime p and an integer a, we define $q_p(a) = (a^{p-1} - 1)/p$ which is an integer if $a \not\equiv 0 \pmod{p}$.

By a number-theoretic approach related to Gauss sums, we establish the following explicit result.

Theorem 1.1. *Let p be a prime, and let $n \in \mathbb{N}$ and $r \in \mathbb{Z}$. Set $n_0 = \{n\}_p$ and $n_1 = \{n_0 - n\}_{p-1} = \{-\lfloor n/p \rfloor\}_{p-1}$. If $n_0 \leqslant n_1$, then*

$$F_p(n, r) \equiv \frac{(-1)^{n_1}}{n_1!} \sum_{k=0}^{n_0} \binom{n_0}{k} (-1)^k (k - r)^{n_1} \pmod{p}. \tag{1.2}$$

If $n_0 > n_1 = 0$, *then*

$$F_p(n,r) \equiv (-1)^{\{r\}_p}\binom{n_0}{\{r\}_p} \pmod{p}. \tag{1.3}$$

If $n_0 > n_1 > 0$, *then*

$$F_p(n,r) \equiv \frac{(-1)^{n_1-1}}{(n_1-1)!}\sum_{k=0}^{n_0}\binom{n_0}{k}(-1)^k(k-r)^{n_1}q_p(k-r) \pmod{p}. \tag{1.4}$$

Corollary 1.1. *Let p be a prime and let $n \in \mathbb{N}$ and $r \in \mathbb{Z}$. Then*

$$F_p(pn,r) \equiv \frac{r^{n^*}}{n^*!} \pmod{p} \tag{1.5}$$

where $n^* = \{-n\}_{p-1}$. Consequently,

$$F_p\left(p\frac{p-1}{2},r\right) \equiv \begin{cases} (-1)^{(h(-p)+1)/2}(\frac{r}{p}) \pmod{p} & \text{if } p \neq 3 \ \&\ 4 \mid p+1, \\ (-1)^{(h(p)-1)/2}(\frac{r}{p})\frac{v}{2} \pmod{p} & \text{if } 4 \mid p-1, \end{cases} \tag{1.6}$$

where $(\frac{\cdot}{p})$ is the Legendre symbol, and $h(-p)$ and $h(p)$ are the class numbers of the quadratic fields $\mathbb{Q}(\sqrt{-p})$ and $\mathbb{Q}(\sqrt{p})$ respectively, and for $p \equiv 1 \pmod{4}$ we write the fundamental unit of $\mathbb{Q}(\sqrt{p})$ in the form $(v+u\sqrt{p})/2$ with $u,v \in \mathbb{Z}$ and $u \equiv v \pmod{2}$.

Proof. Note that $\{pn\}_p = 0$. By Theorem 1.1,

$$F_p(pn,r) \equiv \frac{(-1)^{n^*}}{n^*!}\sum_{k=0}^{0}\binom{0}{k}(-1)^k(k-r)^{n^*} = \frac{r^{n^*}}{n^*!} \pmod{p}.$$

When $p \neq 2$ and $n = (p-1)/2$, we have $n^* = (p-1)/2$ and hence

$$\begin{aligned} F_p\left(p\frac{p-1}{2},r\right) &\equiv r^{(p-1)/2}(-1)^{(p-1)/2}\frac{((p-1)/2)!}{\prod_{k=1}^{(p-1)/2}k(p-k)} \\ &\equiv \left(\frac{r}{p}\right)(-1)^{(p-1)/2}\frac{((p-1)/2)!}{(p-1)!} \text{ (by Euler's criterion)} \\ &\equiv (-1)^{(p+1)/2}\left(\frac{r}{p}\right)\frac{p-1}{2}! \pmod{p} \text{ (by Wilson's theorem).} \end{aligned}$$

If $p > 3$ and $p \equiv 3 \pmod{4}$, then

$$\frac{p-1}{2}! \equiv (-1)^{(h(-p)+1)/2} \pmod{p}$$

by a result of L. J. Mordell [M]. When $p \equiv 1 \pmod 4$ and $\varepsilon_p = (v + u\sqrt{p})/2 > 1$ is the fundamental unit of $\mathbb{Q}(\sqrt{p})$ with $u, v \in \mathbb{Z}$ and $u \equiv v \pmod 2$, by S. Chowla [C] we have

$$\frac{p-1}{2}! \equiv (-1)^{(h(p)+1)/2}\,\frac{v}{2} \pmod p.$$

Combining the above we immediately obtain (1.6). □

Remark. Let n be a positive integer and $p > 2n+1$ be a prime. By the first part of Corollary 1.1 in the case $r = 0$, we have

$$\binom{2pn}{pn}(-1)^n + 2\sum_{k=0}^{n-1}\binom{2pn}{pk}(-1)^k = \sum_{k=0}^{2n}\binom{2pn}{pk}(-1)^{pk} \equiv 0 \pmod{p^{2n+1}}$$

and hence

$$\binom{2pn-1}{pn-1} = \frac{1}{2}\binom{2pn}{pn} \equiv \sum_{k=0}^{n-1}(-1)^{n-1-k}\binom{2pn}{pk} \pmod{p^{2n+1}}. \tag{1.7}$$

When $n = 1$ and $p > 3$, this gives the Wolstenholme congruence

$$\frac{1}{2}\binom{2p}{p} = \binom{2p-1}{p-1} \equiv 1 \pmod{p^3}.$$

When $n = 2$ and $p > 5$, (1.7) yields the following new congruence

$$\binom{4p-1}{2p-1} = \frac{1}{2}\binom{4p}{2p} \equiv \binom{4p}{p} - 1 \pmod{p^5}.$$

Our second approach to Fleck quotients is of combinatorial nature. It involves Stirling numbers of the second kind as well as higher-order Bernoulli polynomials.

Let $n \in \mathbb{N}$. The Stirling numbers $S(n,k)$ $(k \in \mathbb{N})$ of the second kind are given by

$$x^n = \sum_{k \in \mathbb{N}} S(n,k)(x)_k,$$

where

$$(x)_0 = 1 \quad\text{and}\quad (x)_k = x(x-1)\cdots(x-k+1) \text{ for } k = 1, 2, \ldots.$$

Clearly, $S(n,n) = 1$, and $S(n,k) = 0$ if $k > n$. When $n + k > 0$, $S(n,k)$ is actually the number of ways to partition a set of cardinality n into k

nonempty subsets. Here is an explicit formula (cf. [LW, p. 126]) for Stirling numbers of the second kind:

$$S(n,k)=\frac{1}{k!}\sum_{j=0}^{k}\binom{k}{j}(-1)^{k-j}j^n.$$

As $S(i,k)=0$ for all those $i\in\mathbb{N}$ with $i<k$, we have *Euler's identity*

$$\sum_{j=0}^{k}\binom{k}{j}(-1)^jP(j)=0,$$

where $P(x)$ is any polynomial with $\deg P<k$ having complex number coefficients. It is known (cf. [LW, p. 126]) that

$$\sum_{n=k}^{\infty}S(n,k)\frac{x^n}{n!}=\frac{(e^x-1)^k}{k!};$$

in other words,

$$(e^x-1)^k=\sum_{n=k}^{\infty}\bar{S}(n,k)x^n \quad\text{with}\quad \bar{S}(n,k)=\frac{k!}{n!}S(n,k).$$

For $m=0,1,\dots$, the m-th order Bernoulli polynomials $B_n^{(m)}(t)$ $(n\in\mathbb{N})$ are defined by

$$\frac{x^me^{tx}}{(e^x-1)^m}=\sum_{n=0}^{\infty}B_n^{(m)}(t)\frac{x^n}{n!},\tag{1.8}$$

and those $B_n^{(m)}=B_n^{(m)}(0)$ are called the m-th order Bernoulli numbers. The usual Bernoulli polynomials and numbers are $B_n(t)=B_n^{(1)}(t)$ and $B_n=B_n(0)=B_n^{(1)}$ respectively. (It is well known that $B_0=1$, $B_1=-1/2$ and $B_{2k+1}=0$ for $k=1,2,\dots$; the reader may consult [IR, pp. 228–248] for the basic properties of Bernoulli numbers.) For a formal power series $f(x)=\sum_{n=0}^{\infty}a_nx^n$, we use $[x^n]f(x)$ to denote the coefficient a_n of the monomial x^n in $f(x)$. Thus

$$\begin{aligned}B_n^{(m)}(t)=&[x^n]n!\left(\frac{x}{e^x-1}\right)^m e^{tx}\\ =&[x^n]n!\sum_{k=0}^{\infty}B_k^{(m)}\frac{x^k}{k!}\sum_{j=0}^{\infty}\frac{(tx)^j}{j!}=\sum_{k=0}^{n}\binom{n}{k}B_k^{(m)}t^{n-k}.\end{aligned}$$

It is also easy to verify that $B_n^{(m)}(m-t)=(-1)^nB_n^{(m)}(t)$, and

$$\frac{B_n^{(m)}(t)}{n!}=\sum_{k_0+\cdots+k_{m-1}=n}\frac{B_{k_0}(t)}{k_0!}\prod_{0<i<m}\frac{B_{k_i}}{k_i!}\quad\text{provided } m>0.$$

If $0\leqslant n<p-1$, then $B_0,\ldots,B_n$ are p-adic integers by the von Staudt-Clausen theorem (cf. [IR, p. 233]) or the recurrence $\sum_{k=0}^{l}\binom{l+1}{k}B_k=0$ ($l=1,2,\ldots$), therefore $B_n^{(m)}(t)\in\mathbb{Z}_p[t]$ where $\mathbb{Z}_p$ is the ring of p-adic integers.

Our discovery of the next theorem was actually motivated by Theorem 1.1.

Theorem 1.2. *Let p be a prime, and let $n\in\mathbb{N}$ and $r\in\mathbb{Z}$. Set $n^*=\{-n\}_{p-1}$. For any integer $m\equiv n \pmod p$, if $m\geqslant 0$ then $(-1)^nF_p(n,r)$ is congruent to*

$$\begin{aligned}\sum_{k=0}^{n^*}\bar S(n^*-k+m,m)\frac{(-r)^k}{k!}=&\sum_{k=0}^{n^*}\bar S(m+n^*,m+k)\binom{-r}{k}\\=&\sum_{k=0}^{m}\binom{m}{k}(-1)^{m-k}\frac{(k-r)^{m+n^*}}{(m+n^*)!}\end{aligned}\tag{1.9}$$

modulo p; if $m\leqslant 0$ then we have

$$F_p(n,r)\equiv\frac{(-1)^{n^*}}{n^*!}B_{n^*}^{(-m)}(-r)\equiv-(p-1-n^*)!B_{n^*}^{(-m)}(-r)\pmod p.\tag{1.10}$$

The following consequence determines $B_n^{(m)}(a)$ modulo a prime p for $m\in\{1,\ldots,p\}$, $n\in\{0,\ldots,p-2\}$ and $a\in\mathbb{Z}$.

Corollary 1.2. *Let p be a prime and $r\in\mathbb{Z}$. Let $n_0\in\{0,\ldots,p-1\}$ and $n_1\in\{0,\ldots,p-2\}$. If $n_0\leqslant n_1$, then*

$$B_{n_1-n_0}^{(p-n_0)}(-r)\equiv\frac{1}{(n_1)_{n_0}}\sum_{k=0}^{n_0}\binom{n_0}{k}(-1)^{n_0-k}(k-r)^{n_1}\pmod p.\tag{1.11}$$

If $n_0>n_1=0$, then

$$B_{p-n_0+n_1-1}^{(p-n_0)}(-r)\equiv\frac{(-1)^{\{r\}_p-1}}{n_0!}\binom{n_0}{\{r\}_p}\pmod p.\tag{1.12}$$

If $n_0>n_1>0$, then

$$\begin{aligned}B_{p-n_0+n_1-1}^{(p-n_0)}(-r)\equiv&\frac{(-1)^{n_1}}{(n_0-n_1)!(n_1-1)!}\\&\times\sum_{k=0}^{n_0}\binom{n_0}{k}(-1)^k(k-r)^{n_1}q_p(k-r)\pmod p.\end{aligned}\tag{1.13}$$

Proof. Let n be a nonnegative integer with $n \equiv n_0 - pn_1 \pmod{p(p-1)}$. Applying (1.10) with $m = n_0 - p$ we obtain

$$F_p(n,r) \equiv \frac{(-1)^{n^*}}{n^*!} B_{n^*}^{(p-n_0)}(-r) \equiv -(p-1-n^*)! B_{n^*}^{(p-n_0)}(-r) \pmod p,$$

where $n^* = \{-n\}_{p-1}$.

If $n_0 \leqslant n_1$, then $n^* = n_1 - n_0$ and hence

$$B_{n_1-n_0}^{(p-n_0)}(-r) \equiv (-1)^{n_1-n_0}(n_1-n_0)! F_p(n,r) \pmod p,$$

which implies (1.11) with the help of (1.2).

Now we consider the case $n_0 > n_1$. Clearly $n^* = n_1 - n_0 + p - 1$ and $p - 1 - n^* = n_0 - n_1$. Therefore

$$F_p(n,r) \equiv -(n_0 - n_1)! B_{n_1-n_0+p-1}^{(p-n_0)}(-r) \pmod p.$$

The case $n_1 = 0$ of this, together with (1.3), yields (1.12). When $n_1 > 0$, combining the last congruence with (1.4) we obtain (1.13). □

Corollary 1.3. *Let p be a prime and let $n \in \mathbb{Z}^+$. Then* $\operatorname{ord}_p(C_p(n,r)) = \lfloor (n-1)/(p-1) \rfloor$ *for at least $p - n^* \geqslant 2$ values of $r \in \{0, \ldots, p-1\}$, where $n^* = \{-n\}_{p-1}$.*

Proof. For any $r \in \mathbb{Z}$, $\operatorname{ord}_p(C_p(n,r)) = \lfloor (n-1)/(p-1) \rfloor$ if and only if $F_p(n,r) \not\equiv 0 \pmod p$. By Theorem 1.2,

$$F_p(n,r) \equiv \frac{(-1)^{n^*}}{n^*!} B_{n^*}^{(p-\{n\}_p)}(-r) \pmod p \quad \text{for all } r = 0, \ldots, p-1.$$

Recall that $B_{n^*}^{(p-\{n\}_p)}(x) \in \mathbb{Z}_p[x]$ is monic and of degree n^*. Also, a polynomial of degree n^* over the field $\mathbb{Z}/p\mathbb{Z}$ cannot have more than n^* distinct zeroes in the field (cf. [IR, p. 39]). So the congruence equation $F_p(n,r) \equiv 0 \pmod p$ has at most n^* solutions with $r \in \{0, \ldots, p-1\}$. This yields the desired result. □

Corollary 1.4. *Let p be a prime, and let $n \in \mathbb{N}$ and $n^* = \{-n\}_{p-1}$. Then*

$$(-1)^n F_p(n,0) \equiv \bar{S}(n^* + \{n\}_p, \{n\}_p) \equiv \frac{B_{n^*}^{(m)}}{n^*!} \pmod p, \tag{1.14}$$

where m is any nonnegative integer with $m + n \equiv 0 \pmod p$. Also,

$$(-1)^n F_p(pn+p-1,r) \equiv \frac{B_{n^*}(-r)}{n^*!} \equiv -(p-1-n^*)! B_{n^*}(r+1) \pmod p \tag{1.15}$$

for all $r\in\mathbb{Z}$, and in particular

$$\binom{2p-1}{p+r}+(-1)^p\binom{2p-1}{r}\equiv(-1)^r p^2 B_{p-2}(-r)\ (\mathrm{mod}\ p^3) \qquad (1.16)$$

for every $r=0,\ldots,p-1$.

Proof. Applying Theorem 1.2 with $r=0$ we immediately get (1.14).

As $pn+p-1\equiv-1\ (\mathrm{mod}\ p)$ and $n^*=\{-(pn+p-1)\}_{p-1}$, by the second part of Theorem 1.2 and the identity $(-1)^{n^*}B_{n^*}(x)=B_{n^*}(1-x)$, whenever $r\in\mathbb{Z}$ we have

$$\begin{aligned}(-1)^{n^*}F_p(pn+p-1,r)\equiv&\frac{B_{n^*}(-r)}{n^*!}\equiv(-1)^{n^*+1}(p-1-n^*)!B_{n^*}(-r)\\ \equiv&-(p-1-n^*)!B_{n^*}(r+1)\ (\mathrm{mod}\ p)\end{aligned}$$

and hence (1.15) holds.

Now let $r\in\{0,\ldots,p-1\}$. By (1.15) in the case $n=1$,

$$-F_p(2p-1,r)\equiv-(p-1-(p-2))!B_{p-2}(r+1)\ (\mathrm{mod}\ p)$$

and hence

$$F_p(2p-1,r)\equiv B_{p-2}(1-(-r))=(-1)^{p-2}B_{p-2}(-r)\ (\mathrm{mod}\ p)$$

which is equivalent to (1.16). We are done. □

Let p be an odd prime, and let h_p and h_p^+ denote the class numbers of the cyclotomic field $\mathbb{Q}(\zeta_p)$ and its maximal real subfield $\mathbb{Q}(\zeta_p+\zeta_p^{-1})$ respectively, where ζ_p is a primitive p-th root of unity in the complex field $\mathbb{C}$. It is well known that $h_p^-=h_p/h_p^+$ is an integer. If p divides none of the numerators of the Bernoulli numbers $B_0,B_2,\ldots,B_{p-3}\in\mathbb{Z}_p$, then p is said to be a *regular* prime. In 1850 E. Kummer proved that

$$\begin{aligned}p\nmid h_p\iff p\nmid h_p^-\iff&\ p\text{ is regular}\\ \Longrightarrow&\ x^p+y^p=z^p\text{ has no integer solution with }xyz\neq0.\end{aligned}$$

Furthermore,

$$h_p^-\equiv\prod_{0<n\leqslant(p-3)/2}\left(-\frac{B_{2n}}{4n}\right)\ (\mathrm{mod}\ p)$$

by the proof of Theorem 5.16 in [Wa, p. 62].

Corollary 1.5. *Let p be a prime.*

(i) *For every $n = 2, \ldots , p$ we have*

$$\sum_{k=1}^{n}(-1)^{pk-1}\binom{pn-1}{pk-1} \equiv (n-1)!B_{p-n}p^n \pmod{p^{n+1}}. \tag{1.17}$$

(ii) *Suppose that $p > 3$. Then p does not divide the class number h_p of the p-th cyclotomic field $\mathbb{Q}(\zeta_p)$, if and only if*

$$\mathrm{ord}_p\bigg(\sum_{k=1}^{n}(-1)^k\binom{pn-1}{pk-1}\bigg) = n \quad \text{for all } n = 3, 5, \ldots , p-2.$$

Also,

$$\begin{aligned}&\sum_{k=1}^{(p-1)/2}(-1)^{k-1}\binom{p(p-1)/2-1}{pk-1}\\ \equiv&[\![4 \mid p+1]\!](-1)^{(h(-p)+1)/2}h(-p)p^{(p-1)/2} \ \left(\mathrm{mod}\ p^{(p+1)/2}\right),\end{aligned} \tag{1.18}$$

where $h(-p)$ is the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$.

Proof. (i) Let $n \in \{2, \ldots , p\}$. Then $\lfloor (pn-1-1)/(p-1)\rfloor = n$ and hence

$$F_p(pn-1,-1) = (-p)^{-n}C_p(pn-1,-1) = (-p)^{-n}\sum_{k=1}^{n}\binom{pn-1}{pk-1}(-1)^{pk-1}.$$

By Corollary 1.4, $(-1)^nF_p(pn-1,-1)$ is congruent to

$$(p-1-\{-(n-1)\}_{p-1})!B_{\{-(n-1)\}_{p-1}}(-1+1) = (n-1)!B_{p-n}$$

modulo p. Therefore (1.17) holds.

(ii) In view of part (i),

$$\begin{aligned}&\mathrm{ord}_p\bigg(\sum_{k=1}^{n}(-1)^k\binom{pn-1}{pk-1}\bigg) = n \quad \text{for } n = 3, 5, \ldots , p-2\\ \iff& B_{p-n} \not\equiv 0 \pmod p \quad \text{for } n = 3, 5, \ldots , p-2\\ \iff& p \text{ is regular}\\ \iff& h_p \not\equiv 0 \pmod p.\end{aligned}$$

Taking $n = (p-1)/2$ in (1.17) we get

$$\begin{aligned}&\sum_{k=1}^{(p-1)/2}(-1)^{k-1}\binom{p(p-1)/2-1}{pk-1}\\ \equiv&\frac{((p-1)/2)!}{(p-1)/2}p^{(p-1)/2}B_{(p+1)/2} \ \left(\mathrm{mod}\ p^{(p+1)/2}\right).\end{aligned}$$

If $p \equiv 1 \pmod 4$, then $B_{(p+1)/2} = 0$ since $(p+1)/2 \in \{3,5,\ldots\}$. If $p \equiv 3 \pmod 4$, then $h(-p) \equiv -2B_{(p+1)/2} \pmod p$ (cf. [IR, p. 238]), and $((p-1)/2)! \equiv (-1)^{(h(-p)+1)/2} \pmod p$ by Mordell [M]. So (1.18) follows from the above. This concludes the proof. □

Remark. Let p be an odd prime. If $p \geqslant 5$, then (1.17) in the case $n=2$ reduces to Wolstenholme's congruence $\binom{2p-1}{p-1} \equiv 1 \pmod{p^3}$ since $B_{p-2} = 0$. Taking $n=3$ in (1.17) we get

$$\binom{3p-1}{p-1} - \binom{3p-1}{2p-1} + \binom{3p-1}{3p-1} \equiv 2B_{p-3}p^3 \pmod{p^4};$$

as $\binom{3p-1}{2p-1} = 2\binom{3p-1}{p-1}$ this yields the congruence

$$\binom{3p-1}{p-1} \equiv 1 - 2p^3 B_{p-3} \pmod{p^4}.$$

This was first obtained by J.W.L. Glaisher (cf. [G1, p. 21] and [G2, p. 323]) who showed that

$$\binom{pn-1}{p-1} \equiv 1 - \frac{n(n-1)}{3}p^3 B_{p-3} \pmod{p^4} \quad \text{for } n = 1,2,3,\ldots.$$

Corollary 1.6. *Let p be an odd prime, and let $n \in \{3,\ldots,p\}$ and $r \in \mathbb{Z}$. Then*

$$F_p(pn-2,r) \equiv -n!\left(\frac{B_{p-n+1}(-r)}{n-1} + (r+1)\frac{B_{p-n}(-r)}{n}\right) \pmod p. \quad (1.19)$$

Proof. Clearly $\{-(pn-2)\}_{p-1} = p-n+1$. By Theorem 1.2, $F_p(pn-2,r)$ is congruent to

$$-(p-1-(p-n+1))!B^{(2)}_{p-n+1}(-r) = -(n-2)!B^{(2)}_{p-n+1}(-r)$$

modulo p.

Let $m = p-n+1$. By [PS, (2.14)] or [SP, (1.12)],

$$\begin{aligned}
&\frac{(-1)^m}{m}\sum_{k=0}^{m}\binom{m}{k}B_k B_{m-k}(x) - \frac{B_m(1-x)}{m}B_0 \\
=&-\sum_{k=0}^{1}\binom{1}{k}B_{1-k}(x)B_{m-1+k}(1-x) - B_1B_{m-1}(1-x) \\
=&-B_1(x)B_{m-1}(1-x) - B_0(x)B_m(1-x) - B_1B_{m-1}(1-x) \\
=&(-1)^m\left((B_1(x)+B_1)B_{m-1}(x) - B_m(x)\right) \\
=&(-1)^m\left((x-1)B_{m-1}(x) - B_m(x)\right).
\end{aligned}$$

It follows that

$$\begin{aligned}B_m^{(2)}(-r) =&\sum_{k=0}^{m}\binom{m}{k}B_kB_{m-k}(-r)\\ =&(1-m)B_m(-r)+m(-r-1)B_{m-1}(-r)\\ \equiv&(1+n-1)B_{p-n+1}(-r)-(r+1)(-n+1)B_{p-n}(-r)\\ \equiv&n(n-1)\left(\frac{B_{p-n+1}(-r)}{n-1}+(r+1)\frac{B_{p-n}(-r)}{n}\right)\pmod p.\end{aligned}$$

Combining the above we immediately obtain (1.19). □

By Theorem 1.1 or 1.2, for any prime p the Fleck quotient $F_p(n,r)$ (with $n\in\mathbb{N}$ and $r\in\mathbb{Z}$) modulo p only depends on p and r and the remainder of n modulo $p(p-1)$. This observation can be further extended as follows.

Theorem 1.3. *Let p be a prime, and let $a,l,n\in\mathbb{N}$ and $r\in\mathbb{Z}$. Then*

$$\begin{aligned}&\sum_{k=0}^{n}\binom{n}{k}(-1)^kF_p\left(kp^a(p-1)+l,r\right)\\ &\equiv 0 \left(\bmod p^{an+\lceil (n-l^*)/(p-1)\rceil}\right),\end{aligned}\tag{1.20}$$

where $l^*=\{-l\}_{p-1}$ and $\lceil\cdot\rceil$ is the ceiling function.

The following consequence is somewhat similar to Kummer's congruence for Bernoulli numbers (cf. [IR, pp. 238–241]).

Corollary 1.7. *Let p be a prime, and let $a,l\in\mathbb{N}$ and $r\in\mathbb{Z}$. Then*

$$\begin{aligned}F_p(p^a(p-1)+l,r)\equiv&F_p(l,r)\pmod{p^a},\\ F_p(2p^a(p-1)+l,r)\equiv&2F_p(p^a(p-1)+l,r)-F_p(l,r)\pmod{p^{2a}},\\ F_p(3p^a(p-1)+l,r)\equiv&3F_p(2p^a(p-1)+l,r)-3F_p(p^a(p-1)+l,r)\\ &+F_p(l,r)\pmod{p^{3a}}.\end{aligned}$$

Proof. Simply apply (1.20) with $n=1,2,3$. □

Let p be a prime, and let $a\in\mathbb{Z}^+$ and $r\in\mathbb{Z}$. In 1977 C. S. Weisman [We] extended Fleck's result by showing that if $n\geqslant p^{a-1}$ then

$$C_{p^a}(n,r)\equiv 0\left(\bmod p^{\lfloor (n-p^{a-1})/\varphi(p^a)\rfloor}\right),$$

where φ is Euler's totient function. In view of this, we define the *generalized Fleck quotient*

$$F_{p^a}(n,r)=(-p)^{-\lfloor (n-p^{a-1})/\varphi(p^a)\rfloor}C_{p^a}(n,r)+[\![n<p^{a-1}]\!]\in\mathbb{Z}.$$

Note that $F_{p^a}(n,r)\equiv 1\pmod p$ for $n=0,\dots,p^{a-1}-1$.

Theorem 1.4. *Let p be a prime, and let $a, n \in \mathbb{Z}^+$ with $n \geqslant p^{a-1}$.*

(i) *For any $r \in \mathbb{Z}$ we have*

$$F_{p^a}(n,r) \equiv \sum_{k=0}^{d} \binom{r+k-1}{k} F_{p^a}(n+k,0) \pmod{p}, \tag{1.21}$$

where $d = \{p^{a-1}-1-n\}_{\varphi(p^a)}$ is the least nonnegative integer with $n+d \equiv p^{a-1}-1 \pmod{\varphi(p^a)}$.

(ii) *We have*

$$\operatorname{ord}_p\left(C_{p^a}(n,r)\right) = \left\lfloor \frac{n-p^{a-1}}{\varphi(p^a)} \right\rfloor \ (i.e.,\ p \nmid F_{p^a}(n,r)) \quad \text{for some } r \in \mathbb{Z}. \tag{1.22}$$

If $n \geqslant 2p^{a-1}$, then

$$F_{p^a}\left(n + p^a(p-1), r\right) \equiv F_{p^a}(n,r) \pmod{p} \quad \text{for all } r \in \mathbb{Z}. \tag{1.23}$$

In view of the first congruence in Corollary 1.7 and the last congruence in Theorem 1.4, we propose the following conjecture.

Conjecture 1.1. *Let p be a prime, and let $a, b, n \in \mathbb{Z}^+$ and $r \in \mathbb{Z}$. If $n \geqslant 2p^{a+b-2}$, then*

$$F_{p^a}\left(n + \varphi(p^{a+b}), r\right) \equiv F_{p^a}(n,r) \pmod{p^b}.$$

Theorems 1.1, 1.2 and 1.3 will be proved in Sections 2, 3 and 4 respectively. In Section 5 we will first give a new proof of Weisman's congruence via roots of unity, and then establish Theorem 1.4.

2. Proof of Theorem 1.1

Lemma 2.1. *Let p be a prime, and let $n \in \mathbb{N}$ and $n^* = \{-n\}_{p-1}$. Define $G(n) = \sum_{a=1}^{p-1} a^n \zeta_p^a$ and $\pi = 1 - \zeta_p$, where ζ_p is a primitive p-th root of unity in the complex field $\mathbb{C}$. Then*

$$G(n) \equiv (-1)^{n^*-1} \sum_{m=n^*}^{p-2} s(m,n^*) \frac{\pi^m}{m!} \pmod{p}, \tag{2.1}$$

where $s(m,0), \ldots, s(m,m)$ are Stirling numbers of the first kind defined by $(x)_m = \sum_{k=0}^{m} (-1)^{m-k} s(m,k) x^k$.

Proof. Clearly,

$$\begin{aligned}G(n) =&\sum_{a=1}^{p-1}a^n(1-\pi)^a=\sum_{a=1}^{p-1}a^n\sum_{m=0}^{a}\binom{a}{m}(-\pi)^m\\ =&\sum_{m=0}^{p-1}\frac{(-\pi)^m}{m!}\sum_{a=1}^{p-1}a^n(a)_m\\ =&\sum_{m=0}^{p-1}\frac{(-\pi)^m}{m!}\sum_{a=1}^{p-1}a^n\sum_{k=0}^{m}(-1)^{m-k}s(m,k)a^k\\ =&\sum_{m=0}^{p-1}\frac{(-\pi)^m}{m!}\sum_{k=0}^{m}(-1)^{m-k}s(m,k)\sum_{a=1}^{p-1}a^{n+k}.\end{aligned}$$

Since

$$1+x+\cdots+x^{p-1}=\frac{x^p-1}{x-1}=\prod_{a=1}^{p-1}(x-\zeta_p^a),$$

we have

$$\frac{p}{\pi^{p-1}}=\prod_{a=1}^{p-1}\frac{1-\zeta_p^a}{\pi}=\prod_{a=1}^{p-1}\frac{1-(1-\pi)^a}{\pi}\equiv\prod_{a=1}^{p-1}a\equiv-1\ (\mathrm{mod}\ \pi)$$

with the help of Wilson's theorem. Note also that

$$\sum_{a=1}^{p-1}a^{n+k}\equiv-[\![p-1\mid n+k]\!]\ (\mathrm{mod}\ p)$$

by elementary number theory (see, e.g., [IR, pp. 235–236]). Therefore

$$\begin{aligned}G(n)\equiv&\sum_{m=0}^{p-2}\frac{\pi^m}{m!}\sum_{k=0}^{m}(-1)^k s(m,k)(-[\![k=n^*]\!])\\ \equiv&(-1)^{n^*-1}\sum_{m=n^*}^{p-2}s(m,n^*)\frac{\pi^m}{m!}\ (\mathrm{mod}\ p).\end{aligned}$$

This concludes the proof. □

Remark. Let p be an odd prime. For each $a\in\mathbb{Z}$ let $\bar{a}=a+p\mathbb{Z}\in\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$. Let ω be the Teichmüller character of the multiplicative group $\mathbb{F}_p^*=\mathbb{F}_p\setminus\{\bar{0}\}$. For $\bar{a}\in\mathbb{F}_p^*$, $\omega(\bar{a})$ is just the $(p-1)$-th root of unity in the unique unramified extension of the p-adic field $\mathbb{Q}_p$ with $\omega(\bar{a})\equiv a\ (\mathrm{mod}\ p)$. (See, e.g., [Wa, p. 51].) If ζ_p is a primitive p-th root of unity in the algebraic closure of $\mathbb{Q}_p$, then for $n\in\mathbb{N}$ and $\pi=1-\zeta_p$ we have

$$\sum_{a=1}^{p-1}a^n\zeta_p^a\equiv\sum_{a=1}^{p-1}\omega^n(\bar{a})\zeta_p^a\equiv-\frac{(-\pi)^{n^*}}{n^*!}\ \ (\mathrm{mod}\ \pi^{n^*+1})$$

with $n^*=\{-n\}_{p-1}$, by Stickelberger's congruence for Gauss' sums (cf. [BEW, pp. 344–345]).

Lemma 2.2. *Let p be a prime, and let ζ_p be a primitive p-th root of unity in $\mathbb{C}$. Let $n = p^a m + n_0 > 0$ with $a \in \mathbb{Z}^+$ and $m, n_0 \in \mathbb{N}$. Then, for any $r \in \mathbb{Z}$ we have*

$$\begin{aligned}&\pi^{-p^a m} C_p(n,r) - [\![p-1 \mid m]\!] C_p(n_0, r)\\ \equiv&\frac{G(p^a m)}{p} \sum_{k=0}^{n_0} \binom{n_0}{k} (-1)^k (k-r)^{p^a m^*} \ \left(\text{mod } p^{a-1}\pi^{\min\{n_0+1,\, p-1\}}\right),\end{aligned}$$

where $\pi = 1 - \zeta_p$ and $m^* = \{-m\}_{p-1}$.

Proof. Let $j \in \{1, \ldots, p-1\}$. Then

$$\left(\frac{1-\zeta_p^j}{\pi}\right)^m = \left(\frac{1-(1-\pi)^j}{\pi}\right)^m = \left(\sum_{i=1}^{j} \binom{j}{i} (-\pi)^{i-1}\right)^m = j^m + \beta_j \pi,$$

where β_j is a suitable element in the ring $\overline{\mathbb{Z}}$ of algebraic integers. For $i = 0, 1, \ldots,$ if

$$\left(\frac{1-\zeta_p^j}{\pi}\right)^{p^i m} = j^{p^i m} + p^i \pi \beta_j^{(i)}$$

for some $\beta_j^{(i)} \in \overline{\mathbb{Z}}$, then

$$\left(\frac{1-\zeta_p^j}{\pi}\right)^{p^{i+1} m} = \left(j^{p^i m} + p^i \pi \beta_j^{(i)}\right)^p = j^{p^{i+1} m} + p^{i+1} \pi \beta_j^{(i+1)}$$

for some $\beta_j^{(i+1)} \in \overline{\mathbb{Z}}$. So

$$\left(\frac{1-\zeta_p^j}{\pi}\right)^{p^a m} \equiv j^{p^a m} \ (\text{mod } p^a \pi).$$

Observe that

$$pC_p(n,r) = \sum_{j=0}^{p-1} \zeta_p^{-jr} (1-\zeta_p^j)^n = \pi^{p^a m} \sum_{j=1}^{p-1} \zeta_p^{-jr} \left(\frac{1-\zeta_p^j}{\pi}\right)^{p^a m} (1-\zeta_p^j)^{n_0}.$$

As π^{n_0} divides $(1-\zeta_p^j)^{n_0}$ in the ring $\overline{\mathbb{Z}}$, by the above $\pi^{-p^a m} p C_p(n,r)$ is congruent to

$$\sum_{j=1}^{p-1} \zeta_p^{-jr} j^{p^a m} \sum_{k=0}^{n_0} \binom{n_0}{k} (-1)^k \zeta_p^{jk} = \sum_{k=0}^{n_0} \binom{n_0}{k} (-1)^k S_{k-r}$$

modulo $p^a\pi^{n_0+1}$, where

$$S_{k-r}=\sum_{j=1}^{p-1} j^{p^a m}\zeta_p^{j(k-r)}.$$

If $k\not\equiv r \pmod p$, then

$$\begin{aligned}S_{k-r}=&(k-r)^{-p^a m}\sum_{j=1}^{p-1}(j(k-r))^{p^a m}\zeta_p^{j(k-r)}\\ \equiv&(k-r)^{p^a m^*}\sum_{t=1}^{p-1}t^{p^a m}\zeta_p^t=(k-r)^{p^a m^*}G(p^a m) \pmod{p^{a+1}}.\end{aligned}$$

(Note that if $j(k-r)\equiv t \pmod p$ then $(j(k-r))^{p^a}\equiv t^{p^a} \pmod{p^{a+1}}$.)

Choose a primitive root g modulo p. Since

$$(g^{p^a m}-1)\sum_{j=1}^{p-1}j^{p^a m}=\sum_{j=1}^{p-1}(gj)^{p^a m}-\sum_{t=1}^{p-1}t^{p^a m}\equiv 0 \pmod{p^{a+1}},$$

if $p-1\nmid m$ then $g^{p^a m}-1\not\equiv 0 \pmod p$ and so $\sum_{j=1}^{p-1} j^{p^a m}\equiv 0 \pmod{p^{a+1}}$. Thus, when $k\equiv r \pmod p$ we have

$$S_{k-r}=\sum_{j=1}^{p-1}j^{p^a m}\equiv (p-1)[\![p-1\mid m]\!] \pmod{p^{a+1}}.$$

Recall that $p/\pi^{p-1}\equiv -1 \pmod \pi$. In view of the above,

$$\begin{aligned}&\pi^{-p^a m}pC_p(n,r)-\sum_{k=0}^{n_0}\binom{n_0}{k}(-1)^k(k-r)^{p^a m^*}G(p^a m)\\ \equiv&\sum_{\substack{k=0\\ p\mid k-r}}^{n_0}\binom{n_0}{k}(-1)^k\Big([\![p-1\mid m]\!](p-1)-(k-r)^{p^a m^*}G(p^a m)\Big)\\ \equiv&C_p(n_0,r)[\![p-1\mid m]\!]p \quad \Big(\mathrm{mod}\ p^a\pi^{\min\{n_0+1,\,p-1\}}\Big),\end{aligned}$$

where we have noted that if $p-1\mid m$ (i.e., $m^*=0$) then

$$p-1-G(p^a m)\equiv p-\sum_{t=0}^{p-1}\zeta_p^t=p-\frac{1-\zeta_p^p}{1-\zeta_p}=p \pmod{p^{a+1}}.$$

Therefore the desired congruence follows. □

Proof of Theorem 1.1. In the case $n=0$, (1.2) holds since $n_1=n_0=0$ and $F_p(n,r)=-pC_p(0,r)+1$. Below we assume $n>0$.

Let ζ_p be a primitive p-th root of unity in $\mathbb{C}$, and set $\pi=1-\zeta_p$. By Lemma 2.2 in the case $a=1$,

$$\begin{aligned}&\pi^{-p\lfloor n/p\rfloor}C_p(n,r)-[\![n_1=0]\!]C_p(n_0,r)\\ \equiv&\frac{G(p\lfloor n/p\rfloor)}{p}\sum_{k=0}^{n_0}\binom{n_0}{k}(-1)^k(k-r)^{pn_1}\ \left(\mathrm{mod}\ \pi^{\min\{n_0+1,\,p-1\}}\right).\end{aligned}$$

In view of Lemma 2.1,

$$G\left(p\left\lfloor\frac{n}{p}\right\rfloor\right)\equiv G\left(\left\lfloor\frac{n}{p}\right\rfloor\right)\equiv(-1)^{n_1-1}\sum_{m=n_1}^{p-2}s(m,n_1)\frac{\pi^m}{m!}\ (\mathrm{mod}\ p).$$

If $n_0>n_1$, then

$$\sum_{k=0}^{n_0}\binom{n_0}{k}(-1)^k(k-r)^{pn_1}\equiv\sum_{k=0}^{n_0}\binom{n_0}{k}(-1)^k(k-r)^{n_1}=0\ (\mathrm{mod}\ p),$$

where we have applied Fermat's little theorem and Euler's identity (mentioned in Section 1). Therefore

$$\begin{aligned}&\pi^{-p\lfloor n/p\rfloor}C_p(n,r)-[\![n_1=0]\!]C_p(n_0,r)\\ \equiv&\frac{(-1)^{n_1-1}}{p}\sum_{m=n_1}^{p-2}s(m,n_1)\frac{\pi^m}{m!}\sum_{k=0}^{n_0}\binom{n_0}{k}(-1)^k(k-r)^{pn_1}\\ &\qquad\left(\mathrm{mod}\ \pi^{[\![n_0>n_1]\!]\min\{n_0+1,\,p-1\}}\right).\end{aligned}$$

Recall that $-p/\pi^{p-1}\equiv 1\ (\mathrm{mod}\ \pi)$. Since $s(n_1,n_1)=1$ and

$$\frac{p^{[\![n_0\leqslant n_1]\!]}}{\pi^{n_1}}\pi^{[\![n_0>n_1]\!]\min\{n_0+1,\,p-1\}}\equiv 0\ (\mathrm{mod}\ \pi),$$

by the above we have

$$\begin{aligned}&\frac{p^{[\![n_0\leqslant n_1]\!]}C_p(n,r)}{\pi^{p\lfloor n/p\rfloor+n_1}}-p^{[\![n_0=0]\!]}[\![n_1=0]\!]C_p(n_0,r)\\ \equiv&\frac{(-1)^{n_1-1}/n_1!}{p^{[\![n_0>n_1]\!]}}\sum_{k=0}^{n_0}\binom{n_0}{k}(-1)^k(k-r)^{pn_1}\ (\mathrm{mod}\ \pi).\end{aligned}$$

Note that

$$\left\lfloor\frac{n-1}{p-1}\right\rfloor=\left\lfloor\frac{p\lfloor n/p\rfloor+n_0-1}{p-1}\right\rfloor=\frac{p\lfloor n/p\rfloor+n_1}{p-1}-[\![n_0\leqslant n_1]\!]$$

and hence

$$\begin{aligned}\frac{(-p)^{[\![n_0\leqslant n_1]\!]}C_p(n,r)}{\pi^{p\lfloor n/p\rfloor+n_1}}=&\frac{C_p(n,r)}{(-p)^{\lfloor (n-1)/(p-1)\rfloor}}\left(\frac{-p}{\pi^{p-1}}\right)^{(p\lfloor n/p\rfloor+n_1)/(p-1)}\\ \equiv&F_p(n,r)\pmod{\pi}.\end{aligned}$$

In view of the above,

$$\begin{aligned}&(-1)^{[n_0\leqslant n_1]}F_p(n,r)-[\![n_0>n_1=0]\!]C_p(n_0,r)\\ \equiv&\frac{(-1)^{n_1-1}/n_1!}{p^{[\![n_0>n_1]\!]}}\sum_{k=0}^{n_0}\binom{n_0}{k}(-1)^k(k-r)^{pn_1}\pmod{\pi}.\end{aligned}$$

As the rational p-adic integer

$$\begin{aligned}D=&F_p(n,r)-[\![n_0>n_1=0]\!]C_p(n_0,r)\\ &-\frac{(-1)^{n_1}}{(-p)^{[\![n_0>n_1]\!]}\cdot n_1!}\sum_{k=0}^{n_0}\binom{n_0}{k}(-1)^k(k-r)^{pn_1}\end{aligned}$$

is divisible by π, we have $D^{p-1}\equiv 0\pmod{p}$ and hence $D\equiv 0\pmod{p}$. Thus

$$\begin{aligned}&F_p(n,r)-[\![n_0>n_1=0]\!]C_p(n_0,r)\\ \equiv&\frac{(-1)^{n_1}}{(-p)^{[\![n_0>n_1]\!]}\cdot n_1!}\sum_{k=0}^{n_0}\binom{n_0}{k}(-1)^k(k-r)^{pn_1}\pmod{p}.\end{aligned}\tag{2.2}$$

In the case $n_0\leqslant n_1$, (2.2) reduces to (1.2). When $n_0>n_1=0$, (2.2) yields (1.3) since $C_p(n_0,r)=(-1)^{\{r\}_p}\binom{n_0}{\{r\}_p}$ and $\sum_{k=0}^{n_0}\binom{n_0}{k}(-1)^k=(1-1)^{n_0}=0$.

Now assume that $n_0>n_1>0$. As $\sum_{k=0}^{n_0}\binom{n_0}{k}(k-r)^{n_1}=0$ by Euler's identity, (2.2) implies that

$$F_p(n,r)\equiv\frac{(-1)^{n_1-1}}{n_1!}\sum_{k=0}^{n_0}\binom{n_0}{k}(-1)^k\frac{(k-r)^{pn_1}-(k-r)^{n_1}}{p}\pmod{p}.$$

If $n_1=1$, then

$$\frac{(k-r)^{pn_1}-(k-r)^{n_1}}{p}=(k-r)^{n_1}n_1q_p(k-r);$$

if $n_1\geqslant 2$ and $k\equiv r\pmod{p}$, then

$$\frac{(k-r)^{pn_1}-(k-r)^{n_1}}{p}\equiv 0\equiv(k-r)^{n_1}n_1q_p(k-r)\pmod{p};$$

if $a=k-r\not\equiv 0\pmod{p}$, then

$$\frac{(k-r)^{pn_1}-(k-r)^{n_1}}{p}=a^{n_1}\frac{(1+p\cdot q_p(a))^{n_1}-1}{p}\equiv a^{n_1}n_1q_p(a)\pmod{p}.$$

Therefore (1.4) follows.

The proof is now complete. $\square$

3. Proof of Theorem 1.2

The following lemma is a refinement of an induction technique used by Sun [S06].

Lemma 3.1. *Let p be a prime, and let $n \in \mathbb{N}$ with $n \geqslant p$. Then*

$$F_p(n,r) \equiv -\sum_{j=1}^{p-1} \frac{1}{j} \sum_{i=0}^{j-1} F_p(n-p+1, r-i) \pmod{p}. \tag{3.1}$$

Proof. Set $n' = n-(p-1) > 0$. By the Chu-Vandermonde convolution identity (cf. [GKP, (5.27)]),

$$\begin{aligned} F_p(n,r) =& (-p)^{-\lfloor (n-1)/(p-1) \rfloor} \sum_{\substack{0 \leqslant k \leqslant n \\ k \equiv r \pmod{p}}} \sum_{j=0}^{k} \binom{p-1}{j} \binom{n'}{k-j} (-1)^k \\ =& -\frac{1}{p} \sum_{j=0}^{p-1} \binom{p-1}{j} (-p)^{-\lfloor (n'-1)/(p-1) \rfloor} \sum_{\substack{j \leqslant k \leqslant n \\ p \mid k-r}} \binom{n'}{k-j} (-1)^k \\ =& -\frac{1}{p} \sum_{j=0}^{p-1} \binom{p-1}{j} (-1)^j F_p(n', r-j). \end{aligned}$$

For any $j = 0, \ldots, p-1$, clearly

$$\begin{aligned} \binom{p-1}{j}(-1)^j =& \prod_{0<i\leqslant j} \left(1 - \frac{p}{i}\right) \\ \equiv& 1 - \sum_{0<i\leqslant j} \frac{p}{i} \equiv (-1)^{p-1} + p \sum_{j<k<p} \frac{1}{k} \pmod{p^2}. \end{aligned}$$

(Note that $2\sum_{k=1}^{p-1} 1/k = \sum_{k=1}^{p-1}(1/k + 1/(p-k)) \equiv 0 \pmod{p}$.) Also,

$$\sum_{j=0}^{p-1} F_p(n', r-j) = (-p)^{-\lfloor (n'-1)/(p-1) \rfloor} \sum_{k=0}^{n'} \binom{n'}{k} (-1)^k = 0.$$

Therefore

$$F_p(n,r) \equiv -\sum_{j=0}^{p-1} \sum_{j<k<p} \frac{F_p(n', r-j)}{k} = -\sum_{k=1}^{p-1} \frac{1}{k} \sum_{j=0}^{k-1} F_p(n', r-j) \pmod{p}.$$

This proves (3.1). $\square$

Proof of Theorem 1.2. (i) Suppose $m \geqslant 0$. Then

$$\begin{aligned}&\sum_{k=0}^{n^*}\bar{S}(m+n^*-k,m)\frac{(-r)^k}{k!}\\ =&[x^{m+n^*}]\sum_{l=m}^{\infty}\bar{S}(l,m)x^l\sum_{k=0}^{\infty}\frac{(-rx)^k}{k!}\\ =&[x^{m+n^*}](e^x-1)^m e^{-rx}=[x^{n^*}]\left(\frac{e^x-1}{x}\right)^m e^{-rx}\\ =&[x^{m+n^*}]\sum_{k=0}^{m}\binom{m}{k}(-1)^{m-k}e^{(k-r)x}=\sum_{k=0}^{m}\binom{m}{k}(-1)^{m-k}\frac{(k-r)^{m+n^*}}{(m+n^*)!}.\end{aligned}$$

By the identity (2.4) of Sun [S03], for any $l=0,1,\ldots$ we have

$$\begin{aligned}\sum_{k=0}^{m}\binom{m}{k}(-1)^{m-k}(k+l)^{m+n^*}=&\sum_{j=0}^{l}\binom{l}{j}(m+j)!S(m+n^*,m+j)\\ =&\sum_{j=0}^{n^*}\binom{l}{j}(m+j)!S(m+n^*,m+j).\end{aligned}$$

Thus

$$\sum_{k=0}^{m}\binom{m}{k}(-1)^{m-k}(k+x)^{m+n^*}=\sum_{j=0}^{n^*}\binom{x}{j}(m+j)!S(m+n^*,m+j)$$

and hence

$$\sum_{k=0}^{m}\binom{m}{k}(-1)^{m-k}\frac{(k-r)^{m+n^*}}{(m+n^*)!}=\sum_{j=0}^{n^*}\binom{-r}{j}\bar{S}(m+n^*,m+j).$$

If $m \leqslant 0$, then

$$\frac{B_{n^*}^{(-m)}(-r)}{n^*!}=[x^{n^*}]\left(\frac{x}{e^x-1}\right)^{-m}e^{-rx}=[x^{n^*}]\left(\frac{e^x-1}{x}\right)^{m}e^{-rx}.$$

Note also that

$$\frac{1}{n^*!}=\frac{\prod_{j=1}^{p-1-n^*}(p-j)}{(p-1)!}\equiv(-1)^{n^*+1}(p-1-n^*)!\ (\mathrm{mod}\ p)$$

by Wilson's theorem.

In view of the above, whether $m \geqslant 0$ or $m \leqslant 0$, we only need to show that

$$(-1)^n F_p(n,r) \equiv [x^{n^*}]\left(\frac{e^x-1}{x}\right)^m e^{-rx} \pmod p.$$

(ii) All those formal power series $f(x)=\sum_{k=0}^\infty a_kx^k$ with $a_k\in\mathbb{Q}$ and $a_0,\ldots,a_{n^*}\in\mathbb{Z}_p$ form a ring R_{n^*} under the usual addition and multiplication. In particular, this ring contains

$$e^{-rx}=\sum_{k=0}^\infty(-r)^k\frac{x^k}{k!},\quad \frac{e^x-1}{x}=\sum_{k=0}^\infty\frac{x^k}{(k+1)!}\ \text{ and }\ \frac{x}{e^x-1}=\sum_{k=0}^\infty B_k\frac{x^k}{k!}.$$

(Recall that $n^*<p-1$ and $B_0,\ldots,B_{n^*}\in\mathbb{Z}_p$.) If $f(x)=\sum_{k=0}^\infty a_kx^k$ and $g(x)=\sum_{k=0}^\infty b_kx^k$ belong to R_{n^*}, then

$$\begin{aligned}&[x^{n^*}]f(x)g(x)^p=[x^{n^*}]\sum_{j=0}^{n^*}a_jx^j\left(\sum_{k=0}^{n^*}b_kx^k\right)^p\\ \equiv&[x^{n^*}]\sum_{j=0}^{n^*}a_jx^j\sum_{k=0}^{n^*}b_k^px^{pk}=a_{n^*}b_0^p\equiv[x^{n^*}]f(x)[x^0]g(x)\pmod p.\end{aligned}$$

Consequently, for any $a\in\mathbb{Z}$ we have

$$[x^{n^*}]\left(\frac{e^x-1}{x}\right)^m e^{ax}\equiv[x^{n^*}]\left(\frac{e^x-1}{x}\right)^n e^{ax}\pmod p$$

since $m\equiv n \pmod p$. By this and part (i), it suffices to use induction on n to show that

$$(-1)^n F_p(n,r)\equiv[x^{n^*}]\left(\frac{e^x-1}{x}\right)^n e^{-rx}\pmod p. \tag{3.2}$$

(iii) Obviously

$$(-1)^0F_p(0,r)=-pC_p(0,r)+1\equiv1=[x^0]\left(\frac{e^x-1}{x}\right)^0e^{-rx}\pmod p.$$

So (3.2) holds for $n=0$.

Suppose that $0<n\leqslant p-1$. Then $n^*=p-1-n$ and

$$\begin{aligned}&[x^{n^*}]\left(\frac{e^x-1}{x}\right)^n e^{-rx}=[x^{p-1}](e^x-1)^ne^{-rx}\\ =&\sum_{k=0}^n\binom{n}{k}(-1)^{n-k}[x^{p-1}]e^{(k-r)x}=\sum_{k=0}^n\binom{n}{k}(-1)^{n-k}\frac{(k-r)^{p-1}}{(p-1)!}\\ \equiv&(-1)^{n-1}\sum_{k\not\equiv r\,(\mathrm{mod}\ p)}\binom{n}{k}(-1)^k \pmod p.\end{aligned}$$

(To get the last congruence we have applied Wilson's theorem and Fermat's little theorem.) Since

$$-\sum_{k\not\equiv r\,(\mathrm{mod}\ p)}\binom{n}{k}(-1)^k=\sum_{k\equiv r\,(\mathrm{mod}\ p)}\binom{n}{k}(-1)^k=F_p(n,r),$$

the desired (3.2) follows.

Now fix $n\geqslant p$ and assume that (3.2) holds for smaller values of n. Clearly $n'=n-(p-1)>0$ and $\{-n'\}_{p-1}=n^*$. In light of Lemma 3.1,

$$F_p(n,r)\equiv-\sum_{j=1}^{p-1}\frac{1}{j}\sum_{k=0}^{j-1}F_p(n',r-k)\ (\mathrm{mod}\ p).$$

By the induction hypothesis and part (ii),

$$\begin{aligned}(-1)^{n'}F_p(n',r-k)\equiv&[x^{n^*}]\left(\frac{e^x-1}{x}\right)^{n'}e^{-(r-k)x}\\ \equiv&[x^{n^*}]\left(\frac{e^x-1}{x}\right)^{n+1}e^{(k-r)x}\ (\mathrm{mod}\ p).\end{aligned}$$

Thus $(-1)^{n-1}F_p(n,r)$ is congruent to

$$\begin{aligned}&\sum_{j=1}^{p-1}\frac{1}{j}\sum_{k=0}^{j-1}\left([x^{n^*}]\left(\frac{e^x-1}{x}\right)^{n+1}e^{(k-r)x}\right)\\ =&[x^{n^*}]\left(\frac{e^x-1}{x}\right)^{n+1}e^{-rx}\sum_{j=1}^{p-1}\left(\frac{1}{j}\cdot\frac{e^{jx}-1}{e^x-1}\right)\\ =&[x^{n^*}]\left(\frac{e^x-1}{x}\right)^{n}e^{-rx}\sum_{j=1}^{p-1}\frac{e^{jx}-1}{jx}\end{aligned}$$

modulo p. This yields

$$\begin{aligned}(-1)^nF_p(n,r)\equiv&-[x^{n^*}]\left(\frac{e^x-1}{x}\right)^{n}e^{-rx}\sum_{j=1}^{p-1}\sum_{k=1}^{p-1}\frac{(jx)^{k-1}}{k!}\\ \equiv&[x^{n^*}]\left(\frac{e^x-1}{x}\right)^{n}e^{-rx}\ (\mathrm{mod}\ p),\end{aligned}$$

since $n^*<p-1$ and $\sum_{j=1}^{p-1}j^{k-1}\equiv-[\![p-1\mid k-1]\!]\ (\mathrm{mod}\ p)$.

In view of the above, we have completed the proof. □

4. Proof of Theorem 1.3

Proof of Theorem 1.3. Let ζ_p be a primitive p-th root of unity in $\mathbb{C}$, and set $\pi = 1-\zeta_p$. For any $k = 0, \ldots, n$, we have

$$\begin{aligned} pC_p(kp^a(p-1)+l, r) =& \sum_{j=0}^{p-1} \zeta_p^{-jr}(1-\zeta_p^j)^{kp^a(p-1)+l} \\ =& \sum_{j=1}^{p-1} \zeta_p^{-jr}(1-\zeta_p^j)^{kp^a(p-1)+l} + [\![k=l=0]\!] \end{aligned}$$

and thus

$$\begin{aligned} & F_p(kp^a(p-1)+l, r) \\ =& (-p)^{-\lfloor (kp^a(p-1)+l-1)/(p-1)\rfloor} C_p(kp^a(p-1)+l, r) + [\![k=l=0]\!] \\ =& -(-p)^{-kp^a-\lfloor (l-1)/(p-1)\rfloor -1} \sum_{j=1}^{p-1} \zeta_p^{-jr}(1-\zeta_p^j)^{kp^a(p-1)+l}. \end{aligned}$$

Therefore, for $S_n = \sum_{k=0}^n \binom{n}{k}(-1)^k F_p(kp^a(p-1)+l, r)$ we have

$$S_n = -\sum_{j=1}^{p-1} \zeta_p^{-jr}(1-\zeta_p^j)^l (-p)^{-\lfloor (l-1)/(p-1)\rfloor -1} c_{n,j}, \tag{4.1}$$

where

$$\begin{aligned} c_{n,j} =& \sum_{k=0}^n \binom{n}{k}(-1)^k(-p)^{-kp^a}(1-\zeta_p^j)^{kp^a(p-1)} \\ =& \left(1-(-p)^{-p^a}(1-\zeta_p^j)^{p^a(p-1)}\right)^n. \end{aligned}$$

Let $j \in \{1, \ldots, p-1\}$. Clearly

$$\left(\frac{1-\zeta_p^j}{\pi}\right)^{p-1} = \left(\frac{1-(1-\pi)^j}{\pi}\right)^{p-1} \equiv j^{p-1} \equiv 1 \pmod{\pi}$$

and hence

$$b_j := \frac{(1-\zeta_p^j)^{p-1}}{-p} = \left(\frac{1-\zeta_p^j}{\pi}\right)^{p-1} \frac{\pi^{p-1}}{-p} \equiv 1 \pmod{\pi}.$$

(Recall the congruence $p/\pi^{p-1} \equiv -1 \pmod{\pi}$.) It follows that $b_j^{p^a} \equiv 1 \pmod{p^a\pi}$ and

$$c_{n,j} = \left(1-b_j^{p^a}\right)^n \equiv 0 \pmod{p^{an}\pi^n}. \tag{4.2}$$

Since $(1-\zeta_p^j)^l \equiv 0 \pmod{\pi^l}$ and $\operatorname{ord}_p(\pi)=1/(p-1)$, in view of (4.1) and (4.2) we have

$$\operatorname{ord}_p(S_n) \geqslant \frac{l+n}{p-1}+an-\left\lfloor\frac{l-1}{p-1}\right\rfloor-1=an+\frac{l+n}{p-1}-\frac{l+l^*}{p-1}=an+\frac{n-l^*}{p-1}$$

and hence $\operatorname{ord}_p(S_n) \geqslant an+\lceil (n-l^*)/(p-1)\rceil$. This proves (1.20). □

5. On generalized Fleck quotients

Lemma 5.1. *Let $d,q\in\mathbb{Z}^+$, $n\in\mathbb{N}$ and $r\in\mathbb{Z}$. Let ζ_{dq} be a primitive dq-th root of unity in $\mathbb{C}$. Then*

$$C_{dq}(n,r)=\frac{1}{d}\sum_{k=0}^{n}\binom{n}{k}C_q(k,r)\sum_{j=0}^{d-1}\zeta_{dq}^{j(k-r)}\left(1-\zeta_{dq}^{j}\right)^{n-k}. \tag{5.1}$$

Proof. Note that $\zeta=\zeta_{dq}^d$ is a primitive q-th root of unity. Thus

$$\begin{aligned}
&q\sum_{k=0}^{n}\binom{n}{k}C_q(k,r)\sum_{j=0}^{d-1}\zeta_{dq}^{j(k-r)}\left(1-\zeta_{dq}^{j}\right)^{n-k}\\
=&\sum_{k=0}^{n}\binom{n}{k}\sum_{s=0}^{q-1}\zeta^{-sr}(1-\zeta^s)^k\sum_{j=0}^{d-1}\zeta_{dq}^{j(k-r)}\left(1-\zeta_{dq}^{j}\right)^{n-k}\\
=&\sum_{s=0}^{q-1}\sum_{j=0}^{d-1}\zeta_{dq}^{-(ds+j)r}\sum_{k=0}^{n}\binom{n}{k}\left(\zeta_{dq}^{j}(1-\zeta_{dq}^{ds})\right)^k\left(1-\zeta_{dq}^{j}\right)^{n-k}\\
=&\sum_{s=0}^{q-1}\sum_{j=0}^{d-1}\zeta_{dq}^{-(ds+j)r}\left(1-\zeta_{dq}^{ds+j}\right)^{n}\\
=&\sum_{t=0}^{dq-1}\zeta_{dq}^{-tr}\left(1-\zeta_{dq}^{t}\right)^{n}=dqC_{dq}(n,r).
\end{aligned}$$

So we have (5.1). □

With the help of Lemma 5.1 we can prove the following result via roots of unity.

Theorem 5.1 (Weisman, 1977). *Let p be a prime, and let $a\in\mathbb{Z}^+$, $n\in\mathbb{N}$ and $r\in\mathbb{Z}$. Then $F_{p^a}(n,r)\in\mathbb{Z}$.*

Proof. We use induction on a.

The case $a=1$ reduces to Fleck's result. A proof of Fleck's result via roots of unity was given by A. Granville [Gr].

Now let $a \geqslant 2$ and assume that $F_{p^{a-1}}(n', r') \in \mathbb{Z}$ for all $n' \in \mathbb{N}$ and $r' \in \mathbb{Z}$. If $n < p^a$, then $\lfloor (n - p^{a-1})/\varphi(p^a) \rfloor \leqslant 0$ and hence $F_{p^a}(n, r) \in \mathbb{Z}$. Below we suppose $n \geqslant p^a$ and let ζ_{p^a} be a primitive p^a-th root of unity in $\mathbb{C}$.

By Lemma 5.1,

$$C_{p^a}(n, r) = \frac{1}{p} \sum_{k=0}^{n} \binom{n}{k} C_{p^{a-1}}(k, r) \sum_{j=0}^{p-1} \zeta_{p^a}^{j(k-r)} \left(1 - \zeta_{p^a}^{j}\right)^{n-k}. \tag{5.2}$$

Observe that

$$\prod_{\substack{j=1 \\ p \nmid j}}^{p^a - 1} \left(1 - \zeta_{p^a}^{j}\right) = \prod_{\substack{\gamma^{p^a} = 1 \\ \gamma^{p^{a-1}} \neq 1}} (1 - \gamma) = \lim_{x \to 1} \frac{x^{p^a} - 1}{x^{p^{a-1}} - 1} = \frac{p^a}{p^{a-1}} = p.$$

If $p \nmid j$, then $(1 - \zeta_{p^a}^{j})/(1 - \zeta_{p^a})$ is a unit in the ring $\mathbb{Z}[\zeta_{p^a}]$ and thus

$$\operatorname{ord}_p(1 - \zeta_{p^a}^{j}) = \operatorname{ord}_p(1 - \zeta_{p^a}) = \frac{1}{\varphi(p^a)}.$$

By this and the induction hypothesis, for any $k = 0, \ldots, n$ we have

$$\begin{aligned} &\operatorname{ord}_p\left(C_{p^{a-1}}(k, r) \sum_{j=0}^{p-1} \zeta_{p^a}^{j(k-r)} \left(1 - \zeta_{p^a}^{j}\right)^{n-k} \right) \\ \geqslant &\max\left\{0,\ \left\lfloor \frac{k - p^{a-2}}{\varphi(p^{a-1})} \right\rfloor \right\} + \frac{n-k}{\varphi(p^a)} \\ = &\max\left\{0,\ \frac{pk - p^{a-1}}{\varphi(p^a)} - \left\{ \frac{k - p^{a-2}}{\varphi(p^{a-1})} \right\} \right\} + \frac{n-k}{\varphi(p^a)} \\ = &\max\left\{ \frac{n-k}{\varphi(p^a)},\ \frac{n - p^{a-1}}{\varphi(p^a)} + \frac{k}{p^{a-1}} - \left\{ \frac{k - p^{a-2}}{\varphi(p^{a-1})} \right\} \right\} > \frac{n - p^{a-1}}{\varphi(p^a)}. \end{aligned}$$

(Note that if $k \geqslant p^{a-1}$ then $k/p^{a-1} \geqslant 1 > \{(k - p^{a-2})/\varphi(p^{a-1})\}$.) Therefore, from (5.2) we get that

$$\operatorname{ord}_p(C_{p^a}(n, r)) > \frac{n - p^{a-1}}{\varphi(p^a)} - 1 \geqslant \left\lfloor \frac{n - p^{a-1}}{\varphi(p^a)} \right\rfloor - 1.$$

So $F_{p^a}(n, r) = (-p)^{-\lfloor (n - p^{a-1})/\varphi(p^a) \rfloor} C_{p^a}(n, r) \in \mathbb{Z}$ as desired. $\square$

Proof of Theorem 1.4. (i) Write $n + d = p^{a-1} - 1 + m\varphi(p^a)$ with $m \in \mathbb{N}$. Then, for any $k = 0, \ldots, d$ we have

$$\left\lfloor \frac{n + k - p^{a-1}}{\varphi(p^a)} \right\rfloor = \left\lfloor m - \frac{d - k + 1}{\varphi(p^a)} \right\rfloor = m - 1.$$

Below we use induction on d to show the desired congruence (1.21).

In the case $d=0$ (i.e., $n-p^{a-1}\equiv -1 \pmod{\varphi(p^a)}$), we have $F_{p^a}(n,r)\equiv F_{p^a}(n,0) \pmod p$ because

$$F_{p^a}(n,i)-F_{p^a}(n,i-1)=(-p)^{-m+1}C_{p^a}(n+1,i)=-pF_{p^a}(n+1,i)$$

for all $i\in\mathbb{Z}$. Furthermore, by a result of Weisman [We] (see also [SW, Theorem 1.5]), $F_{p^a}(n,r)\equiv 1 \pmod p$ if $d=0$.

Now let $d>0$ and assume that the desired result holds for smaller values of d. Clearly, $(n+1)+(d-1)=p^{a-1}-1+m\varphi(p^a)$ and

$$\left\lfloor\frac{n+1+k-p^{a-1}}{\varphi(p^a)}\right\rfloor=m-1\quad\text{for}\quad k=0,\ldots,d-1.$$

If $r\geqslant 0$ then

$$C_{p^a}(n,r)-C_{p^a}(n,0)=\sum_{0<i\leqslant r}(C_{p^a}(n,i)-C_{p^a}(n,i-1))=\sum_{0<i\leqslant r}C_{p^a}(n+1,i);$$

if $r<0$ then

$$\begin{aligned}C_{p^a}(n,r)-C_{p^a}(n,0)&=\sum_{r<i\leqslant 0}(C_{p^a}(n,i-1)-C_{p^a}(n,i))\\&=-\sum_{r<i\leqslant 0}C_{p^a}(n+1,i).\end{aligned}$$

Therefore

$$F_{p^a}(n,r)-F_{p^a}(n,0)=\begin{cases}\sum_{0<i\leqslant r}F_{p^a}(n+1,i) & \text{if } r\geqslant 0,\\ -\sum_{r<i\leqslant 0}F_{p^a}(n+1,i) & \text{if } r<0.\end{cases}$$

By the induction hypothesis, whenever $i\in\mathbb{Z}$ we have

$$F_{p^a}(n+1,i)\equiv\sum_{k=0}^{d-1}\binom{i+k-1}{k}F_{p^a}(n+1+k,0) \pmod p.$$

For any $k=0,\ldots,d-1$, if $r\geqslant 0$

$$\sum_{0<i\leqslant r}\binom{i+k-1}{k}=\sum_{j=0}^{r+k-1}\binom{j}{k}=\binom{r+k}{k+1}$$

by an identity of S.-C. Chu (cf. [GKP, (5.10)]); if $r<0$ then

$$\begin{aligned}-\sum_{r<i\leqslant 0}\binom{i+k-1}{k}&=(-1)^{k+1}\sum_{r<i\leqslant 0}\binom{-i}{k}=(-1)^{k+1}\sum_{j=0}^{-r-1}\binom{j}{k}\\&=(-1)^{k+1}\binom{-r}{k+1}=\binom{r+k}{k+1}.\end{aligned}$$

Thus, by the above, $F_{p^a}(n,r)$ is congruent to

$$F_{p^a}(n,0)+\sum_{k=0}^{d-1}\binom{r+k}{k+1}F_{p^a}(n+1+k,0)=\sum_{k=0}^{d}\binom{r+k-1}{k}F_{p^a}(n+k,0)$$

modulo p. This concludes the induction proof of (1.21). $\square$

(ii) In the case $a=1$, the desired results in Theorem 1.4(ii) follow from Corollaries 1.3 and 1.7.

Now we let $a\geqslant 2$ and $r\in\mathbb{Z}$. Write $n=p^{a-2}(pn_1+n_0)+s$ and $r=p^{a-2}(pr_1+r_0)+t$, where $s,t\in\{0,\dots,p^{a-2}-1\}$, $n_0,r_0\in\{0,\dots,p-1\}$ and $n_1\in\mathbb{N}$ and $r_1\in\mathbb{Z}$.

If $p^{a-1}\leqslant n<p^a$, then

$$F_{p^a}(n,r)=C_{p^a}(n,r)=\binom{n}{\{r\}_{p^a}}(-1)^{\{r\}_{p^a}},$$

and in particular $\mathrm{ord}_p(C_{p^a}(n,0))=0=\lfloor(n-p^{a-1})/\varphi(p^a)\rfloor$.

Below we assume that $n\geqslant 2p^{a-1}$ (i.e., $n_1\geqslant 2$). By [SD, Theorem 1.7],

$$F_{p^a}(n,r)\equiv(-1)^t\binom{s}{t}F_{p^2}(pn_1+n_0,pr_1+r_0)\pmod p.$$

If $p\mid n_1$, or $p-1\nmid n_1-1$, or $n_0=r_0=p-1$, then by [SW, Theorem 1.2] in the case $l=0$, we have

$$F_{p^2}(pn_1+n_0,pr_1+r_0)\equiv(-1)^{r_0}\binom{n_0}{r_0}F_p(n_1,r_1)\pmod p$$

and hence $F_{p^a}(n,r)\equiv b_{n,r}F_p(n_1,r_1)\pmod p$, where

$$\begin{aligned}b_{n,r}:=&(-1)^{\{r\}_{p^{a-1}}}\binom{\{n\}_{p^{a-1}}}{\{r\}_{p^{a-1}}}=(-1)^{p^{a-2}r_0+t}\binom{p^{a-2}n_0+s}{p^{a-2}r_0+t}\\ \equiv&(-1)^t\binom{s}{t}(-1)^{r_0}\binom{n_0}{r_0}\pmod p\quad\text{(by Lucas' theorem (cf. [HS]))}.\end{aligned}$$

By Corollary 1.3, there is an $r_1'\in\mathbb{Z}$ such that $F_p(n_1,r_1')\not\equiv 0\pmod p$. Thus, if $p\mid n_1$ or $p-1\nmid n_1-1$, then

$$F_{p^a}(n,p^{a-1}r_1')\equiv F_p(n_1,r_1')\not\equiv 0\pmod p.$$

If $n_0=p-1$, then

$$F_{p^a}(n,p^{a-2}(pr_1'+p-1))\equiv(-1)^{p-1}\binom{p-1}{p-1}F_p(n_1,r_1')\not\equiv 0\pmod p.$$

When $p\nmid n_1$, $p-1\mid n_1-1$ and $n_0<r_0$, by applying the second part of [SW, Theorem 1.2] in the case $l=0$, we have

$$F_{p^2}(pn_1+n_0,pr_1+r_0)\equiv [\![n_1>1]\!]\frac{(-1)^{n_0}n_1}{r_0\binom{r_0-1}{n_0}}=\frac{(-1)^{n_0}n_1}{r_0\binom{r_0-1}{n_0}} \pmod p$$

and hence

$$F_{p^a}(n,r)\equiv(-1)^{n_0+t}\frac{n_1\binom{s}{t}}{r_0\binom{r_0-1}{n_0}} \pmod{p}.$$

In particular, if $p\nmid n_1$, $p-1\mid n_1-1$ and $n_0<p-1$, then

$$F_{p^a}(n,p^{a-2}(n_0+1))\equiv\frac{(-1)^{n_0}n_1}{n_0+1}\not\equiv 0 \pmod{p}.$$

In view of the above, we already have (1.22).

To prove the congruence in (1.23), we should also consider the case $p\nmid n_1$, $p-1\mid n_1-1$ and $n_0\geqslant r_0$. By [SW, Lemmas 3.2 and 3.3],

$$\begin{aligned}
&p^{-\lfloor (pn_1+n_0-p)/\varphi(p^2)\rfloor}C_{p^2}(pn_1+n_0,pr_1+r_0)\\
&-(-1)^{r_0}\binom{n_0}{r_0}p^{-\lfloor (n_1-1)/(p-1)\rfloor}C_p(n_1,r_1)\\
\equiv&(-1)^{n_1-1}p^{-\lfloor (n_1-1-1)/(p-1)\rfloor}C_p(n_1-1,r_1)(-1)^{n_1+r_0}n_1\binom{n_0}{r_0}\frac{\sigma_{n_0,r_0}(n_1)}{p}\\
\equiv&-(-1)^{r_0}\binom{n_0}{r_0}p^{-(n_1-1)/(p-1)+1}C_p(n_1-1,r_1)n_1\frac{\sigma_{n_0,r_0}(n_1)}{p} \pmod{p},
\end{aligned}$$

where

$$\sigma_{n_0,r_0}(n_1)=1+(-1)^p\frac{\prod_{1\leqslant i\leqslant p,\, i\neq p-r_0}(p(n_1-1)+r_0+i)}{\prod_{1\leqslant i\leqslant p,\, i\neq p-(n_0-r_0)}(n_0-r_0+i)}\equiv 0 \pmod{p}.$$

Therefore

$$\begin{aligned}
&F_{p^2}(pn_1+n_0,pr_1+r_0)-(-1)^{r_0}\binom{n_0}{r_0}F_p(n_1,r_1)\\
\equiv&(-1)^{r_0}\binom{n_0}{r_0}F_p(n_1-1,r_1)n_1\frac{\sigma_{n_0,r_0}(n_1)}{p} \pmod{p}
\end{aligned}$$

and hence

$$F_{p^a}(n,r)\equiv b_{n,r}\left(F_p(n_1,r_1)+F_p(n_1-1,r_1)n_1\frac{\sigma_{n_0,r_0}(n_1)}{p}\right) \pmod{p},$$

Observe that $n+p^a(p-1)=p^{a-2}(pn_1'+n_0)+s$ with $n_1'=n_1+p(p-1)$. Clearly $F_p(n_1',r_1)\equiv F_p(n_1,r_1) \pmod{p}$ by Corollary 1.7, and $\sigma_{n_0,r_0}(n_1')\equiv\sigma_{n_0,r_0}(n_1) \pmod{p^2}$ if $n_0\geqslant r_0$. Thus, by the above, $F_{p^a}(n+p^a(p-1),r)\equiv F_{p^a}(n,r) \pmod{p}$. This concludes the proof. $\square$

References

[BEW] B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi Sums*, John Wiley & Sons, New York, 1998.

[C] S. Chowla, *On the class number of real quadratic fields*, Proc. Nat. Acad. Sci. U.S.A. **47** (1961), 878.

[Co] P. Colmez, *Une correspondance de Langlands locale p-adique pour les representations semi-stables de dimension 2*, preprint, 2004.

[DS] D. M. Davis and Z. W. Sun, *A number-theoretic approach to homotopy exponents of $SU(n)$*, J. Pure Appl. Algebra **209** (2007), 57–69.

[D] L. E. Dickson, *History of the Theory of Numbers,* Vol. I, AMS Chelsea Publ., 1999.

[G1] J. W. L. Glaisher, *Congruences relating to the sums of products of the first n numbers and to other sums of product*, Quart. J. Pure Appl. Math. **31** (1900), 1–35.

[G2] J. W. L. Glaisher, *On the residues of the sums of products of the first $p-1$ numbers, and their powers, to modulus p^2 or p^3*, Quart. J. Math. **31** (1900), 321–353.

[GKP] R. Graham, D. E. Knuth and O. Patashnik, *Concrete Mathematics*, 2nd ed., Addison Wesley, New York, 1994.

[Gr] A. Granville, *Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers,* in: Organic mathematics (Burnaby, BC, 1995), 253–276, CMS Conf. Proc., 20, Amer. Math. Soc., Providence, RI, 1997.

[HS] H. Hu and Z. W. Sun, *An extension of Lucas' theorem*, Proc. Amer. Math. Soc. **129** (2001), 3471–3478.

[IR] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory* (Graduate texts in math.; 84), 2nd ed., Springer, New York, 1990.

[LW] J.H. van Lint and R. M. Wilson, *A Course in Combinatorics*, 2nd ed., Cambridge Univ. Press, Cambridge, 2001.

[M] L. J. Mordell, *The congruence* $((p-1)/2)! \equiv \pm 1 \pmod p$, Amer. Math. Monthly **68** (1961), 145–146.

[PS] H. Pan and Z. W. Sun, *New identities involving Bernoulli and Euler polynomials*, J. Combin. Theory Ser. A **113** (2006), 156–175.

[S02] Z. W. Sun, *On the sum* $\sum_{k\equiv r \,(\mathrm{mod}\ m)}\binom{n}{k}$ *and related congruences*, Israel J. Math. **128** (2002), 135–156.

[S03] Z. W. Sun, *Combinatorial identities in dual sequences*, European J. Combin. **24** (2003), 709–718.

[S06] Z. W. Sun, *Polynomial extension of Fleck's congruence*, Acta Arith. **122** (2006), 91–100.

[SD] Z. W. Sun and D. M. Davis, *Combinatorial congruences modulo prime powers*, Trans. Amer. Math. Soc., in press. `http://arxiv.org/abs/math.NT/0508087`.

[SP] Z. W. Sun and H. Pan, *Identities concerning Bernoulli and Euler polynomials*, Acta Arith. **125** (2006), 21–39.

[SW] Z. W. Sun and D. Wan, *Lucas-type congruences for cyclotomic ψ-coefficients*, Int. J. Number Theory, in press. `http://arxiv.org/abs/math.NT/0512012`.

[W] D. Wan, *Combinatorial congruences and ψ-operators*, Finite Fields Appl. **12** (2006), 693–703.

[Wa] L. C. Washington, *Introduction to Cyclotomic Fields* (Graduate texts in math.; 83), 2nd ed., Springer, New York, 1997.

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