ON A SPECIAL CONGRUENCE OF CARLITZ

Sandro Mattarei[1]
Dipartimento di Matematica, Università degli Studi di Trento, via Sommarive 14, I-38050 Povo (Trento), Italy
mattarei@science.unitn.it

Received: 2/1/06, Accepted: 3/6/06, Published: 3/13/06

Abstract

We prove that if q is a power of a prime p and p^k divides a, with $k \geq 0$, then

$$1 + (q-1) \sum_{0 \leq b(q-1) < a} \binom{a}{b(q-1)} \equiv 0 \pmod{p^{k+1}}.$$

The special case of this congruence where $q = p$ was proved by Carlitz in 1953 by means of rather deep properties of the Bernoulli numbers. A more direct approach produces our generalization and several related results.

1. Introduction

Sums of binomial coefficients of the form

$$\sum_b \binom{a}{b\,d + r} = |\{X \subseteq \{1, \dots, a\} : |X| \equiv r \pmod{d}\}|$$

occur in combinatorics and number theory. Several classical results give information on the values of such sums modulo a prime or prime power. One of the oldest results of this type is due to Hermite, who proved in 1876 that (in modern notation) a prime p divides $\sum_{b>0} \binom{a}{b(p-1)}$ if a is a positive odd integer (cf. [Dic66, p. 271]). Hermite's result was then generalized in a number of directions, the earliest due to Glaisher in 1899 (cf. [Dic66, p. 272]). Glaisher showed that

$$\sum_{b \geq 0} \binom{a}{b(p-1) + r} \equiv \binom{\bar{a}}{r} \pmod{p} \tag{1}$$

[1] Partially supported by Ministero dell'Istruzione, dell'Università e della Ricerca, Italy, through PRIN "Graded Lie algebras and pro-p-groups: representations, periodicity and derivations".

for p a prime, a a positive integer, and $1 \leq r \leq p-1$, where $\bar{a}$ denotes the smallest positive integer congruent to a modulo $p-1$. This can also be formulated by saying that the value modulo p of the left member of (1) is a periodic function of $a > 0$ with period $p-1$. A proof of Glaisher's result based on Lucas' theorem for evaluating binomial coefficients modulo a prime can be found in [Gra97, Section 6], but see the Introduction of [Sun] for a simpler proof. In Section 2 we present an easy generalization of Glaisher's result which gives an efficient formula for the value modulo p of the sum $\sum_b \binom{a}{b\,d+r}$, where d is any integer prime to p.

In 1953 Carlitz [Car53] generalized Hermite's theorem to a prime power modulus by showing that

$$p + (p-1) \sum_{0<b(p-1)<a} \binom{a}{b(p-1)} \equiv 0 \pmod{p^{k+1}} \tag{2}$$

if p is an odd prime and p^k divides the positive integer a. (This is trivially true also for $p=2$, because the left member equals 2^a in this case.) Unlike the proofs mentioned above of Glaisher's congruence (1), Carlitz's proof of (2) is quite sophisticated. It relies on certain congruences satisfied by the Bernoulli numbers, namely that B_m/m is a p-adic integer if $(p-1) \nmid m$, see [IR90, p. 238], and that $(B_m + p^{-1} - 1)/m$ is a p-adic integer if $(p-1) \mid m$, see [IR90, p. 247], the latter result being due to Carlitz himself. It seems that no other proof of Carlitz's congruence has ever appeared, except for the special case where $p-1$ divides a, which follows from [ST, Corollary 1.1].

It appears most natural to prove Carlitz's congruence (2) by multisection of series. In fact, this route allows us to prove the following generalization, which does not seem amenable to Carlitz's original approach.

Theorem 1 *If q is a power of a prime p and p^k divides a, with $k \geq 0$, then*

$$1 + (q-1) \sum_{0\leq b(q-1)<a} \binom{a}{b(q-1)} \equiv 0 \pmod{p^{k+1}}.$$

Although our approach does not allow an evaluation modulo p^{k+1} (for $k>0$) of the more general sum $\sum_b \binom{a}{b(q-1)-r}$ where r is any integer (except for the case where $q-1$ divides a, considered in Corollary 3 below), it does produce the following remarkable symmetry.

Theorem 2 *Let p be a prime, $q = p^f$, let h, k be nonnegative integers with $h \geq k$ and $f \mid h+k$, and let r, s be positive integers. Then we have*

$$(-1)^{p\,s} \sum_b \binom{s\,p^k}{b(q-1)-r} \equiv (-1)^{p\,r} \sum_b \binom{r\,p^h}{b(q-1)-s} \pmod{p^{k+1}}.$$

The case of Theorem 2 where $q-1$ divides s has the following consequence, which complements Theorem 1 in the special case where $q-1$ divides a.

Corollary 3 *If q is a power of a prime p, the number $(q-1)p^k$ divides a, with $k \geq 0$, and $q-1$ does not divide r, then*

$$(q-1)\sum_b \binom{a}{b(q-1)-r} \equiv -(-1)^{pr} \pmod{p^{k+1}}.$$

Carlitz went further in [Car53] by evaluating the left member of his congruence (2) modulo p^{k+2}, in terms of the Bernoulli numbers B_{2s} and Wilson's quotient $w_p = ((p-1)!+1)/p$. With notation slightly adapted to our present needs, Carlitz's result reads

$$p^{-k-1}\biggl\{1+(p-1)\sum_{0\leq b(p-1)<sp^k}\binom{sp^k}{b(p-1)}\biggr\}$$
$$\equiv s\biggl\{\frac{1}{2}-\sum_{\substack{0<2j<sp^k\\ p-1\nmid 2j}}\binom{sp^k-1}{2j-1}\frac{B_{2j}}{2j}+\delta_s\frac{w_p}{p-1}\biggr\} \pmod{p} \quad (3)$$

for $p \geq 3$ (although stated for $p>3$ in [Car53], see the beginning of our Section 4), where $\delta_s = 1$ if $p-1 \mid s-1$ and $\delta_s = 0$ otherwise.

Congruence (3) is useless for the purpose of a fast evaluation modulo p of its left member, because its right member is more complicated than the former, and contains more summands. The first of our couple of contributions to (3) is a proof that the value modulo p of the left member of (3) is actually independent of k, which is not apparent from the form of the right member. In particular, the left member can be most conveniently evaluated modulo p by replacing k with 0, thus reducing the summation to about $s/(p-1)$ binomial coefficients. Although the deeper connection with Bernoulli numbers shown by Carlitz's sharper congruence (3) does not extend in an obvious way with a prime power q replacing p, we keep with the spirit of our previous results by allowing a prime power q in place of p.

Theorem 4 *Let $q = p^f$ be a power of a prime p, and let s be a positive integer. Then the value modulo p of the expression*

$$p^{-k-1}\biggl\{1+(q-1)\sum_{0\leq b(q-1)<sp^k}\binom{sp^k}{b(q-1)}\biggr\},$$

as a function of $k \geq 0$ (but $k \geq 2$ if $p=2$ and $s=1$), depends only on the remainder of k modulo f.

It is quite easy to see, in a way which we point out in Remark 11, that when p is odd the value modulo p of the expression considered in Theorem 4 is also a periodic function of $s>0$, with period dividing $(q-1)p$. Thus, one only needs consider the range $0 < s \leq (q-1)p$. Our final result displays a symmetry in the dependency on s which allows one to further restrict this range in certain cases. This is the only one among our results where we need to assume the prime p to be odd. We expand on the reasons for this after its proof in Section 4.

Theorem 5 *Let $q = p^f$ be a power of an odd prime p, and let k be a nonnegative integer. Then the value modulo p^{k+2} of the expression*

$$1 + (q-1) \sum_{0 \leq b(q-1) < sp^k} \binom{sp^k}{b(q-1)}$$

is unaffected by replacing the positive integer s with $p^t - s$, where t is any integer such that $p^t > s$ and $f \mid k + t$.

Computer calculations performed by means of the symbolic manipulation package `MAPLE` have been extremely useful for discovering and checking congruences, notably those of Theorems 4 and 5.

2. Glaisher's congruence

A standard way of dealing with sums like that of Glaisher is based on the identity

$$\sum_b \binom{a}{bd+r} x^{bd+r} = \frac{1}{d} \sum_{j=0}^{d-1} \omega^{-ir}(1+\omega^i x)^a \tag{4}$$

in the polynomial ring $F[x]$, where F is any field containing a primitive dth root of unity ω. This is identity (1.53) in [Gou72] (where F is the complex field and $\omega = \exp(2\pi\mathrm{i}/d)$), and follows by applying the more general formula for multisection of series [Com74, Chapter 1, Exercise 26] to the generating function of the binomial coefficients, $(1+x)^n = \sum_m \binom{n}{m} x^m$. Here we follow the standard convention that unrestricted summation indices run over the integers; however, the sum in (4) is a finite sum since a is positive integer, if $\binom{a}{c}$ is defined to be 0 for $c < 0$, as usual. The following result is the generalization of Glaisher's congruence announced in the Introduction.

Proposition 6 *Let p be a prime, let a and d be positive integers with $p \nmid d$, and let r be an integer. If f is the period of p modulo d and $\bar{a}$ is the smallest positive integer congruent to a modulo $p^f - 1$, then we have*

$$\sum_b \binom{a}{bd+r} \equiv \sum_b \binom{\bar{a}}{bd+r} \pmod{p}.$$

In particular, for $d = q - 1$ with q a power of p we have

$$\sum_b \binom{a}{b(q-1)+r} \equiv \binom{\bar{a}}{r} + \binom{\bar{a}}{r+q-1} \pmod{p}.$$

First proof. Let ω a primitive dth root of unity in the finite field of $q = p^f$ elements $\mathbb{F}_q$. By evaluating identity (4) for $x = 1$ we obtain

$$\sum_b \binom{a}{bd+r} = \frac{1}{d} \sum_{\alpha \in \langle \omega \rangle} \alpha^{-r}(1+\alpha)^a.$$

The desired conclusion follows since the right member of the equality, as a function of the positive integer a, depends only on the value of a modulo $q - 1$. □

We give another proof which does not use multisection of series.

Second proof. The sum $\sum_b \binom{a}{bd+r}$ equals the coefficient of x^r in the reduction of $(1 + x)^a$ modulo $x^d - 1$. If d divides $q - 1$, then $x^d - 1$ divides $x^{q-1} - 1$, and we have

$$(1-x)^q = 1 - x^q \equiv 1 - x \pmod{x^d - 1}.$$

Consequently, $(1-x)^{a+(q-1)} \equiv (1-x)^a \pmod{x^d - 1}$ if $a > 0$, and the desired conclusion follows. □

Remark 7 The general case of Proposition 6 can also be deduced from its special case $d = q - 1$, by writing $\sum_b \binom{a}{bd+r}$ as

$$\sum_{j=1}^{(q-1)/d} \sum_b \binom{a}{b(q-1)+r+jd},$$

where d divides $q - 1$.

3. Carlitz's congruence

Carlitz's congruence can be read as an equality in the ring $\mathbb{Z}/p^{k+1}\mathbb{Z}$. We could then prove it by applying a version of identity (4) over this ring. In fact, it is easily shown that identity (4) holds in the polynomial ring $R[x]$, where R is any commutative ring such that $d{\cdot}1$ is invertible in R, and ω is a unit of R such that $\omega^d = 1$ but $\omega^i - 1$ is not a zero-divisor of R for $0 < i < d$. Instead of this approach, we adopt here the equivalent but more standard way of working in the (algebraic) integers and computing modulo p^{k+1}. Nevertheless, a crucial ingredient of our proof of Carlitz's congruence would be the following basic fact concerning the finite ring

$\mathbb{Z}/p^{k+1}\mathbb{Z}$, for p odd [IR90, Chapter 4]: its group of units is the direct product of two cyclic groups, one of order $p-1$ and one of order p^k.

In order to generalize Carlitz's congruence and prove Theorem 1 we need a corresponding result for the ring $R = \mathcal{O}/p^{k+1}\mathcal{O}$, where ω is a primitive complex $(q-1)$-th root of unity and $\mathcal{O}$ is the ring of integers in the cyclotomic field $\mathbb{Q}(\omega)$. Note that $\mathcal{O}/p\mathcal{O}$ is the field of q elements $\mathbb{F}_q$.

Lemma 8 *The group of units of $R = \mathcal{O}/p^{k+1}\mathcal{O}$, for $k \geq 0$, is the direct product of a cyclic group of order $q-1$ and the group $1+pR$ of order q^k. When p is odd the latter is isomorphic with the additive group pR, and hence has exponent p^k. When $p = 2$, the group $1+2R$ is the direct product of its subgroup $\{\pm 1\}$ and a subgroup isomorphic with a subgroup of index two of the additive group $2R$; in particular, $1+2R$ has exponent 2^{k-1} if $q = 2$, and 2^k if $q > 2$.*

One can prove Lemma 8 in an elementary way by induction on k and similar calculations as those performed in the standard proof, given in [IR90, Chapter 4, §1], of its special case where $q = p$ (namely, Equation (5) in our proof of Theorem 4 in the next section). Such a proof can be found in [McD74], for example, where our Lemma 8 appears as Theorem XVI.9, viewing R as the Galois ring $GR(p^{k+1}, f)$. However, the following proof in the context of local fields seems more illuminating.

Proof. The finite quotient ring R is unaffected if we replace $\mathbb{Q}(\omega)$ with its completion $\mathbb{Q}_p(\omega)$ with respect to the prime divisor $p\mathcal{O}$. In other words, we may work in the algebraic closure $\mathbb{C}_p$ of the field $\mathbb{Q}_p$ of p-adic numbers, and let ω be a primitive $(q-1)$th root of unity in $\mathbb{C}_p$. Then $K = \mathbb{Q}_p(\omega)$ is an unramified extension of $\mathbb{Q}_p$ of degree f, hence with residue field $\mathbb{F}_q$. If $O = \{x \in K : v_p(x) \geq 0\}$ is the valuation ring of K, and $P = \{x \in K : v_p(x) \geq 1\}$ is the maximal ideal of O, then $O/P^{k+1} \cong \mathcal{O}/p^{k+1}\mathcal{O} = R$.

According to [Rob00, (III.4.4)], the group of units of O splits into a direct product $\mu_{q-1} \times (1+P)$, where μ_{q-1} is the group of $(q-1)$th roots of unity in $\mathbb{C}_p$, which is generated by ω. Suppose first that p is odd. Since $1+P$ does not contain any nontrivial root of unity with p-power order, [Rob00, (V.4.2)] shows that the logarithm map

$$1+\gamma \mapsto \sum_{j\geq 0} (-1)^{j-1}\gamma^j/j$$

maps the multiplicative group $1+P$ isomorphically and isometrically onto the additive group P. In particular, it maps $1+P^j$ onto P^j, for all positive integers j. Consequently, the logarithm map induces an isomorphism of the multiplicative group $(1+P)/(1+P^{k+1})$ onto the additive group $P/P^{k+1} \cong pR$. However, $(1+P)/(1+P^{k+1})$ is the image of $1+P$ in the quotient ring O/P^{k+1}, and hence is isomorphic with $1+pR$, as claimed.

Suppose now that $p = 2$, and assume that $k > 0$ as we may. Again according to [Rob00, (V.4.2)], the logarithm map gives a group homomorphism of $1+P$ into P with kernel $\mu_2 = \{\pm 1\}$, which is the set of roots of unity of 2-power order in $1+P$. Its restriction to $1+P^2$ is an isometry onto P^2, and hence maps $1+P^j$ bijectively onto P^j for every $j \geq 2$. Because the index q of $1+P^2$ in $1+P$ equals the index of P^2 in P, the logarithm maps $1+P$ onto a subgroup of index two of P. Since, as before, $1+2R$ is isomorphic with $(1+P)/(1+P^{k+1})$, its quotient $(1+2R)/\{\pm 1\}$ is isomorphic with a subgroup of index two of $2R$, call it A. This leaves only two possibilities for the group structure of $1+2R$: either it is isomorphic with $2R$, or it is the direct product of its subgroup $\{\pm 1\}$ and a subgroup isomorphic with A. The former possibility would entail that -1, being an element of order two, should belong to $(1+2R)^2 \leq 1+4R$, and is therefore to be excluded. □

The crucial part of Lemma 8 needed in the following proofs is the fact that the exponent of $1+pR$ divides p^k.

Proof of Theorem 1. Let ω be a primitive complex $(q-1)$-th root of unity and let $\mathcal{O}$ be the ring of integers in the cyclotomic field $\mathbb{Q}(\omega)$. According to identity (4) evaluated for $x=1$, in $\mathcal{O}$ we have

$$1+(q-1)\sum_{0\leq b(q-1)\leq a}\binom{a}{b(q-1)} = \sum_{\alpha\in\mu_{q-1}\cup\{0\}}(1+\alpha)^a,$$

where $\mu_{q-1} = \langle\omega\rangle$. Since the elements $\alpha \in \mu_{q-1}\cup\{0\}$ are a set of representatives for the cosets of the additive subgroup $p\mathcal{O}$ of $\mathcal{O}$, so are the elements $1+\alpha$.

Now view the above equality in the quotient ring $R = \mathcal{O}/p^{k+1}\mathcal{O}$, denoting by $\bar{\mu}_{q-1}$ the image of μ_{q-1} in R. In particular, because $\beta(1+pR) = \beta+pR$ for $\beta \in R$, the elements $1+\alpha$ for $\alpha \in \bar{\mu}_{q-1}\cup\{0\}\setminus\{-1\}$ are a set of representatives for the cosets of $1+pR$ in the group of units U of R. According to Lemma 8, the group U is the direct product of its subgroups $\bar{\mu}_{q-1}$ and $1+pR$, and the latter has exponent p^k (or p^{k-1} when $q=2$, a trivial case here). Consequently, if β ranges over a set of representatives for the cosets of $1+pR$ in U, then β^{p^k} ranges over the elements of $\bar{\mu}_{q-1}$. Taking into account also the case where $\alpha=-1$, it follows that the elements $(1+\alpha)^{p^k}$ for $\alpha\in\bar{\mu}_{q-1}\cup\{0\}$ are distinct and coincide with the elements of $\bar{\mu}_{q-1}\cup\{0\}$. Hence, in the ring R we have

$$1+(q-1)\sum_{0\leq b(q-1)\leq a}\binom{a}{b(q-1)} = \sum_{\gamma\in\bar{\mu}_{q-1}\cup\{0\}}\gamma^{a/p^k} = \begin{cases}0 & \text{if } (q-1)\nmid a,\\ q-1 & \text{if } (q-1)\mid a.\end{cases}$$

In both cases it follows that

$$1+(q-1)\sum_{0\leq b(q-1)<a}\binom{a}{b(q-1)} = 0$$

in R, which is equivalent to the desired conclusion. □

In general, it does not seem possible to evaluate similarly modulo p^{k+1} the more complicated right member of the identity

$$\sum_b\binom{a}{b(q-1)-r} = \frac{1}{q-1}\sum_{\alpha\in\mu_{q-1}}\alpha^r(1+\alpha)^a.$$

However, one can somehow interchange the roles of the elements α and $1+\alpha$ in this formula, as in the following proof.

Proof of Theorem 2. We adopt the same setting and notation as in the proof of Theorem 1. We postpone consideration of the case $p=2$ to the end of the proof and assume for now that p is odd.

Let $\alpha \in \bar{\mu}_{q-1} \setminus \{-1\}$ and consider the element $\beta = (-1-\alpha)^{p^k}$ of R. It is invertible and different from -1, because $\beta \equiv -1-\alpha^{p^k} \not\equiv 0, -1 \pmod{\bar{P}}$, where $\bar{P}$ denotes the image of P in R, the unique maximal ideal of R. Lemma 8 then implies that β has multiplicative order dividing $q-1$, and hence belongs to $\bar{\mu}_{q-1} \setminus \{-1\}$. Hence the correspondence $\alpha \mapsto \beta = (-1-\alpha)^{p^k}$ maps $\bar{\mu}_{q-1} \setminus \{-1\}$ into itself, and so does the map $\beta \mapsto \alpha = (-1-\beta)^{p^h}$, because $h \geq k$. We claim that these maps are inverse of each other.

In fact, if $\beta = (-1-\alpha)^{p^k}$ then $(-1-\beta)^{p^h} \equiv (\alpha^{p^k})^{p^h} = \alpha \pmod{\bar{P}}$, because $\alpha^q = \alpha$. Since both $(-1-\beta)^{p^h}$ and α belong to $\bar{\mu}_{q-1}$, the congruence must be an equality. Thus, the correspondence $\alpha \mapsto \beta = (-1-\alpha)^{p^k}$ is a permutation of $\bar{\mu}_{q-1} \setminus \{-1\}$.

Consequently, in R we have

$$\begin{aligned}
(-1)^{ps} \sum_b \binom{sp^k}{b(q-1)-r} &= \frac{1}{q-1} \sum_{\alpha \in \bar{\mu}_{q-1} \setminus \{-1\}} \alpha^r (-1-\alpha)^{sp^k} \\
&= \frac{1}{q-1} \sum_{\beta \in \bar{\mu}_{q-1} \setminus \{-1\}} (-1-\beta)^{rp^h} \beta^s \\
&= (-1)^{pr} \sum_b \binom{rp^h}{b(q-1)-s},
\end{aligned}$$

which is equivalent to the desired conclusion.

The only difference when $p=2$ is that β is not invertible when $\alpha = 1$ and, in fact, $\beta = (-1-1)^{2^k} = 0$, because $2^k \geq k+1$. Hence, in this case the map $\alpha \mapsto \beta = (-1-\alpha)^{p^k}$ does not send $\bar{\mu}_{q-1} \setminus \{-1\} = \bar{\mu}_{q-1}$ into itself, but it does send $\bar{\mu}_{q-1} \setminus \{1\}$ into itself. Therefore, the final calculation remains valid by reading the summations over $\bar{\mu}_{q-1} \setminus \{1\}$ rather than over $\bar{\mu}_{q-1} \setminus \{-1\}$. □

Remark 9 When either $r=0$ or $s=0$, but not both, the congruence given in Theorem 2 would be off by a summand $1/(q-1)$, as one can verify by going through the above proof in this anomalous situation. In fact, this statement is equivalent to the special case of Theorem 1 where p^k is a power of q.

Remark 10 Because of the explicit formulas $\sum_k \binom{n}{k} = 2^n$ and $\sum_k \binom{n}{2k} = \sum_k \binom{n}{2k+1} = 2^{n-1}$, which follow from Equation (4), in the special cases where $q=2$ or $q=3$ the congruence stated in Theorem 2 reads $2^{sp^k} \equiv 2^{rp^h} \pmod{2^{k+1}}$, and

$$(-1)^s \cdot 2^{s \cdot 3^k - 1} \equiv (-1)^r \cdot 2^{r \cdot 3^h - 1} \pmod{3^{k+1}},$$

which are easy to verify directly.

Remark 11 Proposition 6 (with our first proof, using Lemma 8) extends at once to deal with congruences modulo a prime power p^{k+1}. In view of Remark 7 this extension boils down to the following statement, for p odd: for integers a and r with a a positive multiple of p^k we have

$$\sum_b \binom{a}{b(q-1)+r} \equiv \sum_b \binom{\bar{a}}{b(q-1)+r} \pmod{p^{k+1}},$$

where $\bar{a}$ is the smallest positive integer congruent to a modulo $(q-1)p^k$. (When $p = 2$ the assertion holds only by taking $a, \bar{a} \geq k+1$, because of the exceptional role of $\alpha = 1$ in the proof of Theorem 2.) In the special case where p^k divides a, such an assertion can also be deduced (in an admittedly twisted way) from Theorem 2, where the left member of the congruence is unaffected by adding to s any multiple of $q-1$, because the right member does.

Proof of Corollary 3. Write $a = sp^k$, thus $q-1 \mid s$, and hence $(-1)^s = 1$. Choose an integer h such that $h \geq k$ and $q-1 \mid h+k$. Using Theorem 2 and Theorem 1 in turn we obtain

$$(q-1)\sum_b \binom{s\,p^k}{b(q-1)-r} \equiv (-1)^{pr} \cdot (q-1)\sum_b \binom{r\,p^h}{b(q-1)} \equiv -(-1)^{pr},$$

the congruences being modulo p^{k+1}. □

Remark 12 The above proof of Corollary 3 exploits the special case of Theorem 2 where $q-1$ divides s but not r. In contrast, the special case of Theorem 2 where both r and s are multiples of $q-1$, which reads

$$\sum_b \binom{s\,p^k}{b(q-1)} \equiv \sum_b \binom{r\,p^h}{b(q-1)} \pmod{p^{k+1}},$$

yields no new information, since both sides of the congruences are already known to be congruent to $q/(q-1)$ according to Theorem 1.

4. Carlitz's sharper congruence

As we have pointed out in the Introduction, Carlitz stated congruence (3) under the stronger hypothesis $p > 3$. In fact, his proof relies on a congruence for Bernoulli numbers which is valid only for $p > 3$. However, when $p = 3$ congruence (3) remains valid by interpreting as zero the empty summation in the right member. In fact, the left member equals $(2^s - (-1)^s)/3^{k+1}$, which is easily seen to be congruent to $s(1+\delta_s)/2$ modulo 3. There appears to be no obvious interpretation of Equation (3) for $p = 2$, where its left member equals 2^{s2^k-k-1}, and hence is congruent to 0 modulo 2 except when $s = 1$ and $k = 0$ or 1.

Computer calculations show that the exceptional behaviour of (3) for small values of s and k when $p = 2$ persists when generalizing to a power q of 2, as the statement of Theorem 4 reflects. The reason for this will be clear at the end of its proof.

Proof of Theorem 4. We continue with the setting introduced in the proof of Theorem 1. Thus, let ω be a primitive complex $(q-1)$-th root of unity, let $\mathcal{O}$ be the ring of integers in the cyclotomic field $\mathbb{Q}(\omega)$, and let $\mu_{q-1} = \langle\omega\rangle$. We have

$$1 + (q-1) \sum_{0 \le b(q-1) < sp^k} \binom{sp^k}{b(q-1)} = -\delta_s \cdot (q-1) + \sum_{\alpha \in \mu_{q-1} \cup \{0\}} (1+\alpha)^{sp^k},$$

where $\delta_s = 1$ if $q - 1 \mid s - 1$ and $\delta_s = 0$ otherwise.

We now assume that p is odd and postpone a discussion of the case $p = 2$ to the last paragraph of the proof. For each $\alpha \in \mu_{q-1} \cup \{0\}$ we can write

$$(1+\alpha)^{p^k} = \beta_\alpha(1 + p^{k+1}\gamma_\alpha).$$

with (uniquely determined) $\beta_\alpha \in \mu_{q-1} \cup \{0\}$ and $\gamma_\alpha \in \mathcal{O}$. In fact, apart from the trivial case where $\alpha = -1$, Lemma 8 implies that the image of $(1+\alpha)^{p^k}$ in the quotient ring $R = \mathcal{O}/p^{k+1}\mathcal{O}$ belongs to the image $\bar{\mu}_{q-1}$ of μ_{q-1}. Consequently, there exists a unique $\beta_\alpha \in \mu_{q-1}$ such that $(1+\alpha)^{p^k}\beta_\alpha^{-1} \in 1 + p^{k+1}\mathcal{O}$, as desired.

For every positive integer n we have

$$(1+t)^n \equiv 1 + nt \pmod{pnt\mathcal{O}} \tag{5}$$

provided $t \in p\mathcal{O}$ for p odd, and $t \in 4\mathcal{O}$ for $p = 2$. This can be proved by extending standard calculations in the integers done in [IR90, Chapter 4, §1], but can also be deduced from its slightly more elegant p-adic version given in [Rob00, (III.4.3)]. Since $p^{k+1} > 2$ by hypothesis, it follows that

$$(1+\alpha)^{sp^k} \equiv \beta_\alpha^s(1 + sp^{k+1}\gamma_\alpha) \pmod{p^{k+2}},$$

and because $\beta_\alpha^q = \beta_\alpha$ we also have

$$(1+\alpha)^{sp^k q} \equiv \beta_\alpha^s(1 + sp^{k+1}q\gamma_\alpha) \pmod{p^{k+2}q}.$$

An argument seen in the Proof of Theorem 1 shows that β_α ranges over $\mu_{q-1} \cup \{0\}$ when α ranges over $\mu_{q-1} \cup \{0\}$, and hence

$$-\delta_s \cdot (q-1) + \sum_{\alpha \in \mu_{q-1} \cup \{0\}} \beta_\alpha^s = 0.$$

Consequently, we have

$$p^{-k-1}q^{-1}\biggl\{1+(p-1)\sum_{0\le b(p-1)<sp^kq}\binom{sp^kq}{b(p-1)}\biggr\}\equiv\sum_{\alpha\in\mu_{q-1}\cup\{0\}}\beta_\alpha^s s\gamma_\alpha$$
$$\equiv p^{-k-1}\biggl\{1+(p-1)\sum_{0\le b(p-1)<sp^k}\binom{sp^k}{b(p-1)}\biggr\}\pmod p,$$

which implies the desired conclusion.

The peculiarity of the case $p=2$ is that $(1+\alpha)^{2^k}$ cannot be expressed in the form $\beta_\alpha(1+2^{k+1}\gamma_\alpha)$ when $\alpha=1$. However, this discrepancy has no consequences if we just set $\beta_1=0$, provided $2^{s2^k}\equiv 0 \pmod{2^{k+2}}$, which is satisfied except when $s=1$ and $k=0$ or 1. □

Proof of Theorem 5. With notation as in the Proof of Theorem 4 we have

$$1+(q-1)\sum_{0\le b(q-1)<sp^k}\binom{sp^k}{b(q-1)}=\sum_{\alpha\in\mu_{q-1}\setminus\{-1\}}\bigl((1+\alpha)^{sp^k}-\beta_\alpha^s\bigr),$$

where β_α is the unique element of μ_{q-1} which is congruent to $(1+\alpha)^{p^k}$ modulo p. We already know from Theorem 1 that the expression at the right member belongs to $p^{k+1}\mathcal{O}$.

For each $\alpha\in\mu_{q-1}\setminus\{-1\}$, let $\tilde\alpha$ be the unique element of $\mu_{q-1}\setminus\{-1\}$ which is congruent to $-\alpha/(1+\alpha)$ modulo p; equivalently, let $\tilde\alpha\in\mu_{q-1}\setminus\{-1\}$ be defined by the condition $1+\tilde\alpha\equiv(1+\alpha)^{-1}\pmod p$. The desired conclusion will follow from the congruence

$$(1+\tilde\alpha)^{sp^k}-\beta_{\tilde\alpha}^s\equiv(1+\alpha)^{(p^t-s)p^k}-\beta_\alpha^{p^t-s}\pmod{p^{k+2}},\tag{6}$$

which we prove in the following paragraphs.

Lemma 8 implies that $\beta_\alpha\equiv(1+\alpha)^{p^kq}\pmod{p^{k+2}}$. Note that we actually have $\beta_\alpha\equiv(1+\alpha)^{p^kq^i}\pmod{p^{k+2}}$ for every $i>0$, because $\gamma^{uq}=\gamma^u$ for all $\gamma\in\mathcal{O}/p^{k+2}\mathcal{O}$ if p^{k+1} divides u. We will use this observation without mention in the sequel by multiplying or dividing certain exponents by appropriate powers of q whenever convenient. Since $\beta_{\tilde\alpha}=\beta_\alpha^{-1}$, the claimed congruence (6) can be written in the equivalent form

$$(1+\tilde\alpha)^{sp^k}-(1+\alpha)^{-sp^kq}\equiv(1+\alpha)^{(p^t-s)p^k}-(1+\alpha)^{(p^t-s)p^kq}\pmod{p^{k+2}}.\tag{7}$$

According to Lemma 8 we have $\tilde\alpha\equiv-\alpha/(1+\alpha)^{p^{k+t}}\pmod{p^{k+2}}$. Therefore, the left member of congruence (7) satisfies

$$\begin{aligned}(1+\tilde\alpha)^{sp^k}-(1+\alpha)^{-sp^kq}&\equiv\left(1-\frac{\alpha}{(1+\alpha)^{p^{k+t}}}\right)^{sp^k}-(1+\alpha)^{-sp^kq}\\&\equiv(1+\alpha)^{-sp^kq}\Bigl(\bigl((1+\alpha)^{p^{k+t}}-\alpha\bigr)^{sp^k}-1\Bigr)\\&\equiv(1+\alpha)^{-sp^kq}sp^k\bigl((1+\alpha)^{p^{k+t}}-\alpha-1\bigr)\pmod{p^{k+2}}\\&=(1+\alpha)^{1-sp^kq}sp^k\bigl((1+\alpha)^{p^{k+t}-1}-1\bigr)\end{aligned}$$

where we have used Equation (5) in the next-to-last passage, because $(1+\alpha)^{p^{k+t}}-\alpha \in 1+p\mathcal{O}$. Similarly, the right member of congruence (7) satisfies

$$\begin{aligned}(1+\alpha)^{(p^t-s)p^k}-(1+\alpha)^{(p^t-s)p^kq} &\equiv (1+\alpha)^{p^{k+t}-sp^k}-(1+\alpha)^{p^{k+t}-sp^kp^{k+t}}\\ &\equiv (1+\alpha)^{p^{k+t}-sp^kp^{k+t}}\big((1+\alpha)^{(p^{k+t}-1)sp^k}-1\big)\\ &\equiv (1+\alpha)^{p^{k+t}-sp^kq}sp^k\big((1+\alpha)^{p^{k+t}-1}-1\big) \pmod{p^{k+2}}\end{aligned}$$

where we have used Equation (5) in the last passage, this time because $(1+\alpha)^{p^{k+t}-1} \in 1+p\mathcal{O}$.

In order to complete a proof of congruence (7), and hence of Theorem 5, it suffices to observe that

$$(1+\alpha)^{p^{k+t}-1}-1 \equiv (1+\alpha)^{p^{k+t}-1}\big((1+\alpha)^{p^{k+t}-1}-1\big) \pmod{p^2}.$$

In fact, this congruence is equivalent to

$$\big((1+\alpha)^{p^{k+t}-1}-1\big)^2 \equiv 0 \pmod{p^2},$$

which holds because $(1+\alpha)^{p^{k+t}-1}-1 \equiv 0 \pmod{p}$. □

The above proof breaks down for $p=2$, mainly because of the two appeals to Equation (5), which requires $t \in 4\mathcal{O}$ rather than $t \in 2\mathcal{O}$ when $p=2$. In fact, computer calculations show that the statement of Theorem 5 fails for $p=2$ and $q>4$, even subject to (reasonable) restrictions on k. We have considered the trivial case where $q=2$ earlier in this section. When $q=4$, one can show by means of Equation (4) that the expression considered in Theorem 5 equals 2^{s2^k} for $k>0$ and is, therefore, a multiple of 2^{k+2} except when $(s,k)=(1,1)$.

References

[Car53] L. Carlitz, *A special congruence*, Proc. Amer. Math. Soc. **4** (1953), 933–936. MR MR0058621 (15,400h)

[Com74] Louis Comtet, *Advanced combinatorics*, enlarged ed., D. Reidel Publishing Co., Dordrecht, 1974, The art of finite and infinite expansions. MR MR0460128 (57 #124)

[Dic66] Leonard Eugene Dickson, *History of the theory of numbers. Vol. I: Divisibility and primality.*, Chelsea Publishing Co., New York, 1966. MR MR0245499 (39 #6807a)

[Gou72] Henry W. Gould, *Combinatorial identities*, Henry W. Gould, Morgantown, W.Va., 1972, A standardized set of tables listing 500 binomial coefficient summations. MR MR0354401 (50 #6879)

[Gra97] Andrew Granville, *Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers*, Organic mathematics (Burnaby, BC, 1995), CMS Conf. Proc., vol. 20, Amer. Math. Soc., Providence, RI, 1997, pp. 253–276. MR MR1483922 (99h:11016)

[IR90] Kenneth Ireland and Michael Rosen, *A classical introduction to modern number theory*, second ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990. MR MR1070716 (92e:11001)

[McD74] Bernard R. McDonald, *Finite rings with identity*, Marcel Dekker Inc., New York, 1974, Pure and Applied Mathematics, Vol. 28. MR MR0354768 (50 #7245)

[Rob00] Alain M. Robert, *A course in p-adic analysis*, Graduate Texts in Mathematics, vol. 198, Springer-Verlag, New York, 2000. MR MR1760253 (2001g:11182)

[ST] Zhi-Wei Sun and Roberto Tauraso, *Congruences for sums of binomial coefficients*, preprint, 2005, `arXiv:math.NT/0502187`.

[Sun] Zhi-Wei Sun, *On sums of binomial coefficients and their applications*, preprint, 2004, `arXiv:math.NT/0404385`.