Discrete Math. 262(2003), 253–276.

GENERAL CONGRUENCES FOR BERNOULLI POLYNOMIALS

Zhi-Wei Sun

Department of Mathematics, Nanjing University, Nanjing 210093, P. R. China
E-mail: zwsun@nju.edu.cn

Abstract. In this paper we establish some explicit congruences for Bernoulli polynomials modulo a general positive integer. In particular Voronoi's and Kummer's congruences are vastly extended.

1. Introduction

The Bernoulli numbers $B_0, B_1, B_2, \cdots$ are defined by the power series

$$\frac{z}{e^z-1}=\sum_{k=0}^{\infty}B_k\frac{z^k}{k!}\qquad (0<|z|<2\pi);$$

they can also be defined recursively:

$$B_0=1\ \text{ and }\ \sum_{k=0}^{n}\binom{n+1}{k}B_k=0\ \text{ for } n\in\mathbb{Z}^+=\{1,2,3,\cdots\}.$$

Here are some interesting analytic results:

$$\tan x=\sum_{k=1}^{\infty}(-1)^{k-1}\frac{2^{2k}(2^{2k}-1)B_{2k}}{(2k)!}x^{2k-1}\ \text{ for } x\in\left(-\frac{\pi}{2},\frac{\pi}{2}\right),$$

$$\zeta(-k)=-\frac{B_{k+1}}{k+1}\ \text{ and }\ \zeta(2k)=(-1)^{k-1}\frac{(2\pi)^{2k}}{2(2k)!}B_{2k}\ \text{ for } k\in\mathbb{Z}^+$$

where $\zeta(s)$ denotes the Riemann zeta function.

Let $\mathbb{N}$ be the set of nonnegative integers. For $k\in\mathbb{N}$ the kth Bernoulli polynomial $B_k(x)$ is given by

$$B_k(x)=\sum_{j=0}^{k}\binom{k}{j}B_jx^{k-j},$$

Keywords: Bernoulli polynomial; Congruence; q-adic number.

2000 *Mathematics Subject Classifications:* Primary 11B68; Secondary 11A07, 11S05.

The research was supported by the Teaching and Research Award Program for Outstanding Young Teachers in Higher Education Institutions of MOE, and the National Natural Science Foundation of P. R. China.

therefore $B_k = B_k(0)$. It is well known that

$$B_k(x+1) - B_k(x) = kx^{k-1} \tag{1.1}$$

where we regard $0x^{-1}$ as 0 even if $x = 0$; moreover

$$B_k(x+y) = \sum_{j=0}^{k} \binom{k}{j} B_j(x) y^{k-j}.$$

A useful theorem of Raabe (see §1.13 of [E]) asserts that

$$\sum_{r=0}^{n-1} B_k\left(\frac{x+r}{n}\right) = n^{1-k} B_k(x) \quad \text{for } n = 1, 2, 3, \cdots. \tag{1.2}$$

For a Dirichlet character χ modulo a positive integer m, the generalized Bernoulli polynomial $B_{k,\chi}(x)$ is defined by

$$B_{k,\chi}(x) = m^{k-1} \sum_{r=0}^{m-1} \chi(r) B_k\left(\frac{x+r}{m}\right); \tag{1.3}$$

by Raabe's theorem $B_{k,\chi}(x) = B_k(x)$ if χ is the principal character χ_0 with $\chi_0(a) = 1$ for all $a \in \mathbb{Z}$; we also have

$$B_{k,\chi}(x) = \sum_{j=0}^{k} \binom{k}{j} B_{j,\chi} x^{k-j}$$

where the generalized Bernoulli number $B_{j,\chi}$ refers to $B_{j,\chi}(0)$.

Bernoulli polynomials are of particular importance in number theory; they have close connections with p-adic analysis, Dirichlet L-functions and ideal class groups of cyclotomic fields. (Cf. pp. 100–109 of P. Ribenboim [R], pp. 9–19 of J. Urbanowicz and K. S. Williams [UW], and pp. 29–35, 54–63 and 77–86 of L. C. Washington [W].) A great deal of research on them has been done by many mathematicians. It is recommended that the interested reader consult [DSS], which contains a complete bibliography of related papers published during the period 1713–1990.

Number-theoretic properties of Bernoulli polynomials are fascinating and quite useful. The classical von Staudt–Clausen theorem (see pp. 233–236 of [IR]) asserts that

$$B_k + \sum_{p-1|k} \frac{1}{p} \in \mathbb{Z} \qquad \text{for all } k \in 2\mathbb{Z}^+ = \{2, 4, 6, \cdots\} \tag{1.4}$$

where the sum is over all primes p such that $p - 1 \mid k$. In 1889 G. F. Voronoi (cf. p. 237 of [IR]) discovered that if $k \in 2\mathbb{Z}^+$ and $B_k = U_k/V_k$ (where $U_k \in \mathbb{Z}$ and $V_k \in \mathbb{Z}^+$) then

$$\left(m^k - 1\right) U_k \equiv k m^{k-1} V_k \sum_{j=1}^{q-1} j^{k-1} \left\lfloor \frac{jm}{q} \right\rfloor \pmod{q} \tag{1.5}$$

for all relatively prime positive integers m and q. (As usual, for each c in the field $\mathbb{R}$ of real numbers, $\lfloor c\rfloor$ denotes the greatest integer not exceeding c, and we also set $\{c\}=c-\lfloor c\rfloor$.) E. Kummer's approach to Fermat's Last Theorem made him essentially obtain the following result in 1851: When p is a prime and k is a positive integer with $p-1\nmid k$, p does not divide the denominator of B_k/k, and

$$(1-p^{k-1})\frac{B_k}{k}\ (\mathrm{mod}\ p^\alpha)\ \text{only depends on}\ k\ (\mathrm{mod}\ \varphi(p^\alpha)) \tag{1.6}$$

where $\alpha\in\mathbb{Z}^+$ and φ denotes Euler's totient function. (This is Theorem 5 in Chapter 15 of [IR]; actually Kummer only handled the case $\alpha=1$.)

Bernoulli polynomials have many applications, they are of independent interest as well. In this paper we aim to give explicit congruences for Bernoulli polynomials modulo a *general* positive integer.

From now on we always let q `be a fixed integer greater than one`, $\mathbb{Q}_q$ the ring of q-adic numbers and $\mathbb{Z}_q$ the ring of q-adic integers. A rational number in $\mathbb{Z}_q$ is usually called a *q-integer*, and by the von Staudt-Clausen theorem qB_k is a q-integer for any $k\in\mathbb{N}$. It is well known that $\mathbb{Q}_p$ forms a field if p is a prime. A good introduction to q-adic numbers can be found in K. Mahler [M].

Set $R(q)=\{0,1,\cdots,q-1\}$ and $R_*(q)=\{r\in R(q)\colon r\ \text{is coprime to}\ q\}$. For $x\in\mathbb{Z}_q$, we let $\langle x\rangle_q$ denote the unique $r\in R(q)$ such that $x-r\in q\mathbb{Z}_q$, and $[x]_q$ represent the unique $y\in\mathbb{Z}_q$ with $qy-x\in R(q)$; clearly $[x]_q=(x+\langle -x\rangle_q)/q$.

Let $n\in\mathbb{N}$. If $n>0$ then $\mathbb{Q}_{q^n}$ and $\mathbb{Z}_{q^n}$ can be identified with $\mathbb{Q}_q$ and $\mathbb{Z}_q$ respectively (cf. pp. 40–41 of [M]); if $w_1,w_2\in\mathbb{Z}_q$ and $w_1-w_2\in q^n\mathbb{Z}_q$ then we say that w_1 is congruent to w_2 modulo q^n and denote this relation by $w_1\equiv w_2\ (\mathrm{mod}\ q^n)$; for polynomials $P(x),Q(x)\in\mathbb{Z}_q[x]$ we write $P(x)\equiv Q(x)\ (\mathrm{mod}\ q^n)$ if all corresponding coefficients of $P(x)$ and $Q(x)$ are congruent modulo q^n.

For integers $a_1,\cdots,a_k$, let $(a_1,\cdots,a_k)$ represent, as usual, the greatest common divisor of $a_1,\cdots,a_k$. For $x\in\mathbb{Z}_q$, (x,q) refers to $(\langle x\rangle_q,q)$. For a positive integer n and a prime p, by $\mathrm{ord}_p(n)$ we mean the largest $\alpha\in\mathbb{N}$ such that $p^\alpha\mid n$; if $\alpha=\mathrm{ord}_p(n)$ then we also write $p^\alpha\|n$. For $m,n\in\mathbb{Z}^+$, $m\sim_2 n$ stands for $\mathrm{ord}_2(m)=\mathrm{ord}_2(n)$. For convenience we also use the logical notations $\wedge$ (*and*), $\vee$ (*or*), $\Leftrightarrow$ (*if and only if*). For an assertion A, we set

$$[A]=\begin{cases}1 & \text{if } A \text{ holds},\\ 0 & \text{otherwise.}\end{cases} \tag{1.7}$$

Due to their generality, the results in this paper are somewhat complicated. Below we state the main theorems and derive some consequences.

Our generalization of Voronoi's congruences is as follows.

Theorem 1.1. *Let $c\in\mathbb{R}$, $d,k,m\in\mathbb{Z}^+$ and $d\mid m$. Then the polynomial*

$$\frac{1}{km/d}\left(m^kB_k\left(\frac{x}{m}\right)-\left(\frac{m}{d}(d,q)\right)^kB_k\left(\frac{d}{(d,q)}\cdot\frac{x}{m}-\left\lfloor\frac{c}{(d,q)}\right\rfloor\right)\right) \tag{1.8}$$

is in $\mathbb{Z}_q[x]$ *and is congruent to*

$$\sum_{j=0}^{q-1}(x+jm)^{k-1}\left(\left\lfloor\frac{c+jd}{q}\right\rfloor+\frac{1-d}{2}\right)+\frac{q}{2}[2\|q\wedge 2\mid m\wedge d\sim_2 m](k-1)x^{k-2}$$

modulo q.

Corollary 1.1. *Let* k,m *be positive integers and* x *a* q*-integer. Then*

$$\frac{1}{k}\left(m^kB_k\left(\frac{x}{m}\right)-(m,q)^kB_k\left(\left\{\frac{x}{(m,q)}\right\}\right)\right) \tag{1.9}$$

is a q*-adic integer congruent to*

$$\begin{aligned}&\sum_{j=0}^{q-1}(x+jm)^{k-1}\left(\left\lfloor\frac{x+jm}{q}\right\rfloor+\frac{1-m}{2}\right)\\&+\frac{q}{2}[2\|q\wedge 2\mid k\wedge 2\mid m\wedge(k=2\vee x\notin 2\mathbb{Z}_q)]\end{aligned}$$

modulo q.

Proof. Apply Theorem 1.1 with $c=x$ and $d=m$.

Corollary 1.2. *Let* $k,m\in\mathbb{Z}^+$ *and* $y\in\mathbb{Q}\cap\mathbb{Z}_q$. *Then*

$$\frac{1}{k(m,q)}\left(m^kB_k\left(\frac{x+y}{m}\right)-\left(m,q^2\right)^kB_k\left(\frac{x}{(m,q^2)}+\left\{\frac{y}{(m,q^2)}\right\}\right)\right) \tag{1.10}$$

is in $\mathbb{Z}_q[x]$ *and is congruent to*

$$\sum_{j=0}^{q-1}(x+y+jm)^{k-1}\left(\left\lfloor\frac{y+jm}{(m,q)q}\right\rfloor+\frac{1}{2}\left(1-\frac{m}{(m,q)}\right)\right)$$

modulo q.

Proof. Put $c=y/(m,q)$, $d=m/(m,q)$ and substitute $x+y$ for x in Theorem 1.1.

Corollary 1.3. *Let* $a\in\mathbb{Z}$, $k,m\in\mathbb{Z}^+$ *and* $(m,q)=1$. *Then*

$$\begin{aligned}&\frac{1}{k}\left(m^kB_k\left(\frac{x+a}{m}\right)-B_k(x)\right)\\\equiv&\sum_{j=0}^{q-1}\left(\left\lfloor\frac{a+jm}{q}\right\rfloor+\frac{1-m}{2}\right)(x+a+jm)^{k-1}\pmod q.\end{aligned} \tag{1.11}$$

Proof. This follows from Corollary 1.2 in the case $y=a$.

Remark 1.1. Under the condition of Corollary 1.3, Z.-H. Sun [S] announced that

$$\frac{m^kB_k(a/m)-B_k}{k}\equiv\sum_{j=0}^{q-1}\left\lfloor\frac{a+jm}{q}\right\rfloor(a+jm)^{k-1}+\left(1-\frac{m+1}{2}m^{k-1}\right)qB_{k-1}$$
$$+[k>1]\left(1-\frac{m+1}{2}m^{k-2}\right)\frac{k-1}{2}q^2B_{k-2}\pmod q.$$

The right-hand side of this congruence contains two unpleasant terms involving Bernoulli numbers; our (1.11) seems better.

We call a function $f\colon\mathbb{Z}^+\to\mathbb{Z}_q$ *q-normal* if there are constants $c_r\in\mathbb{Z}_q$ ($r\in R_*(q)$) such that

$$f(k)\equiv\sum_{r\in R_*(q)}c_rr^k\pmod q\quad\text{for all }k\in\mathbb{Z}^+.\tag{1.12}$$

Clearly the set of q-normal functions forms a commutative ring with respect to the functional addition and multiplication.

Our next theorem is a completely new result.

Theorem 1.2. *Let $x,y\in\mathbb{Z}_q$, $m\in\mathbb{Z}^+$ and $(m,q)=1$. Set*

$$F(k)=\frac{1}{km^{k-1}}\sum_{d\mid q}\mu(d)d^{k-1}\left(m^kB_k([x]_d)-B_k([y]_d)\right)\quad\text{for }k\in\mathbb{Z}^+\tag{1.13}$$

where μ denotes the Möbius function. Then F is q-normal, and furthermore

$$F(k)\equiv\sum_{\substack{j=0\\(x+j,q)=1}}^{q-1}\left(\left\lfloor\frac{\langle mx-y\rangle_{q^2}+jm}{q}\right\rfloor+\frac{1-m}{2}\right)(x+j)^{k-1}\pmod q.\tag{1.14}$$

Corollary 1.4. *Let $k,m\in\mathbb{Z}^+$ and $(m,q)=1$. Then*

$$\varphi_k(q)(1-m^k)\frac{B_k}{k}\equiv\sum_{\substack{r=1\\(r,q)=1}}^{q-1}r^{k-1}\left(A_r(m,q)-\frac{m+1}{2}\right)\pmod q\tag{1.15}$$

where $\varphi_k(q)=\prod_{p\mid q}(1-p^{k-1})$ and $A_r(m,q)$ denotes the least positive integer x such that $qx-r\in m\mathbb{Z}$.

Proof. Let $j\in R(q)$. Denote by r the least positive residue of $-jm$ modulo q. Obviously $1\leqslant r\leqslant q$. Since $\lfloor jm/q\rfloor\in R(m)$ and $jm=q\lfloor jm/q\rfloor+q-r$, we must have $A_r(m,q)=\lfloor jm/q\rfloor+1$. Note that $(j,q)=1$ if and only if $(r,q)=1$.

In view of the above,

$$\sum_{j\in R_*(q)}(-jm)^{k-1}\left(\left\lfloor\frac{jm}{q}\right\rfloor+\frac{1-m}{2}\right)\equiv\sum_{r\in R_*(q)}r^{k-1}\left(A_r(m,q)-\frac{m+1}{2}\right)\pmod q.$$

Clearly $(-1)^k\varphi_k(q)B_k=\varphi_k(q)B_k$, for, $\varphi_1(q)=0$, and $B_k=0$ if $k\in\{3,5,\cdots\}$. So (1.15) follows from Theorem 1.2 in the case $x=y=0$. □

Remark 1.2. Let $q>2$, $m\in\mathbb{Z}^+$ and $(m,q)=1$. It is apparent that

$$\sum_{\substack{r=1\\(r,q)=1}}^{q-1}\frac{1}{r}=\sum_{\substack{1\leqslant r<q/2\\(r,q)=1}}\left(\frac{1}{r}+\frac{1}{q-r}\right)\equiv 0\pmod q.$$

As we will see later,

$$B_{\varphi(q)}\prod_{p\mid q}\left(1-\frac{p^{\varphi(q)}-1}{p-1}\right)\equiv 1\pmod q. \tag{1.16}$$

So (1.15) in the case $k=\varphi(q)$ implies the following celebrated congruence discovered by H. F. Baker [B] and M. Lerch [Le] in 1906:

$$\frac{m^{\varphi(q)}-1}{q}\equiv-\sum_{\substack{r=1\\(r,q)=1}}^{q-1}\frac{A_r(m,q)}{r}\pmod q. \tag{1.17}$$

Now we turn to congruences of Kummer's type modulo a general positive integer.

Theorem 1.3. *Let $x\in\mathbb{Z}_q$ and*

$$S_q=\{k\in\mathbb{Z}^+\colon k\not\equiv 0\pmod{p-1}\ \textit{for any prime divisor } p \textit{ of } q\}. \tag{1.18}$$

(i) *We can find $c_r\in\mathbb{Z}_q$ $(r\in R_*(q))$ such that*

$$\sum_{d\mid q}\mu(d)\frac{d^{k-1}}{k}B_k([x]_d)\equiv\sum_{r\in R_*(q)}c_r r^k\pmod q\quad\textit{for all } k\in S_q. \tag{1.19}$$

(ii) *If $l\in S_q$, then*

$$\sum_{k=0}^{n}\binom{n}{k}\frac{(-1)^k}{k\varphi(q)+l}\sum_{d\mid q}\mu(d)d^{k\varphi(q)+l-1}B_{k\varphi(q)+l}([x]_d)\equiv 0\pmod{q^n} \tag{1.20}$$

for every $n=0,1,2,\cdots$.

Remark 1.3. Let q be a prime power p^α. Then the Kummer result follows from Theorem 1.3(i) in the case $x=0$, and Theorem 1.3(ii) was recently showed by P. T. Young in [Y1, Y2] where p-adic integrals and measures are employed. When q is a prime, Theorem 1.3(ii) in the case $x=0$ gives the strong version of Kummer's congruences (see L. Carlitz [C]), and in the case $x\neq 0$ it was first obtained by Z.-H. Sun [S].

For generalized Bernoulli polynomials, we have

Theorem 1.4. *Let $m \in \mathbb{Z}^+$ and $(m,q)=1$. Let $\mathbb{Q}_q^*$ denote the algebraic closure of $\mathbb{Q}_q$, and $\mathbb{Z}_{q,m}$ stand for the ring*

$$\left\{ \sum_{\gamma\in\mathbb{Q}_q^*,\ \gamma^{\varphi(m)}=1} a_\gamma\gamma\colon a_\gamma\in\mathbb{Z}_q \right\}.$$

Let $\chi\colon \mathbb{Z}\to\mathbb{Z}_{q,m}$ be a Dirichlet character modulo m and $r(q)$ be the product of distinct prime divisors of q. Let $x\in\mathbb{Z}_q$ and

$$G(k)=\sum_{d\mid q}\mu(d)\chi(d)\frac{d^{k-1}}{k}\left(B_{k,\chi}\left(\frac{r(q)}{d}x\right)-[\chi=\chi_0]B_k\right)\ \text{for } k\in\mathbb{Z}^+. \tag{1.21}$$

Then we can find $c_r\in\mathbb{Z}_{q,m}$ $(r\in R_*(q))$ such that

$$G(k)-\sum_{r\in R_*(q)} c_r r^k\in q\mathbb{Z}_{q,m}\quad \text{for all } k=1,2,3,\cdots. \tag{1.22}$$

If $l\in\mathbb{Z}^+$ then

$$\sum_{k=0}^{n}\binom{n}{k}(-1)^k G(k\varphi(q)+l)\in q^n\mathbb{Z}_{q,m}\quad \text{for } n=0,1,2,\cdots. \tag{1.23}$$

Remark 1.4. For generalized Bernoulli numbers, the analogue of Kummer's result obtained by R. Ernvall [Er] follows from the first part of Theorem 1.4. When q is a power of a prime p and χ is non-principal, the second part of Theorem 1.4 was recently obtained by Young [Y1, Y2], and independently given by Z.-H. Sun [S] in the case $x=0$ and $p-1\nmid l$. Theorem 1.4 in the case $\chi=\chi_0$, together with Theorem 1.3 in the case $x=0$, shows that we can substitute $(r(q)/d)x$ for $[x]_d$ in Theorem 1.3.

Let us give one more theorem.

Theorem 1.5. *Let n be a positive integer with $r(n)=r(q)$. Let $x\in\mathbb{Z}_q$ and $(x,q)=1$. For $k\in\mathbb{Z}^+$ let $S_k(n)=\sum_{r\in R_*(n)} r^k$ and*

$$H(k)=S_k(n)\left(\varphi(n)\frac{n^{k-1}}{k}B_k\left(\frac{x}{n}\right)-\varphi_k(n)\frac{B_k}{k}\right). \tag{1.24}$$

Then the function H is q-normal, and there are $c_r\in\mathbb{Z}_q$ $(r\in R_*(q))$ such that

$$S_k(n)\frac{n^{k-1}}{k}B_k\left(\frac{x}{n}\right)\equiv\sum_{r\in R_*(q)} c_r r^k\pmod q\quad \text{for all } k\in S_q. \tag{1.25}$$

Theorem 1.5 yields the following analogue of Kummer's congruences.

Corollary 1.5. *Let p be a fixed prime and x a fixed p-adic integer with $(x,p)=1$. For $\alpha,k\in\mathbb{Z}^+$ with $p-1\mid k$,*

$$P_k(x):=\frac{p^{k-1}}{k}B_k\left(\frac{x}{p}\right)+\frac{p^{k-1}-1}{p-1}\cdot\frac{B_k}{k}\in\mathbb{Z}_p, \tag{1.26}$$

and

$$P_k(x)\ (\mathrm{mod}\ p^\alpha)\ \textit{only depends on}\ k\ (\mathrm{mod}\ \varphi(p^\alpha)). \tag{1.27}$$

Proof. Applying Theorem 1.5 with $q=p^\alpha$ and $n=p$, we find that $S_k(p)P_k(x)=H(k)/(p-1)\in\mathbb{Z}_p$ for $k\in\mathbb{Z}^+$, and that $S_k(p)P_k(x)\ (\mathrm{mod}\ p^\alpha)$ only depends on $k\ (\mathrm{mod}\ \varphi(p^\alpha))$. If $p-1\mid k$ then $S_k(p)=\sum_{r=1}^{p-1}r^k\equiv p-1\not\equiv 0\ (\mathrm{mod}\ p)$; if $l\in\mathbb{Z}^+$ and $l\equiv k\ (\mathrm{mod}\ \varphi(p^\alpha))$ then $S_l(p)\equiv S_k(p)\ (\mathrm{mod}\ p^\alpha)$. So the desired result follows. □

We shall provide auxiliary results in the next section and prove a key theorem in Section 3. In Section 4 we will be able to extend Voronoi's congruences greatly. In the last section we will prove Theorems 1.2–1.5.

2. Preliminaries

Lemma 2.1. *Let n be a positive integer. Then*

(i) $\frac{q^{n-1}}{n!}\in\mathbb{Z}_q$, $\frac{q^{n-2}}{n}\in\mathbb{Z}_q$ *if* $n>2$, *and* $\frac{q^{n-3}}{n(n-1)}\in\mathbb{Z}_q$ *if* $n>4$.

(ii) $\frac{q}{n}\in\mathbb{Z}_q$ *if n is squarefree, and* $\binom{x}{n}\in\mathbb{Z}_q$ *if* $x\in\mathbb{Z}_q$.

(iii) $\frac{q^2}{20}\equiv\frac{q^2}{12}\equiv\frac{q^2}{4}\equiv\frac{q}{2}[2\|q]\ (\mathrm{mod}\ q)$, *and*

$$\frac{q}{2}x^n\equiv\frac{q}{2}x\equiv\frac{q}{2}[x\notin 2\mathbb{Z}_q]\ \ (\mathrm{mod}\ q)\quad \textit{for}\ x\in\mathbb{Z}_q.$$

Proof. i) Let p be any prime divisor of q. Then

$$\mathrm{ord}_p(n!)=\sum_{i=1}^{n}\left\lfloor\frac{n}{p^i}\right\rfloor<\sum_{i=1}^{\infty}\frac{n}{p^i}=\frac{n}{p-1}$$

and hence $(p-1)\mathrm{ord}_p(n!)\leqslant n-1\leqslant\mathrm{ord}_p(q^{n-1})$. If $p>2$ and $n>1$, then

$$\mathrm{ord}_p(n)\leqslant\mathrm{ord}_p(n(n-1))\leqslant\mathrm{ord}_p(n!)\leqslant\frac{n-1}{p-1}\leqslant\frac{n-1}{2}.$$

Clearly $(n-1)/2$ is not more than $n-2$ or $n-3$ according as $n>2$ or $n>4$. If $n>2$ then $\mathrm{ord}_2(n)\leqslant\mathrm{ord}_2(n!/2)\leqslant n-1-1$; if $n>5$ then $\mathrm{ord}_2(n(n-1))\leqslant\mathrm{ord}_2(n!/(2\cdot 4))\leqslant n-1-3$; we also have $\mathrm{ord}_2(5\cdot(5-1))=5-3$. So part (i) follows, moreover $q^{n-4}/(n(n-1))\in\mathbb{Z}_q$ if $n>5$.

ii) If n is squarefree, then $(q,n/(q,n))=1$ and hence $\frac{q}{n}=\frac{q/(q,n)}{n/(q,n)}\in\mathbb{Z}_q$.

Suppose that the q-adic expansion of $x \in \mathbb{Z}_q$ is $x = a_0 + a_1 q + a_2 q^2 + \cdots$ where the digits a_i lie in $R(q)$. Let $a = a_0 + a_1 q + \cdots + a_{n-1} q^{n-1}$. Then $x \equiv a \pmod{q^n}$ and hence

$$\binom{x}{n} - \binom{a}{n} = \frac{1}{n!}\Big(\prod_{i=0}^{n-1}(x-i) - \prod_{i=0}^{n-1}(a-i)\Big) \equiv 0 \pmod{q}$$

since $\frac{q^{n-1}}{n!} \in \mathbb{Z}_q$ by part (i). Therefore $\binom{x}{n} \in \mathbb{Z}_q$.

iii) By part (ii), $\frac{q^2}{m} = \frac{q}{m} q \equiv 0 \pmod{q}$ for $m = 5, 6$. If $2 \nmid q$ or $4 | q$ then $\frac{q^2}{4} = \frac{q}{4} q \equiv 0 \pmod{q}$; if $2 \| q$ then $\frac{q^2}{4} - \frac{q}{2} = q\frac{q/2-1}{2} \equiv 0 \pmod{q}$. So

$$\frac{q^2}{20} = \frac{q^2}{4} - \frac{q^2}{5} \equiv \frac{q^2}{12} = \frac{q^2}{4} - \frac{q^2}{6} \equiv \frac{q^2}{4} \equiv \frac{q}{2}[2\|q] \pmod{q}.$$

Let $x \in \mathbb{Z}_q$. Then $\frac{x^n - x}{2} = \sum_{0<i<n} x^{i-1}\binom{x}{2} \in \mathbb{Z}_q$. If $\frac{x}{2} \notin \mathbb{Z}_q$, then q is even and the initial digit $a_0 = \langle x \rangle_q$ of $x \in \mathbb{Z}_q$ is odd, therefore $\frac{x-1}{2} \in \mathbb{Z}_q$. Thus

$$\frac{q}{2} x^n \equiv \frac{q}{2} x = \frac{q}{2} + \frac{q}{2}(x-1) \equiv \frac{q}{2}[x \notin 2\mathbb{Z}_q] \pmod{q}.$$

The proof of Lemma 2.1 is now complete. □

Notation 2.1. For $k \in \mathbb{N}$ and $m \in \mathbb{Z} \setminus \{0\}$ we define $\delta_m^{(k)}(x) \in \mathbb{Q}[x]$ and $\delta_{m,q}^{(k)}(x) \in \mathbb{Z}_q[x]$ as follows:

$$\delta_m^{(k)}(x) = m^{k-1}\left(B_k\left(\frac{x}{m}\right) - \left(\frac{x}{m}\right)^k\right) = \sum_{0<l\leqslant k} \binom{k}{l} B_l m^{l-1} x^{k-l} \tag{2.1}$$

and

$$\delta_{m,q}^{(k)}(x) = q\delta_m^{(k)}(x) + [k>0]\frac{q^2}{2} k \delta_m^{(k-1)}(x). \tag{2.2}$$

Lemma 2.2. *Let $k \geqslant 0$ and $m \neq 0$ be integers.*

(i) *For each $w \in \mathbb{Z}_q$ we have*

$$\delta_m^{(k)}(x + (m,q)w) - \delta_m^{(k)}(x) \in \mathbb{Z}_q[x]. \tag{2.3}$$

(ii) *If $k > 0$ and $y \in \mathbb{Z}_q$ then*

$$\frac{1}{k}\left(\delta_m^{(k)}(x+qy) - \delta_m^{(k)}(x)\right) \equiv y\delta_{m,q}^{(k-1)}(x) \pmod{q}. \tag{2.4}$$

Proof. The case $k = 0$ is trivial, so we assume $k > 0$. Clearly

$$\begin{aligned}\delta_m^{(k)}(x+m) - \delta_m^{(k)}(x) =& m^{k-1}\left(B_k\left(\frac{x}{m}+1\right) - B_k\left(\frac{x}{m}\right) - \left(\frac{x}{m}+1\right)^k + \left(\frac{x}{m}\right)^k\right)\\ =& m^{k-1}\left(k\left(\frac{x}{m}\right)^{k-1} - \sum_{j=0}^{k-1}\binom{k}{j}\left(\frac{x}{m}\right)^j\right) \in \mathbb{Z}[x].\end{aligned}$$

For $w\in\mathbb{Z}_q$ we can choose $a\in\mathbb{Z}$ and $n\in\mathbb{Z}^+$ so that $w\equiv a\pmod q$ and $\frac{m}{(m,q)}n\equiv a\pmod{\frac{q}{(m,q)}}$. Then $(m,q)w\equiv(m,q)a\equiv mn\pmod q$. As $qB_l\in\mathbb{Z}_q$ for all $l\in\mathbb{N}$, we have $\delta_m^{(k)}(x+(m,q)w)-\delta_m^{(k)}(x+mn)\in\mathbb{Z}_q[x]$. On the other hand,

$$\delta_m^{(k)}(x+mn)-\delta_m^{(k)}(x)=\sum_{i=0}^{n-1}\Big(\delta_m^{(k)}(x+im+m)-\delta_m^{(k)}(x+im)\Big)\in\mathbb{Z}[x].$$

So (2.3) holds.

Let $y\in\mathbb{Z}_q$ and $D=(\delta_m^{(k)}(x+qy)-\delta_m^{(k)}(x))/k$. Then

$$\begin{aligned}D&=\frac{m^{k-1}}{k}\sum_{l=1}^{k}\binom{k}{l}\left(B_{k-l}\left(\frac{x}{m}\right)-\left(\frac{x}{m}\right)^{k-l}\right)\left(\frac{qy}{m}\right)^l\\&=\sum_{l=1}^{k}\binom{k-1}{l-1}q\delta_m^{(k-l)}(x)\frac{q^{l-1}}{l}y^l\equiv\delta_{m,q}^{(k-1)}(x)y\pmod q\end{aligned}$$

where in the last step we notice that $\frac{q}{2}y^2\equiv\frac{q}{2}y\pmod q$ and $q^{l-1}/l=qq^{l-2}/l\equiv 0\pmod q$ for $l=3,4,\cdots$. This proves (2.4). □

Lemma 2.3. *Let $m,n\in\mathbb{Z}^+$, $k\in\mathbb{N}$, $w_0,\cdots,w_{n-1},y\in\mathbb{Z}_q$ and $w=qny/m\in\mathbb{Z}_q$. Then*

$$\frac{1}{m}\sum_{i=0}^{n-1}\frac{(x_i+iqy)^{k+1}-x_i^{k+1}}{k+1}-\frac{n-1}{2}wR_{q,n}^{(k)}(x,y)\equiv 0\pmod q\tag{2.5}$$

where $x_i=x+(m,qn)w_i$ and

$$R_{q,n}^{(k)}(x,y)=x^k+\frac{q}{6}(2n-1)kx^{k-1}y+[2\|q]q\binom{k}{3}x^{k-3}y^3.\tag{2.6}$$

Proof. For $t=0,1,2,\cdots$ we set

$$S(t)=\frac{q^t}{(t+1)(t+2)}\sum_{s=0}^{t+1}\binom{t+2}{s+1}B_{t+1-s}n^s.$$

By simple calculations,

$$S(0)=\frac{n-1}{2},\ S(1)=\frac{q}{12}(n-1)(2n-1),\ S(2)=\frac{q^2}{6}(n-1)\binom{n}{2}\equiv 0\pmod q,$$

and

$$\begin{aligned}S(3)&=\frac{q^3}{20}\left(n^4-\frac{5}{2}n^3+\frac{5}{3}n^2-\frac{1}{6}\right)\equiv-\frac{q}{2}n^3\cdot\frac{q^2}{4}+qn^2\cdot\frac{q^2}{12}-\frac{q}{10}\cdot\frac{q^2}{12}\\&\equiv-\frac{q}{2}n\cdot\frac{q}{2}[2\|q]-\frac{q}{10}\cdot\frac{q}{2}[2\|q]\equiv\frac{q}{2}[2\|q](n-1)\pmod q.\end{aligned}$$

For any integer $t>3$, $\frac{q^{t-2}}{(t+1)(t+2)}\in\mathbb{Z}_q$ by the proof of Lemma 2.1(i), and so

$$S(t)=q\cdot\frac{q^{t-2}}{(t+1)(t+2)}\sum_{s=0}^{t+1}\binom{t+2}{s+1}(qB_{t+1-s})n^s\equiv 0\pmod q.$$

Notice that

$$\begin{aligned}&\frac{1}{n}\sum_{t=0}^{k}\binom{k}{t}\frac{q^t}{t+1}x^{k-t}y^t\sum_{i=0}^{n-1}i^{t+1}-\frac{n-1}{2}R_{q,n}^{(k)}(x,y)\\ =&\frac{1}{n}\sum_{t=0}^{k}\binom{k}{t}x^{k-t}y^t\frac{q^t}{t+1}\cdot\frac{B_{t+2}(n)-B_{t+2}}{t+2}-\frac{n-1}{2}R_{q,n}^{(k)}(x,y)\\ =&\sum_{t=0}^{k}\binom{k}{t}x^{k-t}y^tS(t)-\frac{n-1}{2}R_{q,n}^{(k)}(x,y)\equiv 0\pmod q.\end{aligned}$$

Let u and v be integers such that $mu+qnv=(m,qn)$. Then $\frac{qy}{m}(m,qn)=q(uy+vw)\equiv 0\pmod q$. Thus, for the left-hand side L of (2.5) we have

$$\begin{aligned}L=&\frac{1}{m}\sum_{i=0}^{n-1}\frac{1}{k+1}\sum_{j=1}^{k+1}\binom{k+1}{j}x_i^{k+1-j}(iqy)^j-\frac{n-1}{2}wR_{q,n}^{(k)}(x,y)\\ =&\frac{qy}{m}\sum_{j=1}^{k+1}\binom{k}{j-1}\frac{q^{j-1}}{j}y^{j-1}\sum_{i=0}^{n-1}i^jx_i^{k+1-j}-\frac{n-1}{2}wR_{q,n}^{(k)}(x,y)\\ \equiv&\frac{w}{n}\sum_{t=0}^{k}\binom{k}{t}\frac{q^t}{t+1}x^{k-t}y^t\sum_{i=0}^{n-1}i^{t+1}-\frac{n-1}{2}wR_{q,n}^{(k)}(x,y)\equiv 0\pmod q.\end{aligned}$$

This concludes the proof. □

Proof of (1.16). Let p be any prime divisor of $q>2$. Set $k=\varphi(q)$ and $\alpha=\mathrm{ord}_p(q)$. Then

$$\sum_{r=1}^{p-1}r^k=\frac{1}{k+1}\sum_{l=0}^{k}\binom{k+1}{k-l}B_{k-l}p^{l+1}=pB_k+pk\sum_{l=1}^{k}\binom{k-1}{l-1}(pB_{k-l})\frac{p^{l-1}}{l(l+1)}.$$

As $p^\alpha\mid pk$ and $k>\alpha$, we have $p-1\equiv pB_k\pmod{p^\alpha}$ and $(1-p^{k-1})\frac{p}{p-1}B_k\equiv 1\pmod{p^\alpha}$. If $p_*\neq p$ is another prime divisor of q and $\beta=\mathrm{ord}_p(p_*-1)$, then $\varphi(p^{\alpha+\beta})\mid\varphi(q)$ and so p^α divides $(p_*^{\varphi(q)}-1)/(p_*-1)$. Clearly (1.16) follows from the above. □

3. A Crucial Theorem

Lemma 3.1. *Let $k\in\mathbb{N}$, $m\in\mathbb{Z}^+$ and $r\in\mathbb{Z}$. Then*

$$\frac{k+1}{m^k}\sum_{\substack{0\leqslant j<q\\ m\mid j-r}}(x+j)^k=B_{k+1}\left(\frac{x+q}{m}+\left\{\frac{r-q}{m}\right\}\right)-B_{k+1}\left(\frac{x}{m}+\left\{\frac{r}{m}\right\}\right). \quad (3.1)$$

Proof. Let $f(y)=\frac{1}{k+1}B_{k+1}(\frac{x+r}{m}+y)$ for $y\in\mathbb{Z}$. Then $\Delta f(y)=f(y+1)-f(y)=(\frac{x+r}{m}+y)^k$. Note that $1+\lfloor\frac{-1-r}{m}\rfloor=\lfloor\frac{m-1}{m}-\{\frac{r}{m}\}-\lfloor\frac{r}{m}\rfloor\rfloor=-\lfloor\frac{r}{m}\rfloor$. Therefore

$$\begin{aligned}&\frac{1}{m^k}\sum_{\substack{0\leqslant j<q\\ m\mid j-r}}(x+j)^k=\sum_{\substack{0\leqslant j<q\\ m\mid j-r}}\Delta f\left(\frac{j-r}{m}\right)=\sum_{\frac{-1-r}{m}<i\leqslant\frac{q-1-r}{m}}\Delta f(i)\\ =&f\left(\left\lfloor\frac{q-1-r}{m}\right\rfloor+1\right)-f\left(\left\lfloor\frac{-1-r}{m}\right\rfloor+1\right)=f\left(-\left\lfloor\frac{r-q}{m}\right\rfloor\right)-f\left(-\left\lfloor\frac{r}{m}\right\rfloor\right)\\ =&\frac{1}{k+1}\left(B_{k+1}\left(\frac{x+q}{m}+\left\{\frac{r-q}{m}\right\}\right)-B_{k+1}\left(\frac{x}{m}+\left\{\frac{r}{m}\right\}\right)\right).\end{aligned}$$

This ends the proof. □

Remark 3.1. Since (3.1) is our starting point, we'd better give some historical remarks. It was first observed by E. Lehmer ([L]) in the case $x=0$ and $r=q$. In 1991 the author obtained a congruence version of (3.1), then his brother Z.-H. Sun derived (3.1) in the case $x=0$ by a complicated method.

Lemma 3.2. *Let $k\geqslant 0$, $m>0$, $n>0$ and r be integers, and $\lambda\colon\mathbb{N}\to\mathbb{Z}_q$ be a function with $\lambda(0)=0$. Then*

$$\begin{aligned}&\sum_{s=1}^{n}\lambda(s)\sum_{\substack{0\leqslant j<q\\ m\mid j-r-qs}}(x+j)^k\\ \equiv&\frac{m^k}{k+1}\sum_{t=0}^{n-1}\Delta\lambda(t)B_{k+1}\left(\frac{x-qt}{m}+\left\{\frac{r+qt}{m}\right\}\right)\\ &-\frac{m^k}{k+1}\lambda(n)B_{k+1}\left(\frac{x-qn}{m}+\left\{\frac{r+qn}{m}\right\}\right)\pmod q.\end{aligned}$$

Proof. By Lemma 3.1 we have

$$\begin{aligned}&\frac{k+1}{m^k}\sum_{s=1}^{n}\lambda(s)\sum_{\substack{0\leqslant j<q\\ m\mid j-r-qs}}(x-qs+j)^k\\ =&\sum_{s=1}^{n}\lambda(s)B_{k+1}\left(\frac{x-q(s-1)}{m}+\left\{\frac{r+q(s-1)}{m}\right\}\right)\\ &-\sum_{s=1}^{n}\lambda(s)B_{k+1}\left(\frac{x-qs}{m}+\left\{\frac{r+qs}{m}\right\}\right),\end{aligned}$$

so the desired result follows by Abel's partial summation identity. □

Lemma 3.3. *Let $k \in \mathbb{N}$, $m, n \in \mathbb{Z}^+$ and $y \in \mathbb{R}$. Then*

$$n^k \sum_{r=0}^{n-1} B_{k+1}\left(\frac{x}{n} + \left\{\frac{mr+y}{n}\right\}\right) = (m,n)^{k+1} B_{k+1}\left(\frac{x}{(m,n)} + \left\{\frac{y}{(m,n)}\right\}\right).$$

Proof. Set $\bar{w} = w/(m,n)$ for $w \in \{m, n, x, y\}$. Then

$$\begin{aligned}&\sum_{r=0}^{n-1} B_{k+1}\left(\frac{x}{n} + \left\{\frac{mr+y}{n}\right\}\right) = \sum_{u=0}^{\bar{n}-1} \sum_{v=0}^{(m,n)-1} B_{k+1}\left(\frac{x}{n} + \left\{\frac{\bar{m}(u+\bar{n}v)+\bar{y}}{\bar{n}}\right\}\right)\\ =&(m,n)\sum_{u=0}^{\bar{n}-1} B_{k+1}\left(\frac{x}{n} + \left\{\frac{\bar{m}u + \lfloor \bar{y}\rfloor + \{\bar{y}\}}{\bar{n}}\right\}\right) = (m,n)\sum_{t=0}^{\bar{n}-1} B_{k+1}\left(\frac{\bar{x}}{\bar{n}} + \frac{t+\{\bar{y}\}}{\bar{n}}\right).\end{aligned}$$

Applying Raabe's theorem we then obtain the desired identity. □

Now we are ready to give

Theorem 3.1. *Let d, m and n be positive integers for which $d \mid n$ and $m \mid qn$. Let $\bar{d} = (d, qn/m)$, $\bar{m} = (m, qn/d)$, $k \in \mathbb{N}$ and $r \in \mathbb{Z}$. Suppose that $2 \nmid d$ or $2 \nmid q$ or $2 \mid \frac{qn}{m}$. Then*

$$\begin{aligned}&\frac{1}{k+1}\left(dm^k B_{k+1}\left(\frac{x}{m} + \left\{\frac{r}{m}\right\}\right) - \bar{d}\bar{m}^k B_{k+1}\left(\frac{x}{\bar{m}} + \left\{\frac{r}{\bar{m}}\right\}\right)\right)\\ \equiv&\sum_{s=1}^{n}\left(\left\lfloor -\frac{ds}{n}\right\rfloor + \frac{d+1}{2}\right) \sum_{\substack{0\leqslant j<q\\ m\mid j-r-qs}} (x+j)^k\\ &+\left(\frac{q}{4}[4 \mid d] - \frac{q}{3}[3 \mid d]\right)\frac{qn}{m}\cdot\frac{n}{d}k(x+r)^{k-1} \pmod q.\end{aligned} \tag{3.2}$$

Proof. Clearly we may assume $r \in R(m)$. Let $y = n/d$ and $\lambda_d(s) = \lfloor -s/y\rfloor$ for $s \in \mathbb{N}$. Then $\lambda_d(0) = 0$, $\lambda_d(n) = -d$, $\Delta\lambda_d(s) = 0$ if $y \nmid s$, and $\Delta\lambda_d(ty) = -1$ for $t \in \mathbb{N}$. Set

$$x_t = x - qty + m\left\{\frac{r+qty}{m}\right\} \quad \text{for } t \in R(d).$$

Obviously $x_0 = x + r$ and $x_t - x_0 \in m\mathbb{Z}$.

Let $S(a,x) = \sum_{\substack{0\leqslant j<q\\ m\mid j-a}} (x+j)^k$ for $a \in \mathbb{Z}$. By Lemma 3.2, $\sum_{s=1}^{n} \lambda_d(s) S(r+qs, x)$ is congruent to

$$\begin{aligned}&\frac{m^k}{k+1}\sum_{s=0}^{n-1}\Delta\lambda_d(s) B_{k+1}\left(\frac{x-qs}{m} + \left\{\frac{r+qs}{m}\right\}\right)\\ &-\frac{m^k}{k+1}\lambda_d(n) B_{k+1}\left(\frac{x-qn}{m} + \left\{\frac{r+qn}{m}\right\}\right)\\ =&-\frac{m^k}{k+1}\left(\sum_{t=0}^{d-1} B_{k+1}\left(\frac{x_t}{m}\right) - dB_{k+1}\left(\frac{x_0-qn}{m}\right)\right)\end{aligned}$$

modulo q.

In view of the above and Lemmas 2.2 and 2.3,

$$\begin{aligned}
&-\sum_{s=1}^n S(r+qs,x)=\sum_{s=1}^n \lambda_1(s)S(r+qs,x)\\
\equiv&\frac{m^k}{k+1}\left(B_{k+1}\left(\frac{x_0-qn}{m}\right)-B_{k+1}\left(\frac{x_0}{m}\right)\right)\\
=&\frac{\delta_m^{(k+1)}(x_0-qn)-\delta_m^{(k+1)}(x_0)}{k+1}+\frac{1}{m}\cdot\frac{(x_0-qn)^{k+1}-x_0^{k+1}}{k+1}\\
\equiv&-n\delta_{m,q}^{(k)}(x_0)+\frac{2-1}{2}\cdot\frac{q2(-n)}{m}R_{q,2}^{(k)}(x_0,-n)\\
\equiv&-n\delta_{m,q}^{(k)}(x_0)-\frac{qn}{m}\left(x_0^k+\frac{q}{6}(2\cdot 2-1)kx_0^{k-1}(-n)\right)\pmod q.
\end{aligned}$$

If $2\mid(d,q)$, then $m\mid q\frac{n}{2}$ and hence

$$\begin{aligned}
&\frac{1}{2}\sum_{s=1}^n S(r+qs,x)=\sum_{s=1}^{n/2}S(r+qs,x)\\
\equiv&\frac{n}{2}\delta_{m,q}^{(k)}(x_0)+\frac{qn/2}{m}\left(x_0^k-\frac{q}{2}\cdot\frac{n}{2}kx_0^{k-1}\right)\pmod q
\end{aligned}$$

in a similar way. If $2\nmid d$ or $2\nmid q$, then $(d+1)/2\in\mathbb{Z}_q$. Therefore the right-hand side of the congruence (3.2) belongs to $\mathbb{Z}_q[x]$, and

$$\begin{aligned}
S:=&\frac{d+1}{2}\sum_{s=1}^n S(r+qs,x)+\frac{dm^k}{k+1}\left(B_{k+1}\left(\frac{x_0-pn}{m}\right)-B_{k+1}\left(\frac{x_0}{m}\right)\right)\\
\equiv&\frac{d+1}{2}n\delta_{m,q}^{(k)}(x_0)+\frac{d+1}{2}\cdot\frac{qn}{m}\left(x_0^k-\frac{q}{2}\cdot\frac{n}{(2,d,q)}kx_0^{k-1}\right)\\
&-dn\delta_{m,q}^{(k)}(x_0)-d\frac{qn}{m}\left(x_0^k-\frac{q}{2}nkx_0^{k-1}\right)\\
\equiv&\frac{1-d}{2}n\delta_{m,q}^{(k)}(x_0)+\frac{1-d}{2}\cdot\frac{qn}{m}\left(x_0^k+\frac{q}{2}\cdot\frac{n}{(2,d,q)}kx_0^{k-1}\right)\pmod q.
\end{aligned}$$

We also have

$$\begin{aligned}
&\sum_{s=1}^n\left(\left\lfloor-\frac{ds}{n}\right\rfloor+\frac{d+1}{2}\right)S(r+qs,x)\\
=&\sum_{s=1}^n\lambda_d(s)S(r+qs,x)+\frac{d+1}{2}\sum_{s=1}^n S(r+qs,x)\\
\equiv&\frac{m^k}{k+1}\left(dB_{k+1}\left(\frac{x_0}{m}\right)-\sum_{t=0}^{d-1}B_{k+1}\left(\frac{x_t}{m}\right)\right)+S=W+R+S\pmod q
\end{aligned}$$

where

$$W=\frac{m^k}{k+1}\bigg(dB_{k+1}\left(\frac{x_0}{m}\right)-\sum_{t=0}^{d-1}B_{k+1}\bigg(\frac{x_t+tqy}{m}\bigg)\bigg)$$

and

$$R=\frac{m^k}{k+1}\sum_{t=0}^{d-1}\bigg(B_{k+1}\left(\frac{x_t+tqy}{m}\right)-B_{k+1}\left(\frac{x_t}{m}\right)\bigg).$$

In light of Lemma 3.3 and the equality $d\bar{m}=\bar{d}m$,

$$\begin{aligned}&-(k+1)W+dm^kB_{k+1}\bigg(\frac{x}{m}+\left\{\frac{r}{m}\right\}\bigg)=m^k\sum_{t=0}^{d-1}B_{k+1}\left(\frac{x}{m}+\left\{\frac{r}{m}+\frac{qn}{m}\cdot\frac{t}{d}\right\}\right)\\&=m^k\frac{\bar{d}^{k+1}}{d^k}B_{k+1}\bigg(\frac{dx/m}{\bar{d}}+\left\{\frac{dr/m}{\bar{d}}\right\}\bigg)=\bar{d}\bar{m}^kB_{k+1}\bigg(\frac{x}{\bar{m}}+\left\{\frac{r}{\bar{m}}\right\}\bigg).\end{aligned}$$

Let $D=\frac{1}{(k+1)m}\sum_{t=0}^{d-1}((x_t+tqy)^{k+1}-x_t^{k+1})$. By Lemma 2.2,

$$R-D\equiv\sum_{t=0}^{d-1}ty\delta_{m,q}^{(k)}(x_t)\equiv\frac{d(d-1)}{2}y\delta_{m,q}^{(k)}(x_0)\pmod q.$$

Since $\frac{d-1}{2}\cdot\frac{qdy}{m}=\frac{d-1}{2}\cdot\frac{qn}{m}\in\mathbb{Z}_q$, applying Lemma 2.3 we get

$$D\equiv\frac{d-1}{2}\cdot\frac{qdy}{m}R_{q,d}^{(k)}(x_0,y)\equiv\frac{d-1}{2}\cdot\frac{qn}{m}\left(x_0^k+\frac{q}{6}(2d-1)kx_0^{k-1}y\right)\pmod q.$$

It follows that

$$\begin{aligned}(R-D)+D+S\equiv&\frac{d-1}{2}\cdot\frac{qn}{m}\cdot\frac{n}{d}kx_0^{k-1}\left((2d-1)\left(\frac{q}{2}-\frac{q}{3}\right)-\frac{q}{2}\cdot\frac{d}{(2,d,q)}\right)\\\equiv&\left(\frac{q}{3}[3\mid d]-\frac{q}{4}[4\mid d]\right)\frac{qn}{m}\cdot\frac{n}{d}kx_0^{k-1}\pmod q.\end{aligned}$$

Combining the above we obtain (3.2). □

4. General Version of Voronoi's Congruences

Lemma 4.1. *Let $k\in\mathbb{N}$, $d,m,n\in\mathbb{Z}^+$, $d\mid n$, $m\mid qn$ and $r\in R(m)$. Let f be any function from $\mathbb{Z}$ to $\mathbb{Z}_q$. Then*

$$\begin{aligned}&\sum_{s=1}^{n}f\left(\left\lfloor-\frac{ds}{n}\right\rfloor\right)\sum_{\substack{0\leqslant j<q\\ m\mid j-r-qs}}(x+j)^k\\&\equiv\sum_{j=0}^{qn/m-1}(x+r+jm)^kf\left(\left\lfloor\frac{r+jm}{qn/d}\right\rfloor-d\right)\pmod q.\end{aligned}\tag{4.1}$$

Proof. Let R denote the right-hand side of the congruence (4.1). Then

$$\begin{aligned}R=&\sum_{\substack{0\leqslant a<qn\\ a\equiv r\pmod m}}(x+a)^kf\bigg(\left\lfloor\frac{ad}{qn}\right\rfloor-d\bigg)=\sum_{\substack{1\leqslant b\leqslant qn\\ m\mid qn-b-r}}(x+qn-b)^kf\bigg(\left\lfloor\frac{-bd}{qn}\right\rfloor\bigg)\\ \equiv&\sum_{\substack{1\leqslant b\leqslant qn\\ m\mid b+r}}(x-b)^kf\bigg(\left\lfloor\frac{-b/q}{n/d}\right\rfloor\bigg)=\sum_{s=1}^n\sum_{\substack{0\leqslant j<q\\ m\mid qs-j+r}}(x+j-qs)^kf\bigg(\left\lfloor\frac{(j-qs)/q}{n/d}\right\rfloor\bigg)\\ \equiv&\sum_{s=1}^n\sum_{\substack{0\leqslant j<q\\ m\mid j-r-qs}}(x+j)^kf\bigg(\left\lfloor\frac{-s}{n/d}\right\rfloor\bigg)\pmod q.\end{aligned}$$

This completes the proof. □

Lemma 4.2. *Let $k\in\mathbb{N}$, $m,n\in\mathbb{Z}^+$, $2\mid n$ and $2m\mid qn$. Then*

$$\begin{aligned}&\sum_{j=0}^{qn/(2m)-1}(x+jm)^k-\frac12\sum_{j=0}^{qn/m-1}(x+jm)^k\\ \equiv&\frac{q}{2}k[2\|n]\left([q\sim_2 m]x^{k-1}+[2\|q\wedge 2\nmid m]\Delta(x^{k-1})\right)\pmod q.\end{aligned}\tag{4.2}$$

Proof. Since $\frac12(q\frac{n}{2})^2=q\frac{q}{2}(\frac{n}{2})^2\equiv 0\pmod q$, if $j\in\mathbb{Z}$ then

$$\begin{aligned}d_j:=&\frac12\bigg((x+jm)^k-\Big(x+jm+q\frac{n}{2}\Big)^k\bigg)\\ \equiv&-\frac{k}{2}(x+jm)^{k-1}q\frac{n}{2}=-\frac{q}{2}k\frac{n}{2}\bigg(x^{k-1}+\sum_{0<l<k}\binom{k-1}{l}(jm)^lx^{k-1-l}\bigg)\\ \equiv&\frac{q}{2}k[2\|n]\left(x^{k-1}+jm\left((x+1)^{k-1}-x^{k-1}\right)\right)\pmod q.\end{aligned}$$

As the left-hand side d of the congruence (4.2) equals $\sum_{0\leqslant j<qn/(2m)}d_j$, we have

$$\begin{aligned}d\equiv&\frac{q}{2}k[2\|n]\left(\frac{qn}{2m}x^{k-1}+\frac{m}{2}\cdot\frac{qn}{2m}\left(\frac{qn}{2m}-1\right)\Delta(x^{k-1})\right)\\ \equiv&\frac{q}{2}k[2\|n]\left(\left[2\nmid\frac{qn}{2m}\right]x^{k-1}+\left[2\nmid m\wedge 2\|\frac{qn}{2m}\right]\Delta(x^{k-1})\right)\pmod q\end{aligned}$$

and this concludes the proof. □

Now we are able to give

Theorem 4.1. *Let $k\in\mathbb{N}$, $d,m,n\in\mathbb{Z}^+$, $d\mid n$, $m\mid qn$, and $2\nmid d$ or $2\nmid q$ or $2\mid\frac{qn}{m}$. Put $\bar d=(d,qn/m)$ and $\bar m=(m,qn/d)$. Then for any $y\in\mathbb{R}$ the polynomial*

$$L(x,y)=\frac{1}{k+1}\left(dm^kB_{k+1}\left(\frac{x}{m}\right)-\bar d\bar m^kB_{k+1}\left(\frac{x}{\bar m}-\left\lfloor\frac{y}{\bar m}\right\rfloor\right)\right)\tag{4.3}$$

is in $\mathbb{Z}_q[x]$ *and is congruent to*

$$R(x,y)=\sum_{j=0}^{qn/m-1}(x+jm)^k\left(\left\lfloor\frac{y+jm}{qn/d}\right\rfloor+\frac{1-d}{2}\right)-\frac{q}{3}[3\mid d]\frac{n}{d}\cdot\frac{qn}{m}kx^{k-1}$$
$$+\frac{q}{2}k[d\sim_2 n]\left(\left[2\mid n\wedge 2\|\frac{qn}{m}\right]x^{k-1}+[2\nmid m\wedge 2\|n\wedge 2\|q]\Delta(x^{k-1})\right)$$

modulo q.

Proof. Clearly

$$L(x+m,y+m)-L(x,y)=\frac{dm^k}{k+1}\left(B_{k+1}\left(\frac{x}{m}+1\right)-B_{k+1}\left(\frac{x}{m}\right)\right)=dx^k.$$

Since $\frac{q}{2}[2\mid n\wedge 2\|\frac{qn}{m}]m\equiv 0 \pmod q$ and $qn\frac{d-1}{2}=q\frac{n}{d}\binom{d}{2}\equiv 0 \pmod q$, we also have

$$\begin{aligned}&R(x+m,y+m)-R(x,y)\\ \equiv&\sum_{i=1}^{qn/m}(x+im)^k\left(\left\lfloor\frac{y+im}{qn/d}\right\rfloor+\frac{1-d}{2}\right)-\sum_{j=0}^{qn/m-1}(x+jm)^k\left(\left\lfloor\frac{y+jm}{qn/d}\right\rfloor+\frac{1-d}{2}\right)\\ =&(x+qn)^k\left(\left\lfloor\frac{y+qn}{qn/d}\right\rfloor+\frac{1-d}{2}\right)-x^k\left(\left\lfloor\frac{y}{qn/d}\right\rfloor+\frac{1-d}{2}\right)\equiv dx^k \pmod q.\end{aligned}$$

So we can assume $y\in[0,m)$ without any loss of generality.

Let $r=\lfloor y\rfloor$. Then $L(x,y)=L(x,r)$ and $R(x,y)=R(x,r)$. By Theorem 3.1, $L(x,r)$ is in $\mathbb{Z}_q[x]$ and is congruent to

$$\sum_{s=1}^{n}\left(\left\lfloor-\frac{ds}{n}\right\rfloor+\frac{d+1}{2}\right)\sum_{\substack{0\leqslant j<q\\ m\mid j-r-qs}}(x-r+j)^k+\left(\frac{q}{4}[4\mid d]-\frac{q}{3}[3\mid d]\right)\frac{qn}{m}\cdot\frac{n}{d}kx^{k-1}$$

modulo q. Set

$$P(x)=\sum_{j=0}^{qn/m-1}(x+jm)^k\left(\left\lfloor\frac{r+jm}{qn/d}\right\rfloor+\frac{1-d}{2}\right).$$

If $2\nmid(d,q)$, then $\frac{d+1}{2}\in\mathbb{Z}_q$ and hence

$$L(x,r)\equiv P(x)-\frac{q}{3}[3\mid d]\frac{qn}{m}\cdot\frac{n}{d}kx^{k-1}\equiv R(x,r) \pmod q$$

with the help of Lemma 4.1. In the case $2\mid(d,q)$, by Lemmas 4.1 and 4.2 we have

$$\begin{aligned}&L(x,r)+\frac{q}{3}[3\mid d]\frac{n}{d}\cdot\frac{qn}{m}kx^{k-1}-\frac{q}{2}[4\mid d]\frac{n}{d}\cdot\frac{qn}{2m}kx^{k-1}\\ \equiv&\sum_{s=1}^{n}\left(\left\lfloor-\frac{ds}{n}\right\rfloor+\frac{d}{2}\right)\sum_{\substack{0\leqslant j<q\\ m\mid j-r-qs}}(x-r+j)^k+\sum_{s=1}^{n/2}\sum_{\substack{0\leqslant j<q\\ m\mid j-r-qs}}(x-r+j)^k\\ \equiv&\sum_{j=0}^{qn/m-1}(x+jm)^k\left(\left\lfloor\frac{r+jm}{qn/d}\right\rfloor-\frac{d}{2}\right)+\sum_{j=0}^{qn/(2m)-1}(x+jm)^k\\ \equiv&P(x)+\frac{q}{2}k[2\|n]\left([q\sim_2 m]x^{k-1}+[2\|q\wedge 2\nmid m]\Delta(x^{k-1})\right)\pmod q,\end{aligned}$$

therefore $L(x,r)\equiv R(x,r)\pmod q$. We are done. □

Proof of Theorem 1.1. Simply apply Theorem 4.1 with $n=m$ and $y=cm/d$. □

5. Proofs of Theorems 1.2–1.5

Lemma 5.1. *Let d,k,m,n be positive integers with $(m,q)=1$ and $d\mid(n,q)$, and x,y be q-adic numbers with $nx\in\mathbb{Z}_q$ and $mx-y\in a+(q^2/d)\mathbb{Z}_q$ where $a\in\mathbb{Z}$. Then*

$$\frac{m^kB_k(x)-B_k(y)}{km^{k-1}}-\sum_{j=0}^{q/d-1}\left(\left\lfloor\frac{a+jm}{q/d}\right\rfloor+\frac{1-m}{2}\right)(x+j)^{k-1}\in\frac{q}{n^{k-1}}\mathbb{Z}_q.\tag{5.1}$$

Proof. Write $mx-y=a+(q^2/d)z$ where $z\in\mathbb{Z}_q$. For $1\leqslant l\leqslant k$, $(q^2/d)^{l-1}/l=(q/d)^{l-1}q^{l-1}/l\in\mathbb{Z}_q$ by Lemma 2.1, and

$$\frac{q}{d}B_{k-l}(y)n^{k-l}=\frac{q}{d}(ny)^{k-l}+\sum_{0<h\leqslant k-l}\binom{k-l}{h}(qB_h)(ny)^{k-l-h}\frac{n^h}{d}\in\mathbb{Z}_q$$

since $ny=m(nx)-n(mx-y)\in\mathbb{Z}_q$. Thus

$$\begin{aligned}&\frac{n^{k-1}}{k}\left(B_k(mx-a)-B_k(y)\right)=\frac{n^{k-1}}{k}\sum_{l=1}^{k}\binom{k}{l}\left(\frac{q^2}{d}z\right)^lB_{k-l}(y)\\ =&q\sum_{l=1}^{k}\binom{k-1}{l-1}\frac{(q^2/d)^{l-1}}{l}z^l\frac{q}{d}B_{k-l}(y)n^{k-1}\equiv0\pmod q.\end{aligned}$$

Let $d'=m$, $n'=mn/d$, $m'=mn$, $x'=m'x\in\mathbb{Z}_q$ and $y'=an\in\mathbb{Z}$. Clearly $d'\mid n'$, $m'\mid qn'$, $(d',q)=1$, $(d',qn'/m')=(m,q/d)=1$ and $(m',qn'/d')=(mn,qn/d)=(m,q/d)n=n$. By Theorem 4.1,

$$\begin{aligned}&\frac{1}{k}\left(d'(m')^{k-1}B_k\left(\frac{x'}{m'}\right)-n^{k-1}B_k\left(\frac{x'}{n}-\left\lfloor\frac{y'}{n}\right\rfloor\right)\right)\\ \equiv&\sum_{j=0}^{qn'/m'-1}\left(\left\lfloor\frac{y'+jm'}{qn'/d'}\right\rfloor+\frac{1-d'}{2}\right)(x'+jm')^{k-1}\pmod q.\end{aligned}$$

As $\frac{n^{k-1}}{k}\left(m^kB_k(x)-B_k(y)\right)\equiv\frac{1}{k}\left(d'(m')^{k-1}B_k(x)-n^{k-1}B_k(mx-a)\right)\pmod q$, the desired result follows. □

Proof of Theorem 1.2. For $d\in\mathbb{Z}^+$ with $d\mid q$, let $a_d=\langle m[x]_d-[y]_d\rangle_{q^2}$ and $\psi(d)=(\langle mx-y\rangle_{q^2}+m\langle -x\rangle_d)/d$. Then $\lfloor\psi(d)\rfloor\in a_d+(q^2/d)\mathbb{Z}_q$ because

$$d\lfloor\psi(d)\rfloor\equiv mx-y+m\langle -x\rangle_d-\langle -y\rangle_d=d(m[x]_d-[y]_d)\equiv da_d\pmod{q^2}.$$

Since $[(x+j,q)=1]=\sum_{d\mid(x+j,q)}\mu(d)$, the right-hand side of the congruence (1.14) equals $\sum_{d\mid q}\mu(d)\Psi(d)$ where

$$\begin{aligned}\Psi(d)=&\sum_{\substack{j=0\\ d\mid j-\langle -x\rangle_d}}^{q-1}\left(\left\lfloor\frac{\langle mx-y\rangle_{q^2}+jm}{q}\right\rfloor+\frac{1-m}{2}\right)(x+j)^{k-1}\\ =&\sum_{i=0}^{q/d-1}\left(\left\lfloor\frac{\langle mx-y\rangle_{q^2}+m(\langle -x\rangle_d+id)}{q}\right\rfloor+\frac{1-m}{2}\right)(x+\langle -x\rangle_d+id)^{k-1}\\ =&d^{k-1}\sum_{i=0}^{q/d-1}\left(\left\lfloor\frac{\psi(d)+im}{q/d}\right\rfloor+\frac{1-m}{2}\right)([x]_d+i)^{k-1}\end{aligned}$$

By Lemma 5.1, $\Psi(d)\equiv\frac{d^{k-1}}{km^{k-1}}\left(m^kB_k([x]_d)-B_k([y]_d)\right)\pmod q$. We are done. □

Lemma 5.2. *For some $m\in\mathbb{Z}^+$ with $(m,q)=1$, we can find $c_j\in\mathbb{Z}_q$ $(j\in R_*(q))$ such that*

$$\frac{1}{m^k-1}\equiv\sum_{j\in R_*(q)}c_jj^k\pmod q\ \text{ for all } k\in S_q.\tag{5.2}$$

Proof. Write $q=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ where $p_1,\cdots,p_r$ are distinct primes and $\alpha_1,\cdots,\alpha_r\in\mathbb{Z}^+$. For each $i=1,\cdots,r$ let g_i be a primitive root modulo p_i. By the Chinese Remainder Theorem, there exists an integer $\delta_i\equiv1\pmod{p_i^{\alpha_i}}$ divisible by $q/p_i^{\alpha_i}$, also there is a positive integer m such that $m\equiv m_i\pmod{p_i^{\alpha_i}}$ for all $i=1,\cdots,r$ where $m_i=g_i^{p_i^{\alpha_i-1}}$. Clearly $(m,q)=1$ since $p_i\nmid m_i$.

Let $k\in S_q$. Then $m_i^k\not\equiv1\pmod{p_i}$, $\sum_{j=0}^{p_i-2}m_i^{jk}=(m_i^{(p_i-1)k}-1)/(m_i^k-1)\equiv0\pmod{p_i^{\alpha_i}}$ and so

$$\begin{aligned}(m_i^k-1)\sum_{j=0}^{p_i-2}jm_i^{jk}=&(p_i-2)m_i^{(p_i-1)k}+\sum_{0<j\leqslant p_i-2}(j-1-j)m_i^{jk}\\ \equiv&p_i-2+1-\sum_{j=0}^{p_i-2}m_i^{jk}\equiv p_i-1\pmod{p_i^{\alpha_i}}.\end{aligned}$$

Therefore

$$\frac{1}{m^k-1}\equiv-\sum_{i=1}^r\delta_i\frac{p_i^{\alpha_i}-1}{p_i-1}\sum_{j=0}^{p_i-2}jm^{jk}\pmod q,$$

which concludes the proof. □

Proof of Theorem 1.3. Choose an $m\in\mathbb{Z}^+$ with $(m,q)=1$ as in Lemma 5.2. By Theorem 1.2 the function

$$f(k)=(m^k-1)\sum_{d\mid q}\mu(d)\frac{d^{k-1}}{k}B_k([x]_d)\quad(k\in\mathbb{Z}^+)$$

is q-normal. So the first part of Theorem 1.3 follows.

Let $l\in S_q$. By part (i), (1.20) holds if $n=0$. Let $n\in\mathbb{Z}^+$. Then there are $c_r\in\mathbb{Z}_q$ $(r\in R_*(q^n))$ such that

$$\sum_{d\mid q}\mu(d)\frac{d^{k-1}}{k}B_k([x]_d)=\sum_{d\mid q^n}\mu(d)\frac{d^{k-1}}{k}B_k([x]_d)\equiv\sum_{r\in R_*(q^n)}c_r r^k\pmod{q^n}$$

for all $k\in\mathbb{Z}^+$ with $k\equiv l\pmod{\varphi(q)}$. This implies (1.20) because

$$\sum_{k=0}^n\binom{n}{k}(-1)^k r^{k\varphi(q)+l}=r^l\left(1-r^{\varphi(q)}\right)^n\equiv 0\pmod{q^n}\text{ for all }r\in R_*(q^n).$$

We are done. □

Proof of Theorem 1.4. Let q' be any positive integer dividing q and divisible by $r(q)$. Let $d\in\mathbb{Z}^+$, $d\mid q$ and $\mu(d)\neq 0$. Obviously $d\mid q'$. If $a\in R(m)$, then $m[\frac{q'x}{m}+\{\frac{da}{m}\}]_d=\frac{q'}{d}x+a$ because

$$d\frac{(q'/d)x+a}{m}-\left(\frac{q'x}{m}+\left\{\frac{da}{m}\right\}\right)=\left\lfloor\frac{da}{m}\right\rfloor\in R(d).$$

Thus, for any $k\in\mathbb{Z}^+$ we have

$$m^{1-k}\chi(d)B_{k,\chi}\left(\frac{q'}{d}x\right)=\chi(d)\sum_{a=0}^{m-1}\chi(a)B_k\left(\frac{(q'/d)x+a}{m}\right)$$
$$=\sum_{a=0}^{m-1}\chi(da)B_k\left(\left[\frac{q'x}{m}+\left\{\frac{da}{m}\right\}\right]_d\right)=\sum_{r=0}^{m-1}\chi(r)B_k\left(\left[\frac{q'x+r}{m}\right]_d\right).$$

It is well known that $\sum_{r=0}^{m-1}\chi(r)=0$ if $\chi\neq\chi_0$. By the above,

$$\sum_{d\mid q}\mu(d)\chi(d)\frac{d^{k-1}}{k}\left(B_{k,\chi}\left(\frac{q'}{d}x\right)-[\chi=\chi_0]B_k\right)=\frac{1}{m}\sum_{r=0}^{m-1}\chi(r)\Delta_r$$

where

$$\begin{aligned}\Delta_r &= \sum_{d\mid q}\mu(d)\frac{d^{k-1}}{k}\left(m^kB_k\left(\left[\frac{q'x+r}{m}\right]_d\right)-B_k\right)\\ &\equiv m^{k-1}\sum_{\substack{0\leqslant j<q\\(\frac{q'x+r}{m}+j,q)=1}}\left(\left\lfloor\frac{\langle q'x+r\rangle_{q^2}+jm}{q}\right\rfloor+\frac{1-m}{2}\right)\left(\frac{q'x+r}{m}+j\right)^{k-1}\\ &\equiv \sum_{\substack{0\leqslant j<q\\(r+jm,q)=1}}\left(\left\lfloor\frac{\langle q'x\rangle_{q^2}+r+jm}{q}\right\rfloor+\frac{1-m}{2}\right)(q'x+r+jm)^{k-1}\pmod q.\end{aligned}$$

by Theorem 1.2. Taking $q'=r(q)$ we then obtain the first part of Theorem 1.4.

The second part follows from the first part as in the proof of Theorem 1.3. □

Remark 5.1. By the proofs of Theorems 1.3 and 1.4, we can replace $\varphi(q)$ in (1.20) and (1.23) by any (positive) multiple of $\varphi(q)$.

Proof of Theorem 1.5. Let m be any positive integer with $(m,q)=1$. Since $n\mid q^h$ for sufficiently large h, $mx\in\mathbb{Z}+n\mathbb{Z}_q$ and hence we can let $\langle mx\rangle_n$ denote the unique $a\in R(n)$ such that $mx\in a+n\mathbb{Z}_q$. Let

$$H_m(k)=\frac{n^{k-1}}{k}\left(m^kB_k\left(\frac{x}{n}\right)-B_k\left(\frac{\langle mx\rangle_n}{n}\right)\right)\quad\text{for } k\in\mathbb{Z}^+.$$

As $(\frac{x}{n}n+jn,r(q))=(x,r(q))=1$ for $j\in R(q)$, the function H_m is q-normal by Lemma 5.1.

Observe that

$$\sum_{m\in R_*(n)}H_m(k)=\frac{n^{k-1}}{k}\left(S_k(n)B_k\left(\frac{x}{n}\right)-\sum_{r\in R_*(n)}B_k\left(\frac{r}{n}\right)\right).$$

By (1.2), $\sum_{d\mid l}\sum_{c\in R_*(d)}B_k(\frac{c}{d})=l^{1-k}B_k$ for all $l\in\mathbb{Z}^+$; applying the Möbius inversion formula we get that

$$\sum_{r\in R_*(n)}B_k\left(\frac{r}{n}\right)=\sum_{d\mid n}\mu(d)\left(\frac{n}{d}\right)^{1-k}B_k=n^{1-k}\varphi_k(n)B_k.$$

So the function $H^*(k)=S_k(n)\frac{n^{k-1}}{k}B_k(\frac{x}{n})-\varphi_k(q)\frac{B_k}{k}$ is q-normal. By Corollary 1.4, for any $m\in\mathbb{Z}^+$ with $(m,q)=1$, the function $f_m(k)=(m^k-1)\varphi_k(q)\frac{B_k}{k}$ is also q-normal. Let $H_*(k)=\sum_{m\in R_*(n)}f_m(k)=(S_k(n)-\varphi(n))\varphi_k(q)\frac{B_k}{k}$. Then $H(k)=\varphi(n)H^*(k)-H_*(k)$ is q-normal. In light of Lemma 5.2 and the above, we also have the second part of Theorem 1.5. □

Acknowledgment. The author is indebted to the referees for their many helpful suggestions.

References

[B] H. F. Baker, *Remark on the Eisenstein–Sylvester extension of Fermat's theorem*, Proc. London Math. Soc. **4** (1906), 131–135.

[C] L. Carlitz, *Some congruences for the Bernoulli numbers*, Amer. J. Math. **75** (1953), 163–172.

[DSS] K. Dilcher, L. Skula and I. S. Slavutskii, *Bernoulli numbers—Bibliography (1713–1990)*, Queen's Papers in Pure and Appl. Math. **87** (1991). The web site of the on-line version is `http://www.mathstat.dal.ca/~dilcher/bernoulli.html`.

[E] A. Erdélyi et al., *Higher Transcendental Functions*, vol. I, McGraw-Hill, New York, 1953, Chapter 1.

[Er] R. Ernvall, *Generalized irregular primes*, Mathematika **30** (1983), 67–73.

[IR] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory* (Graduate texts in mathematics; 84), 2nd ed., Springer-Verlag, New York, 1990, Chapter 15.

[L] E. Lehmer, *On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson*, Ann. Math. **39** (1938), 350–360.

[Le] M. Lerch, *Sur les théorèmes de Sylvester concernant le quotient de Fermat*, C. R. Acad. Sci. Paris **142** (1906), 35–38.

[M] K. Mahler, *Introduction to p-adic Numbers and their Functions*, Cambridge Univ. Press, Cambridge, 1973.

[R] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, New York, 1979, §2, 3, 4 in Chapter VI.

[S] Z.-H. Sun, *Congruences concerning Bernoulli numbers and Bernoulli polynomials*, Discrete Appl. Math. **105** (2000), 193–223.

[UW] J. Urbanowicz and K. S. Williams, *Congruences for L-Functions*, Kluwer, Dordrecht, 2000, Chapter 1.

[W] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag, New York, 1982, Chapter 4 and §5.2, 5.3, 5.6.

[Y1] P. T. Young, *Congruences for Bernoulli, Euler, and Stirling numbers*, J. Number Theory **78** (1999), 204–227.

[Y2] P. T. Young, *Kummer congruences for values of Bernoulli and Euler polynomials*, Acta Arith. **99** (2001), 277–288.