A Series of New Congruences for Bernoulli Numbers and Eisenstein Series

Ernst-Ulrich Gekeler

Fachrichtung 6.1 - Mathematik, Universität des Saarlandes, Postfach 15 11 50, D-66041 Saarbrücken, Germany
E-mail: gekeler@math.uni-sb.de

Communicated by K. Ribet

Received October 2, 2001; revised February 1, 2002

We prove congruences of shape \( E_{k+h} \equiv E_k \cdot E_h \mod N \) modulo powers \( N \) of small prime numbers \( p \), thereby refining the well-known Kummer-type congruences modulo these \( p \) of the normalized Eisenstein series \( E_k \). The method uses Serre’s theory of Iwasawa functions and \( p \)-adic Eisenstein series; it presents a rather general procedure to find and verify such congruences with a modest amount of numerical calculation. © 2002 Elsevier Science (USA)

1. INTRODUCTION, NATURE OF RESULTS

We let \( E_k \) (\( k \geq 4 \) even) be the normalized Eisenstein series of weight \( k \) for the modular group \( \text{SL}(2, \mathbb{Z}) \), given through its \( q \)-expansion

\[
E_k = 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n)q^n. \tag{1.1}
\]

Here \( B_k = 1, -\frac{1}{2}, \frac{1}{6}, 0, -\frac{1}{30}, \ldots \) are the Bernoulli numbers defined by

\[
\frac{X}{e^X - 1} = \sum_{k \geq 0} \frac{B_k}{k!} X^k \quad \text{and} \quad \sigma_k(n) = \sum_{d | n} d^k.
\]

We regard the \( E_k \) as formal power series in the indeterminate \( q \). Quite generally, if \( f, g \in \mathbb{Q}[[q]] \) are power series and \( N \) is a natural number, \( f \equiv g \mod N \) means that \( f \) and \( g \) are both \( N \)-integral and the congruence holds coefficientwise. A weakened version of one of our results is
Let \( k \geq 4 \) be an even natural number and \( N := 2^7 \cdot 3^4 \cdot 5^3 \cdot 7^2 \cdot 13 \). Then

\[
E_{k+12} \equiv E_k \cdot E_{12} \pmod{N}
\]

This congruence was announced in [1], where some related arithmetic properties of the \( E_k \) were studied.

Let \( p \) be a prime number, \( p > 2 \), to fix ideas. It is an easy consequence of (1.1) and the congruences of Kummer and Clausen-von Staudt for the \( B_k \) (see e.g. [9, pp. 55, 241]) that

\[
E_k \equiv 1 \pmod{p^r} \quad \text{if} \quad k \equiv 0 \pmod{(p-1)p^{r-1}}
\]

and

\[
E_k \equiv E_\ell \pmod{p^r} \quad \text{if} \quad k \equiv \ell \pmod{(p-1)p^r},
\]

(1.3)
k, \( \ell \geq r + 1 \), and \((k,p),(\ell,p)\) are regular. The last condition signifies that \( p \) does not divide (the numerator of) \( B_k \). It depends only on the residue class of \( k \pmod{p-1} \) and therefore holds simultaneously for \( k \) and \( \ell \).

The congruence \( \pmod{13} \) in (1.2) immediately results from (1.3), as is the case with the congruences modulo 7, 5 or 3^2. We will reduce the verification of the stronger congruence (1.2) to a (small) finite number of numerical checks. There are three steps:

(a) Of course, (1.2) may be proved separately for the relevant powers \( p^r \) of \( p = 2, 3, 5, 7, 13 \). Fixing such a \( p \), we replace \( E_k \) by its “\( p \)-smoothed” version \( E_k^* \) (see Section 2), which does not essentially affect the validity of (1.2).

(b) The congruence

\[
E_{k+12}^* \equiv E_k^* \cdot E_{12}(\pmod{p^r})
\]

(1.2*)
is doubly infinite (in \( k \) and \( n = \text{exponent of } q^n \)) and can therefore not be directly verified through calculation.

For \( n \geq 0 \) and any modular form \( f \), let \( a_n(f) \) be its \( n \)th Fourier coefficient. Fix \( n \geq 0 \) and consider the function

\[
a_n : k \mapsto a_n(E_{k+12}^* - E_k^*E_{12}).
\]

On each residue class modulo \( p - 1 \) (that is, if \( p \neq 2 \); as usual, this must be somewhat modified for \( p = 2 \)), \( a_n \) gives rise to an Iwasawa function \( f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p \) (see Sections 3 and 4). Now it is a basic property of Iwasawa functions \( g \) that

\[
g(\mathbb{Z}_p) \subset p^r\mathbb{Z}_p \iff g(i) \equiv 0 \pmod{p^r}, \quad i = 0, 1, \ldots, r - 1.
\]

(1.4)
Therefore (1.2*) holds for all \( k \) on the \( n \)th coefficient if and only if this is the case for a certain finite set \( \mathcal{K}_0 = \mathcal{K}_0(p') \subset \mathcal{K} = \{4, 6, 8, \ldots\} \) of weights \( k \) depending only on \( p' \) but not on \( n \).

(c) We now use the \( q \)-expansion principle in the following form:

\[
\text{(1.5) Let } f = \sum_{n \geq 0} a_n q^n \text{ be a modular form of weight } k_0 \text{ with coefficients in } \mathbb{Z}(p) = \mathbb{Q} \cap \mathbb{Z}_p. \text{ If } a_n \equiv 0 \pmod{p'} \text{ for } n \leq k_0/12 \text{ then } f \equiv 0 \pmod{p'}, \text{ i.e., all its coefficients } a_n \text{ satisfy the congruence.}
\]

The principle follows with easy considerations like e.g. [1, 2.3] from the traditional form as given in [5, pp. 144/145] or [2, pp. 132–134], say. See also [8], where the case \( r = 1 \) is treated. Applying it with \( k_0 := \max \mathcal{K}_0(p') + 12 \), we reduce the proof of (1.2) to its checking for a finite number of pairs \((k, n)\). In fact, (1.2) turns out as a special case of the following principle (1.6), the parameters of which are specified in (5.3).

\[
\text{(1.6) Principle. Let } h \in \mathcal{K} = \{4, 6, 8, \ldots\}, \text{ } p \text{ a prime number, } \mathcal{C} \subset \mathcal{K} \text{ a residue class modulo } (p - 1)p', \text{ and } a_{n,k,h} := a_n(E_{k+h} - E_k \cdot E_h). \text{ There exists a finite subset } \mathcal{C}_0(h, p') \text{ of } \mathcal{C} \text{ and a constant } n_0(h, p') \text{ such that}
\]

\[
a_{n,k,h} \equiv 0 \pmod{p'} \text{ for } n \leq n_0 \text{ and } k \in \mathcal{C}_0(h, p')
\]

implies

\[
E_{k+h} \equiv E_k \cdot E_h \pmod{p'} \text{ for all } k \in \mathcal{C}, k \geq r + 1.
\]

Whether or not the “initial congruences” for \( n \leq n_0, k \in \mathcal{C}_0 \) are satisfied can in general be considered as random; the fact that they hold in the situation of (1.2) so as to conclude (1.2) from (1.6) is largely due to the trivial identities \( E_4^2 = E_8, \ E_6E_4 = E_{10}, \ E_8E_6 = E_{14} \), which come from \( \dim M_k = 1 \) for the spaces \( M_k \) of modular forms of weights \( k = 8, 10, 14 \). In case such “initial congruences” are satisfied, results like e.g.

\[
k \equiv 0 \pmod{6 \cdot 7} \Rightarrow E_{k+10} \equiv E_k \cdot E_{10} \pmod{7^4}
\]

(1.7)

come out. A sample of similar congruences is given in Section 5. Since the first coefficient of \( E_k \) is

\[
C_k := \frac{2k}{B_k}
\]

(1.6) also produces congruences for the \( C_k \), which apparently have escaped general attention so far, for example from (1.2),

\[
C_{k+12} \equiv C_k + C_{12} \pmod{N}.
\]

(1.8)
But note that congruences like (1.8) need not necessarily extend to the $E_k$
(i.e., to the higher Fourier coefficients; see (5.8)). This contradicts the general
expectation that “all congruences between Bernoulli numbers turn over to
Eisenstein series”.

All the present results are mere corollaries to Serre’s theory of Iwasawa
functions as presented in [6]. The author takes the opportunity to express his
gratitude to Prof. Serre for enlightening and very helpful correspondence
about these questions [7].

2. $p$-adic Eisenstein Series

Write $B_k/k = N_k/D_k$ with integers $N_k$ and $D_k$, $D_k > 0$, $(N_k, D_k) = 1$. Then $N_k$ is also the numerator of $B_k/2k$, and we read off from (1.1) that $E_k \in N_k^{-1}\mathbb{Z}[q]$ with precise denominator $N_k$. In particular, $E_k$ is $p$-integral if $(k, p)$ is regular, which will usually be assumed in what follows. We now fix a
prime $p$ and write

\[ B_k^* = (1 - p^{k-1})B_k, \]
\[ C_k^* = -\frac{2k}{B_k} = (1 - p^{k-1})^{-1}C_k, \]
\[ \tau^*_\ell(n) = \sum_{d\mid n, (d, p) = 1} d^\ell, \]
\[ E_k^* = 1 + C_k^* \sum_{n \geq 1} \tau^*_{k-1}(n)q^n. \] (2.1)

The $E_k^*$ are Serre’s normalized $p$-adic Eisenstein series; due to our regularity
assumption, they are $p$-integral and satisfy

\[ E_k \equiv E_k^* \pmod{p^{k-1}}. \] (2.2)

3. Iwasawa Functions ($p > 2$)

We collect the facts on Iwasawa functions needed in the sequel. Proofs
and more details can be found in [6, Sect. 4].

Suppose that $p > 2$, and let $U_1$ be the group of 1-units in $\mathbb{Z}_p^*$. Then $U_1$ is
topologically isomorphic with the additive group $(\mathbb{Z}_p, +)$. Choose a
generator $u = 1 + \pi$ with $v_p(\pi) = 1$ of $U_1$, for example $u = 1 + p$. An
Iwasawa function on $\mathbb{Z}_p$ is a function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ that may be written as

\[ f(s) = \sum_{n \geq 0} a_n(u^n - 1) \] (3.1)
with a formal power series $g(T) = \sum a_n T^n \in \mathbb{Z}_p[[T]]$. (Note that the function $f_v : s \mapsto v^s$ is well defined for any $v \in U_1$ in view of the binomial theorem.) Clearly, the definition is independent of the choice of the generator $u$, and $f \leftrightarrow g$ provides an isomorphism of the algebra $\Lambda$ of Iwasawa functions with $\mathbb{Z}_p[[T]]$. There are several other descriptions of $\Lambda$, e.g. as the uniform closure of the algebra generated by the $f_v$ in the algebra $\mathcal{C}^0(\mathbb{Z}_p, \mathbb{Z}_p)$ of continuous $\mathbb{Z}_p$-valued functions on $\mathbb{Z}_p$, or as an algebra of distributions on $\mathbb{Z}_p$ [6].

Next, recall that each function $f \in \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Z}_p)$ has a unique Mahler expansion

$$f(s) = \sum_{n \geq 0} \delta_n \binom{s}{n}$$

with coefficients $\delta_n \in \mathbb{Z}_p$, $\delta_n \to 0$, viz.,

$$\delta_n = \sum_i (-1)^i \binom{n}{i} f(n - i).$$

It is a crucial fact [6, Théorème 15] that for $g \in \Lambda$, actually $\delta_n \equiv 0 \pmod{p^n}$ holds. Criterion (1.4) results, i.e.,

$$g(\mathbb{Z}_p) \subset p^n \mathbb{Z}_p \iff g(i) \equiv 0 \pmod{p^n}, \quad i = 0, 1, \ldots, r - 1 \quad (3.3)$$

for Iwasawa functions $g$.

Let now $X = a + p^i \mathbb{Z}_p \subset \mathbb{Z}_p$ be a residue class, and choose an affine isomorphism $\alpha : X \cong \mathbb{Z}_p$. A function $f : X \to \mathbb{Z}_p$ is called Iwasawa on $X$ if $f \circ \alpha^{-1}$ is an Iwasawa function on $\mathbb{Z}_p$. This definition is meaningful and independent of the choice of $\alpha$, as results from

(3.4) **Proposition.** Let $f$ be an Iwasawa function on $\mathbb{Z}_p$.

(i) For any $a, b \in \mathbb{Z}_p$, $s \mapsto f(as + b)$ is an Iwasawa function on $\mathbb{Z}_p$.

(ii) $f$ restricted to $X$ is an Iwasawa function on $X$.

**Proof.** Rearrangement of power series. We omit the details. □

We still need a further extension of the definition. Consider an arithmetic progression

$$\mathcal{C} = \{k, k + (p - 1)p^i, k + 2(p - 1)p^i, \ldots\} \subset \mathcal{X} = \{4, 6, 8, \ldots\} \quad (3.5)$$

modulo $(p - 1)p^i$. A function $f : \mathcal{C} \to \mathbb{Z}_p$ is said to be Iwasawa if it is the restriction to $\mathcal{C}$ of an Iwasawa function (in the above sense) $f : X \to \mathbb{Z}_p$ on
its topological closure $X = k + p^i \mathbb{Z}_p$ in $\mathbb{Z}_p$. For such functions, we can apply the next result, which is an easy consequence of (3.3) and (3.4).

(3.6) Proposition. Let $f$ be an Iwasawa function on $\mathcal{C}$. Then $f \equiv 0 \pmod{p^r}$ if and only if there are $r$ consecutive elements $k_1, k_2 = k_1 + (p - 1)p^i, \ldots, k_r = k_1 + (r - 1)(p - 1)p^i$ of $\mathcal{C}$ such that $f(k_1) \equiv f(k_2) \equiv \cdots \equiv f(k_r) \equiv 0 \pmod{p^r}$.

Finally, the relation with the Eisenstein series $E_k^*$ is as follows:

(3.7) Theorem (Iwasawa, Serre). Let $(k, p)$ be regular and $\mathcal{C} \subset \mathcal{K}$ the class $(\mod p - 1)$ determined by $k$. For each $n \geq 0$, the function $k \mapsto a_n(E_k^*)$ is an Iwasawa function on $\mathcal{C}$.

Remark. The corresponding property is stated in [6, p. 245] for the function $G_k^* = E_k^*/C_k^*$. Thanks to our regularity assumption, $C_k^*$ is a $p$-adic integer for each $k \in \mathcal{C}$, equal to $2\zeta_p^{-1}(1 - k)$, where $\zeta_p$ is a branch of the $p$-adic zeta function. Therefore, $k \mapsto C_k^*$ is an Iwasawa function by Iwasawa’s original results [3, 4], and (3.7) follows from the statement as given in [6].

4. IWASAWA FUNCTIONS ($p = 2$)

Here we have to modify some definitions and statements about Iwasawa functions. We briefly state the necessary changes, see [6] for details. Let $U_2 = 1 + 4\mathbb{Z}_2$ be the subgroup of 2-units in $\mathbb{Z}_2^*$, which is isomorphic with $(\mathbb{Z}_2, +)$. Choosing a topological generator $u$ of $U_2$, an Iwasawa function $f : \mathbb{Z}_2 \to \mathbb{Z}_2$ is a function of the form

$$f(s) = g(u^s - 1) \quad (4.1)$$

with some $g \in \mathbb{Z}_2[[T]]$. Again, $f \leftrightarrow g$ identifies the algebra $\Lambda$ of Iwasawa functions with $\mathbb{Z}_2[[T]]$. For $g \in \Lambda$, the Mahler coefficients $\delta_n$ satisfy even

$$\delta_n \equiv 0 \pmod{4^n}, \quad (4.2)$$

which gives rise to the equivalence

$$g(\mathbb{Z}_2) \subset 2^i \mathbb{Z}_2 \iff g(i) \equiv 0 \pmod{2^i}, \quad i = 0, 1, \ldots \left\lfloor \frac{r - 1}{2} \right\rfloor. \quad (4.3)$$
Proposition 3.4 and the definition of Iwasawa functions on classes $X \pmod{p'}$ in $\mathbb{Z}_p$ and on progressions

\[ \mathscr{C} = \{ k, k + 2^t, k + 2 \cdot 2^t, \ldots \} \subset \mathcal{H} \]  

(4.5)

remain unchanged for $p = 2$. The substitute for (3.6) is

(4.6) Proposition. Let $f$ be an Iwasawa function on $\mathscr{C}$. Then $f \equiv 0 \pmod{2^r}$ if and only if there are $r' := \lceil \frac{r}{2} \rceil$ consecutive elements $k_1, k_1 + 2^t, \ldots, k_{r'} = k_1 + \lceil \frac{r}{2} \rceil 2^t$ of $\mathscr{C}$ such that $f(k_1) \equiv \cdots \equiv f(k_{r'}) \equiv 0 \pmod{2^r}$.

As to the analogue of (3.7), we can suppress the regularity condition. Thus:

(4.7) Theorem. For each $n \geq 0$, the function $k \mapsto a_n(E_k^*)$ is an Iwasawa function on $\mathcal{H} = \{4, 6, 8, \ldots\} \subset \mathbb{Z}_2$.

5. PRECISE STATEMENT AND PROOF OF PRINCIPLE (1.6)

Let $p > 2$ be a prime, $h \in \mathcal{H}$, and $\mathscr{C} \subset \mathcal{H}$ a class modulo $(p - 1)p'$ for some $t \geq 0$. Suppose that $(h, p)$, $(k, p)$, and $(k + h, p)$ are regular. If we wish to prove that

\[ E_{k+h} \equiv E_k \cdot E_h \pmod{p'} \]  

(5.1)

for some $r \geq 1$ and all $k \in \mathscr{C}$, $k \geq r + 1$, we may replace $E_k$ by $E_k^*$ and $E_{k+h}$ by $E_{k+h}^*$, which does not affect (5.1). For fixed $n$, the function $a_n : k \mapsto a_n(E_{k+h}^* - E_k^* \cdot E_h)$ on $\mathscr{C}$ is Iwasawa. Let $k_1, k_2, \ldots, k_r$ be the first $r$ consecutive elements of $\mathscr{C}$ with $k_1 \geq r + 1$, and put

\[ k_0 = k_r + h = \text{weight of } E_{k_r+h} - E_{k_r} \cdot E_h, \]

\[ n_0 = n_0(\mathscr{C}, h, p') = \lfloor k_0/12 \rfloor. \]  

(5.2)

Suppose that

\[ a_n(E_{k+h}^* - E_k^* \cdot E_h) \equiv 0 \pmod{p'} \]  

(5.3)

holds for $k = k_1, \ldots, k_r$ and $n \leq n_0$. Then for these $k, E_{k+h} - E_k \cdot E_h \equiv E_{k+h}^* - E_k^* \cdot E_h \equiv 0 \pmod{p'}$ from the $q$-expansion principle (1.5), i.e., we have the congruences for all the coefficients $a_n$. Referring to (3.6), the Iwasawa function $a_n$ satisfies $a_n \equiv 0 \pmod{p'}$, which in turn gives (5.3) for all $n > 0$ and all $k \in \mathscr{C}$, $k \geq r + 1$, that is (5.1). The same argument, but (3.6)
replaced by its counterpart (4.6), yields a similar result for \( p = 2 \). Together, we have proved the following precise version of principle (1.6).

(5.4) **Theorem.** \((p > 2)\) Let \( p > 2 \) be a prime, \( h \in \mathcal{H} = \{4, 6, 8, \ldots\} \), \( \mathcal{C} \subset \mathcal{H} \) a class modulo \((p-1)p'\), and suppose that \((h,p),(k,p)\), and \((k + h, p)\) are regular for all \( k \in \mathcal{C} \), \( i.e. \), \( p \) divides neither of the numerators of \( B_h, B_k, B_{k+h} \). For given \( r \geq 1 \) and \( 1 \leq j \leq r \), let

\[
k_j = \min\{k \in \mathcal{C} \mid k \geq r + 1\} + (j - 1)(p - 1)p'.
\]

Put further \( k_0 = k_r + h \) and \( n_0 = \lfloor k_0/12 \rfloor \). Then the congruences

\[
a_n(E_{k+h}) \equiv a_n(E_k \cdot E_h) \pmod{p'}
\]

for \( k = k_1, k_2, \ldots, k_r \) and \( n \leq n_0 \) imply

\[
E_{k+h} \equiv E_k \cdot E_h \pmod{p'}
\]

for all \( k \in \mathcal{C} \) with \( k \geq r + 1 \).

\((p = 2)\) Let \( h \in \mathcal{H} \) and \( \mathcal{C} \subset \mathcal{H} \) be a class mod \( 2^r \). For given \( r \geq 1 \) and \( 1 \leq j \leq r' := \lfloor r/2 \rfloor \), let

\[
k_j = \min\{k \in \mathcal{C} \mid k \geq r + 1\} + (j - 1)2'.
\]

Put further \( k_0 = k_r + h \) and \( n_0 = \lfloor k_0/12 \rfloor \). Then the congruences

\[
a_n(E_{k+h}) \equiv a_n(E_k \cdot E_n) \pmod{2^r}
\]

for \( k = k_1, k_2, \ldots, k_r \) and \( n \leq n_0 \) imply

\[
E_{k+h} \equiv E_k \cdot E_h \pmod{2^r}
\]

for all \( k \in \mathcal{C} \) with \( k \geq r + 1 \).

(5.5) **Remark.** (i) If the requirements of (5.4) are fulfilled, then \( E_{k+h}^* \equiv E_k^* \cdot E_h^* \) for all \( k \in \mathcal{C} \), but we cannot, in general, replace the \( E_k^* \) by \( E_k \).

(ii) As the proof shows, even the weaker requirement

\[
a_n(E_{k+h}) \equiv a_n(E_k \cdot E_h) \pmod{p'}
\]

for \( k = k_1, \ldots, k_r \) and \( n \leq \lfloor k+h/12 \rfloor \) suffices to derive the conclusion in (5.4) \((p > 2)\), and similarly for (5.4) \((p = 2)\).

(5.6) **Corollary.** \((p > 2)\) Let the assumptions be as in (5.4) \((p > 2)\).
The congruences
\[ C_{k+h} \equiv C_k + C_h \pmod{p^r} \]
for \( k = k_1, \ldots, k_r \) imply the same congruences for all \( k \in \mathcal{C}, \ k \geq r + 1. \)

\((p = 2)\) In the situation of (5.4) \((p = 2)\), the congruences
\[ C_{k+h} \equiv C_k + C_h \pmod{2^r} \]
for \( k = k_1, \ldots, k_r \) imply the same congruences for all \( k \in \mathcal{C}, \ k \geq r + 1. \)

Proof. Recall that \( C_k = \frac{2k}{B_k} \), and \( C_k^* \) is the linear term of \( E_k^* \). The map \( k \mapsto C_k^* \) is an Iwasawa function on \( \mathcal{C} \). Hence the result follows from (3.6) and (4.6), respectively.

(Strictly speaking, (5.6) is not a corollary to (5.4), but it is suitable to place it here.)

Using a tiny bit of numerical calculation, we now show that (5.4) and (5.6) apply to many situations “in nature” and produce explicit unconditional congruences, among which are those of (1.2).

(5.7) Let \( A(h, a \mod q, p^r) \) (resp. \( B(h, a \mod q, p^r) \)) denote the assertion
\[ E_{k+h} \equiv E_k \cdot E_h \pmod{p^r} \quad \text{(resp.} \quad C_{k+h} \equiv C_k + C_h \pmod{p^r}) \]
whenever \( k \equiv a \mod q \). Here \( h \) and \( k \) are elements of \( \mathcal{K} \). We also write \( A(h, all, p^r) \) (resp. \( B(h, all, p^r) \)) if the congruence holds for all \( k \in \mathcal{K} \). Clearly \( A(\ldots) \) implies \( B(\ldots) \).

(5.8) Corollary. Table I contains some congruences \( A(h, a \mod q, p^r) \) that hold.

Furthermore, some supplementary congruences \( B(h, a \mod q, p^r) \) are given in Table II.

(5.9) Remarks and comments. (i) We listed only such congruences which are not implied by the Kummer and Clausen-von Staudt congruences (1.3). All of them are sharp in a stable sense, i.e., cannot be sharpened by omitting a finite number of \( k \)'s.

(ii) Theorem (5.4) gives congruences only for such weights \( k \) with \( k \geq r + 1 \). It turned out that in each of the cases listed, that restriction was redundant. We therefore omitted that condition also in the definition of the assertions \( A(\ldots) \) and \( B(\ldots) \) in (5.7).

(iii) The assertion \( A(h_1 + h_2, all, p^r) \) is a formal consequence of \( A(h_1, all, p^r) \) and \( A(h_2, all, p^r) \), etc. We listed for \( h = 8, 10, 12 \) only such congruences which we did not recognize as implied from congruences for
\[ h_1 \text{ and } h_2, \quad h = h_1 + h_2, \quad \text{for example, we have } A(10, a \mod 6, 7^2) \text{ for } a = 0 \text{ and } 4, \text{ which however is a consequence of } A(4, a \mod 6, 7^2) \text{ and } A(6, \text{ all}, 7^2). \]

In particular, the congruences stated in (1.2) follow from \( A(4, \text{ all}, 2^7), \quad A(6, \text{ all}, 3^4), \quad A(4, \text{ all}, 5^3), \) and \( A(6, \text{ all}, 7^2). \)

(iv) In all cases analyzed, we found the following behavior (which can be read off from the table in the cases \( h = 4, 6 \) and \( p = 2, 3 \)): If a congruence

\[ h, a \mod q, \quad p^r, \quad a \mod q, \quad p^r \]

\begin{table}[h]
\centering
\begin{tabular}{ccc}
\hline
\textit{h} & \textit{a mod q} & \textit{p}^r \\
\hline
4 & All & \begin{tabular}{c}
27 \\
28 \\
29 \\
210 \\
211 \\
212 \\
213 \\
214 \\
34 \\
35 \\
\end{tabular} \begin{tabular}{c}
6, 10 mod 2 \cdot 3^3 \\
6, 10 mod 2 \cdot 3^4 \\
\text{all} \\
0, 4, 6, 10 mod 4 \cdot 5 \\
6, 10 mod 4 \cdot 5^2 \\
0, 4 mod 6 \\
0, 4, 6, 10 mod 6 \cdot 7 \\
0 mod 10 \\
6 mod 12 \\
6 mod 12 \cdot 13 \\
\end{tabular} \begin{tabular}{c}
3^6 \\
3^7 \\
5^2 \\
5^4 \\
5^5 \\
7^2 \\
7^3 \\
11^2 \\
13^2 \\
13^3 \\
\end{tabular} \\
6 & All & \begin{tabular}{c}
26 \\
27 \\
28 \\
29 \\
210 \\
211 \\
212 \\
213 \\
34 \\
35 \\
\end{tabular} \begin{tabular}{c}
0, 8 mod 2 \cdot 3^2 \\
0, 8 mod 2 \cdot 3^3 \\
8, 108 mod 2 \cdot 3^4 \\
0 mod 4 \\
0, 8 mod 4 \cdot 5 \\
8, 20 mod 4 \cdot 5^2 \\
\text{all} \\
0, 4, 8 mod 6 \cdot 7 \\
4 mod 10 \\
4 mod 10 \cdot 11 \\
\end{tabular} \begin{tabular}{c}
3^6 \\
3^7 \\
3^8 \\
5^2 \\
5^3 \\
5^6 \\
7^2 \\
7^3 \\
11^2 \\
11^3 \\
\end{tabular} \\
8 & 0 mod 2 \cdot 3 & \begin{tabular}{c}
35 \\
\end{tabular} \begin{tabular}{c}
0 mod 6 \\
\end{tabular} \begin{tabular}{c}
7^3 \\
\end{tabular} \\
10 & 0 mod 6 \cdot 7 & 7^4 \\
12 & 0, 2 mod 12 & 13^2 \\
\end{tabular}
\end{table}

\begin{table}[h]
\centering
\begin{tabular}{ccc}
\hline
\textit{h} & \textit{a mod q} & \textit{p}^r \\
\hline
4 & 10 mod 28 & \begin{tabular}{c}
29^2 \\
\end{tabular} \begin{tabular}{c}
0 mod 52 \\
\end{tabular} \begin{tabular}{c}
53^2 \\
\end{tabular} \\
6 & 8 mod 16 & \begin{tabular}{c}
17^2 \\
\end{tabular} \begin{tabular}{c}
0 mod 30 \\
\end{tabular} \begin{tabular}{c}
31^2 \\
\end{tabular} \\
12 & 0 mod 12 & \begin{tabular}{c}
13^3 \\
\end{tabular} \begin{tabular}{c}
0 mod 28 \\
\end{tabular} \begin{tabular}{c}
29^2 \\
\end{tabular} \\
\end{tabular}
\end{table}
A(h, a \mod q, p') with \( r \geq 2 \) holds, there exist one or several classes \( a' \mod q \cdot p \) such that \( A(h, a' \mod q \cdot p, p'^{+1}) \) also is satisfied. This indicates that the functions \( k \mapsto a_n(E^*_k + h - E^*_k \cdot E_h) \) should have a common zero \( \hat{k} \in \mathbb{Z}_p \), \( \hat{k} \equiv a \pmod{q} \equiv a' \pmod{q \cdot p} \equiv \ldots \), and presumably each “super-Kummer congruence” as listed in (5.8) comes from such a zero.

(v) We point out that the “natural” extensions of the congruences \( B(h, a \mod q, p') \) (see end of (5.8)) to \( E_k \) fail to hold, even after omitting small values of \( k \).

The proof of (5.8) is straightforward from checking the conditions of (5.4) or (5.6), respectively. In order to convince the reader that at least (1.2) can be achieved with a pocket calculator or even by hand, we present the details in two significant cases. Let us first give a list of the relevant \( C_k \) in factorized form.

(5.10) Table. \( C_4 = 2^4 \cdot 3 \cdot 5 \), \( C_6 = -2^3 \cdot 3^2 \cdot 7 \), \( C_8 = 2^5 \cdot 3 \cdot 5 \), \( C_{10} = -2^3 \cdot 3 \cdot 11 \), \( C_{12} = 2^4 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13/691 \), \( C_{14} = -2^3 \cdot 3 \), \( C_{16} = 2^6 \cdot 3 \cdot 5 \cdot 17/3617 \), \( C_{18} = -2^3 \cdot 3^3 \cdot 7 \cdot 19/43867 \), \( C_{20} = 2^4 \cdot 3 \cdot 5^2 \cdot 11/283 \cdot 617 \).

Proof of \( A(4, \text{all, } 2^7) \). With the notation of (5.4) \( (p = 2) \) we have \( r' = 4 \), \( k_1, k_2, k_3, k_4 = 8, 10, 12, 14 \), \( k_0 = 18, n_0 = 1 \). Thus we must check only the linear terms, i.e., \( C_{k+4} \equiv C_k + C_4 \pmod{2^7} \) for the \( k_j, 1 \leq j \leq 4 \), which can be done with the table above. So we have the statement for all \( k \geq 8 \). However we know a priori that \( E_8 = E_4 \cdot E_4 \) and \( E_{10} = E_6 \cdot E_4 \).  

Proof of \( A(6, \text{all, } 7^2) \). We have to consider the three classes of 4, 6, and 8 (mod 6) in \( \mathcal{X}' \). In each case, the number \( n_0 \) of (5.4) equals 1, so we are reduced to showing that \( C_{k+6} \equiv C_k + C_6 \pmod{7^2} \) for \( k = 4, 10, 6, 12 \), and 8, 14.  

We found and verified the congruences stated in (5.8) using a list of Bernoulli numbers \( B_k \) with \( k \leq 3000 \). Accepting massive use of computing power, it is certainly possible to extend the results to congruences involving larger primes \( p \), larger exponents \( r \), and larger increments \( h \). In that case it was preferable to replace the costly rational arithmetic of large Bernoulli numbers by \( p \)-adic arithmetic. The actual calculations were performed on MAPLE by Bodo Wack, whose help is gratefully acknowledged.

REFERENCES