Universität des Saarlandes

Fachrichtung 6.1 – Mathematik

Preprint

A series of new congruences for Bernoulli numbers and Eisenstein series

Ernst-Ulrich Gekeler

Preprint No. 53

Saarbrücken 2002

Universität des Saarlandes

Fachrichtung 6.1 – Mathematik

A series of new congruences for Bernoulli numbers and Eisenstein series

Ernst-Ulrich Gekeler

Saarland University
Department of Mathematics
Postfach 15 11 50
D–66041 Saarbrücken
Germany
E-Mail: gekeler@math.uni-sb.de

submitted: February 19, 2002

Preprint No. 53

Saarbrücken 2002

Edited by
FR 6.1 – Mathematik
Im Stadtwald
D–66041 Saarbrücken
Germany

Fax:	+ 49 681 302 4443
e-mail:	preprint@math.uni-sb.de
WWW:	http://www.math.uni-sb.de/

A series of new congruences for Bernoulli numbers and Eisenstein series

Ernst-Ulrich Gekeler

MSC 2000: 11 F 33, 11 B 68

Abstract

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.

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 $\mathrm{SL}(2, \mathbb{Z})$, given through its q-expansion

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

Here $B_k = 1, -1/2, 1/6, 0, -1/30, \ldots$ are the Bernoulli numbers defined by

$$\frac{X}{e^X - 1} = \sum_{k \geq 0} \frac{B_k}{k!} X^k, \text{ and } \sigma_\ell(n) = \sum_{d|n} d^\ell.$$

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, $f \equiv g \pmod N$ means that f and g are both N-integral and the congruence holds coefficientwise. A weakened version of one of our results is

1.2 Theorem. *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*

$$E_{k+12} = E_k \cdot E_{12} \pmod N.$$

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] p. 55, p. 241) that

$$(1.3) \qquad \begin{array}{llll} E_k \equiv & 1 \pmod{p^r} & \text{if } k \equiv 0 \pmod{(p-1)p^{r-1}} & \text{and} \\ E_k \equiv & E_\ell \pmod{p^r} & \text{if } k \equiv \ell \pmod{(p-1)p^r}, & \end{array}$$

$k, \ell \geq r+1$, and $(k,p), (\ell,p)$ are regular. The last condition signifies that p doesn't 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 ℓ.

The congruence (mod 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 doesn't essentially affect the validity of (1.2).

(b) The congruence

$$(1.2^*) \qquad E_{k+12}^* \equiv E_k^* \cdot E_{12} \pmod{p^r}$$

is doubly infinite (in k and n = 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

$$a_n : k \longmapsto a_n(E_{k+12}^* - E_k^* E_{12}).$$

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 $f : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p$ (see sect. 3, 4). Now it is a basic property of Iwasawa functions g that:

$$(1.4) \qquad g(\mathbb{Z}_p) \subset p^r\mathbb{Z}_p \Leftrightarrow g(i) \equiv 0 \pmod{p^r},\ i = 0, 1, \ldots, r-1.$$

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 $\mathcal{K}_0 = \mathcal{K}_0(p^r) \subset \mathcal{K} := \{4, 6, 8, \ldots\}$ of weights k depending only on p^r but not on n.

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

(1.5) *Let* $f = \sum_{n\geq 0} a_n q^n$ *be a modular form of weight* k_0 *with coefficients in* $\mathbb{Z}_{(p)} = \mathbb{Q} \cap \mathbb{Z}_p$. *If* $a_n \equiv 0 \pmod{p^r}$ *for* $n \leq k_0/12$ *then* $f \equiv 0 \pmod{p^r}$, *i.e., all its coefficients* a_n *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 $k_0 := \max\ \mathcal{K}_0(p^r) + 12$, 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).

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

$$a_{n,k,h} \equiv 0 \pmod{p^r} \text{ for } n \leq n_0 \text{ and } k \in \mathcal{C}_0(h, p^r)$$

implies

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

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 $E_4^2 = E_8$, $E_6 E_4 = E_{10}$, $E_8 E_6 = E_{14}$, 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.

$$(1.7) \qquad k \equiv 0 \pmod{6 \cdot 7} \Rightarrow E_{k+10} \equiv E_k \cdot E_{10} \pmod{7^4}$$

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. E.g. from (1.2),

$$(1.8) \qquad C_{k+12} \equiv C_k + C_{12} \pmod{N}.$$

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

$$\begin{aligned} B_k^* &= (1-p^{k-1})B_k \\ C_k^* &= -\tfrac{2k}{B_k^*} = (1-p^{k-1})^{-1}C_k \\ \sigma_\ell^*(n) &= \sum_{d|n,(d,p)=1} d^\ell \\ E_k^* &= 1 + C_k^* \sum_{n\geq 1} \sigma_{k-1}^*(n) q^n. \end{aligned} \tag{2.1}$$

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

$$E_k \equiv E_k^* \pmod{p^{k-1}}. \tag{2.2}$$

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], section 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 $f : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p$ that may be written

$$f(s) = \sum_{n\geq 0} a_n(u^s - 1) \tag{3.1}$$

with a formal power series $g(T) = \sum a_n T^n \in \mathbb{Z}_p[[T]]$. (Note that the function $f_v : s \longmapsto v^s$ 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 Λ

of Iwasawa functions with $\mathbb{Z}_p[[T]]$. There are several other descriptions of Λ, e.g. as the uniform closure of the algebra generated by the f_v in the algebra $C^0(\mathbb{Z}_p, \mathbb{Z}_p)$ of continuous $\mathbb{Z}_p$-valued functions on $\mathbb{Z}_p$, or as an algebra of distributions on $\mathbb{Z}_p$ (*loc. cit.*).

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

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

with coefficients $\delta_n \in \mathbb{Z}_p$, $\delta_n \longrightarrow 0$, 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. Thus criterion (1.4) results, i.e.,

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

for Iwasawa functions g.

Let now $X = a + p^t\mathbb{Z}_p \subset \mathbb{Z}_p$ be a residue class, and choose an affine isomorphism $\alpha : X \xrightarrow{\cong} \mathbb{Z}_p$. A function $f : X \longrightarrow \mathbb{Z}_p$ 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 α, as results from

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

(i) *For any $a, b \in \mathbb{Z}_p$, $s \longmapsto f(as + b)$ 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. $\square$

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

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

modulo $(p-1)p^t$. A function $f : \mathcal{C} \longrightarrow \mathbb{Z}_p$ is said to be Iwasawa if it is the restriction to $\mathcal{C}$ of an Iwasawa function (in the above sense) $f : X \longrightarrow \mathbb{Z}_p$ on its topological closure $X = k + p^t\mathbb{Z}_p$ 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 $k_1, k_2 = k_1 + (p-1)p^t, \ldots, k_r = k_1 + (r-1)(p-1)p^t$ of $\mathcal{C}$ such that $f(k_1) \equiv$*

$f(k_2) \equiv \cdots f(k_r) \equiv 0 \pmod{p^r}$.

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 $k \longmapsto a_n(E_k^*)$ 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 ζ_p is a branch of the p-adic zeta function. Therefore, $k \longmapsto C_k^*$ 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 $f: \mathbb{Z}_2 \longrightarrow \mathbb{Z}_2$ is a function of the form

$$f(s) = g(u^s - 1) \tag{4.1}$$

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

$$\delta_n \equiv 0 \pmod{4^n}, \tag{4.2}$$

which gives rise to the equivalence

$$g(\mathbb{Z}_2) \subset 2^r\mathbb{Z}_2 \Leftrightarrow g(i) \equiv 0 \pmod{2^r},\ i = 0, 1, \ldots \left[\frac{r-1}{2}\right]. \tag{4.3}$$

Proposition 3.4 and the definition of Iwasawa functions on classes X (mod p^t) in $\mathbb{Z}_p$ and on progressions

$$\mathcal{C} = \{k, k+2^t, k+2\cdot 2^t, \ldots\} \subset \mathcal{K} \tag{4.5}$$

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

4.6 Proposition. *Let f be an Iwasawa function on $\mathcal{C}$. Then $f \equiv 0 \pmod{2^r}$ if and only if there are $r' := \left[\frac{r+1}{2}\right]$ consecutive elements $k_1, k_1 + 2^t, \ldots, k_{r'} = k_1 + \left[\frac{r-1}{2}\right] 2^t$ of $\mathcal{C}$ 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 $k \longmapsto a_n(E_k^*)$ is an Iwasawa function on $\mathcal{K} = \{4, 6, 8, \ldots\} \subset \mathbb{Z}_2$.*

5. Precise statement and proof of Principle 1.6.

Let $p > 2$ be a prime, $h \in \mathcal{K}$, and $\mathcal{C} \subset \mathcal{K}$ a class modulo $(p-1)p^t$ for some $t \geq 0$. Suppose that (h,p), (k,p), and $(k+h,p)$ are regular. If we wish to prove that

$$E_{k+h} \equiv E_k \cdot E_h \pmod{p^r} \tag{5.1}$$

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

$$\begin{array}{rcl} k_0 & = & k_r + h = \text{weight of } E_{k_r+h} - E_{k_r} \cdot E_h, \\ n_0 & = & n_0(\mathcal{C}, h, p^r) = [k_0/12]. \end{array} \tag{5.2}$$

Suppose that

$$a_n(E_{k+h} - E_k \cdot E_h) \equiv 0 \pmod{p^r} \tag{5.3}$$

holds for $k = k_1, \ldots, k_r$ and $n \leq n_0$. Then for these k, $E_{k+h} - E_k \cdot E_h \equiv E_{k+h}^* - E_k^* \cdot E_h \equiv 0 \pmod{p^r}$ 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 $a_n \equiv 0 \pmod{p^r}$, which in turn gives (5.3) for *all* $n \geq 0$ and *all* $k \in \mathcal{C}$, $k \geq r+1$, 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, $h \in \mathcal{K} = \{4, 6, 8, \ldots\}$, $\mathcal{C} \subset \mathcal{K}$ a class modulo $(p-1)p^t$, 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*

$$k_j = \min\{k \in \mathcal{C} \mid k \geq r+1\} + (j-1)(p-1)p^t.$$

Put further $k_0 = k_r + h$ and $n_0 = [k_0/12]$. Then the congruences

$$a_n(E_{k+h}) \equiv a_n(E_k \cdot E_h) \pmod{p^r}$$

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

$$E_{k+h} \equiv E_k \cdot E_h \pmod{p^r}$$

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

$(p=2)$ *Let* $h \in \mathcal{K}$ *and* $\mathcal{C} \subset \mathcal{K}$ *be a class mod* 2^t. *For given* $r \geq 1$ *and* $1 \leq j \leq r' := \left[\frac{r+1}{2}\right]$, *let*

$$k_j = \min\{k \in \mathcal{C} \mid k \geq r+1\} + (j-1)2^t.$$

Put further $k_0 = k_{r'} + h$ *and* $n_0 = [k_0/12]$. *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 Remarks. (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

$$a_n(E_{k+h}) \equiv a_n(E_k \cdot E_h) \pmod{p^r}$$

for $k = k_1, \ldots, k_r$ and $n \leq \left[\frac{k+h}{12}\right]$ 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 $k \longmapsto C^*_k$ is an Iwasawa function on $\mathcal{C}$. Hence the result follows from (3.6) and (4.6), respectively. $\square$

(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 those of (1.2).

(5.7) Let $A(h, a \bmod q, p^r)$ (resp. $B(h, a \bmod q, p^r)$) denote the assertion

$$E_{k+h} \equiv E_k \cdot E_h \pmod{p^r} \quad (\text{resp. } C_{k+h} \equiv C_k + C_h \pmod{p^r})$$

whenever $k \equiv a \bmod q$. Here h and k are elements of $\mathcal{K}$. We also write $A(h, \text{all}, p^r)$ (resp. $B(h, \text{all}, p^r)$) if the congruence holds for all $k \in \mathcal{K}$. Clearly $A(\ldots)$ implies $B(\ldots)$.

5.8 Corollary. *The following congruences $A(h, a \bmod q, p^r)$ hold:*

h	$a \bmod q$	p^r	$a \bmod q$	p^r
4	all	2^7	6,10 mod $2 \cdot 3^3$	3^6
	2 mod 2^2	2^8	6,10 mod $2 \cdot 3^4$	3^7
	2 mod 2^3	2^9	all	5^3
	10 mod 2^4	2^{10}	0,4,6,10 mod $4 \cdot 5$	5^4
	10 mod 2^5	2^{11}	6,10 mod $4 \cdot 5^2$	5^5
	10 mod 2^6	2^{12}	0,4 mod 6	7^2
	74 mod 2^7	2^{13}	0,4,6,10 mod $6 \cdot 7$	7^3
	202 mod 2^8	2^{14}	0 mod 10	11^2
	all	3^3	0,10 mod $10 \cdot 11$	11^3
	0,4 mod $2 \cdot 3$	3^4	6 mod 12	13^2
	6,10 mod $2 \cdot 3^2$	3^5	6 mod $12 \cdot 13$	13^3
6	all	2^6	0,8 mod $2 \cdot 3^2$	3^6
	0 mod 2^2	2^7	0,8 mod $2 \cdot 3^3$	3^7
	0 mod 2^3	2^8	8,108 mod $2 \cdot 3^4$	3^8
	8 mod 2^4	2^9	0 mod 4	5^4
	8 mod 2^5	2^{10}	0,8 mod $4 \cdot 5$	5^5
	8 mod 2^6	2^{11}	8,20 mod $4 \cdot 5^2$	5^6
	8 mod 2^7	2^{12}	all	7^2
	136 mod 2^8	2^{13}	0,4,8 mod $6 \cdot 7$	7^3
	all	3^4	4 mod 10	11^2
	0,2 mod $2 \cdot 3$	3^5	4 mod $10 \cdot 11$	11^3
8	0 mod $2 \cdot 3$	3^5	0 mod 6	7^3
10	0 mod $6 \cdot 7$	7^4		
12	0,2 mod 12	13^2		

Furthermore, we have the supplementary congruences $B(h, a \bmod q, p^r)$*:*

h	$a \bmod q$	p^r	$a \bmod q$	p^r
4	$10 \bmod 28$	29^2	$0 \bmod 52$	53^2
6	$8 \bmod 16$	17^2	$0 \bmod 30$	31^2
12	$0 \bmod 12$	13^3	$0 \bmod 28$	29^2
	$0 \bmod 12 \cdot 13$	13^5		

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 $A(\dots)$ and $B(\dots)$ in (5.7).
(iii) The assertion $A(h_1 + h_2, \mathrm{all}, p^r)$ is a formal consequence of $A(h_1, \mathrm{all}, p^r)$ and $A(h_2, \mathrm{all}, p^r)$, etc. We listed for $h = 8, 10, 12$ only such congruences which we didn't recognize as implied from congruences for h_1 and h_2, $h = h_1 + h_2$. E.g., we have $A(10, a \bmod 6, 7^2)$ for $a = 0$ and 4, which however is a consequence of $A(4, a \bmod 6, 7^2)$ and $A(6, \mathrm{all}, 7^2)$. In particular, the congruences stated in (1.2) follow from $A(4, \mathrm{all}, 2^7)$, $A(6, \mathrm{all}, 3^4)$, $A(4, \mathrm{all}, 5^3)$, and $A(6, \mathrm{all}, 7^2)$.
(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 $A(h, a \bmod q, p^r)$ with $r \geq 2$ holds, there exist one or several classes $a' \bmod q \cdot p$ such that also $A(h, a' \bmod q \cdot p, p^{r+1})$ is satisfied. This indicates that the functions $k \longmapsto a_n(E^*_{k+h} - E^*_k \cdot E_h)$ should have a common zero $\hat{k}$ in $\mathbb{Z}_p$, $\hat{k} \equiv a \pmod{q} \equiv a' \pmod{q \cdot p} \equiv \dots$, 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 $B(h, a \bmod q, p^r)$ (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. $C_4 = 2^4{\cdot}3{\cdot}5$, $C_6 = -2^3{\cdot}3^2{\cdot}7$, $C_8 = 2^5{\cdot}3{\cdot}5$, $C_{10} = -2^3{\cdot}3{\cdot}11$, $C_{12} = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13/691$, $C_{14} = -2^3 \cdot 3$, $C_{16} = 2^6 \cdot 3 \cdot 5 \cdot 17/3617$, $C_{18} = -2^3 \cdot 3^3 \cdot 7 \cdot 19/43867$, $C_{20} = 2^4 \cdot 3 \cdot 5^2 \cdot 11/283 \cdot 617$.

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 $\mathcal{K}$. 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

[1] E.-U. Gekeler, Some observations on the arithmetic of Eisenstein series for the modular group $\mathrm{SL}(2, \mathbb{Z})$. Arch. Math. **77**, 5–21 (2001).

[2] H. Hida, Elementary theory of L-functions and Eisenstein series. Cambridge University Press 1993.

[3] K. Iwasawa, On p-adic L-functions. Ann. Math. **89**, 198–205 (1969).

[4] K. Iwasawa, Lectures on p-adic L-functions. Ann. Math. Studies, Princeton University Press 1972.

[5] B. Schöneberg, Elliptic modular functions. Springer-Verlag 1974.

[6] J-P. Serre, Formes modulaires et fonctions zêta p-adiques. In: Lecture Notes in Mathematics **350**, Springer-Verlag 1973.

[7] J-P. Serre, e-mail messages to the author, November 2000.

[8] J. Sturm, The congruence of modular forms. In: New York Number Theory Seminar 1984–85. Lecture Notes in Mathematics **1240**, Springer-Verlag 1987.

[9] L. Washington, Introduction to cyclotomic fields. Springer-Verlag 1982.