On a conjecture about numerators of the Bernoulli numbers

Bernd C. Kellner

Abstract

In this paper we disprove a conjecture about numerators of divided Bernoulli numbers B_n/n and $B_n/n(n-1)$ which was suggested by Roland Bacher. We give some counterexamples. Subsequently we extend the results to the general case.

Keywords: Bernoulli number, Kummer congruences, irregular pair, Chinese remainder theorem

Mathematics Subject Classification 2000: 11B68

1 Introduction

Let B_n be the n-th Bernoulli number with $n \geq 0$. They are defined by

$$\frac{z}{e^z - 1} = \sum_{n=0}^{\infty} B_n \frac{z^n}{n!}, \qquad |z| < 2\pi$$

where all numbers B_n are zero with odd index $n > 1$. Therefore, we will consider only even indices concerning Bernoulli numbers throughout this paper. These numbers play an important role in several topics in mathematics. Here, we are interested in the numbers

$$\frac{B_n}{n} \quad \text{and} \quad \frac{B_n}{n(n-1)}.$$

The latter numbers occur, e.g., in approximation formulas of harmonic numbers H_n resp. Stirling's approximation of $\log \Gamma(x)$, see [2, pp. 480–482].

For rational numbers r we use the representation $r = a/b$ where $\gcd(a, b) = 1$ and $b > 0$. We define $\operatorname{num}(r) = |a|$ for the unsigned numerator of r. The notation $m \mid r$ where m is a positive integer means that $m \mid \operatorname{num}(r)$; we shall also write $r \equiv 0 \pmod{m}$ in that case.

Now, we need some basic facts about Bernoulli numbers, see [3, Chapter 15].

Definition 1.1. Let p be an odd prime. A pair (p, l) is called an *irregular pair* if $p \mid B_l$ with $2 \leq l \leq p-3$ and even l. The *index of irregularity* of p is defined by

$$i(p) := \#\{(p, l) \text{ is an irregular pair} : \; l = 2, 4, \ldots, p-3\}.$$

Then p is called an *irregular* prime if $i(p) > 0$, otherwise a *regular* prime.

Let φ be Euler's totient function. The classical Kummer congruences state for even positive integers n, n', p prime with $p-1 \nmid n$, and $n \equiv n' \pmod{\varphi(p)}$ that

$$\frac{B_n}{n} \equiv \frac{B_{n'}}{n'} \pmod{p}. \tag{1.1}$$

It is well known that the numerator $\mathrm{num}(B_n/n)$ equals 1 for $n = 2, 4, 6, 8, 10, 14$; otherwise the numerator is a product of powers of irregular primes. Let (p, l) be an irregular pair. Then the Kummer congruences (1.1) provide for all $k \in \mathbb{N}_0$ that

$$p \mid \frac{B_{l+k\varphi(p)}}{l+k\varphi(p)}. \tag{1.2}$$

The following conjecture about numerators of B_n/n and $B_n/n(n-1)$ was suggested by Roland Bacher; see The Online Encyclopedia of Integer Sequences [5], sequence **A092291**. First values are given by 574, 1269, 1910, 3384, 1185, 1376, 9611. The statements differ by a factor 2, because we use only even indices n instead of $2n$.

Conjecture 1.2. *Let (p, l) be an irregular pair with smallest index l in case $i(p) > 1$. Define*

$$A(p) = \min_{m \in 2\mathbb{N}} \left\{ m \;\middle|\; \mathrm{num}\left(\frac{B_m}{m}\right) \Big/ \mathrm{num}\left(\frac{B_m}{m(m-1)}\right) \;=\; p \right\}.$$

Then $A(p) = (l-1)p + 1$.

Actually, let p_n be the n-th irregular prime (sequence **A000928**: 37, 59, 67, 101, 103, ...), then $A(p_n)/2$ gives sequence **A092291**.

2 Counterexamples

Since Conjecture 1.2 does not cover all irregular pairs, we shall extend our research to all of them. Note that, for example, $(157, 62)$ and $(157, 110)$ are irregular pairs and the index of irregularity is $i(157) = 2$.

Theorem 2.1. *Let (p, l) be an irregular pair. Define*

$$A(p, l) = \min_{k \in \mathbb{N}_0} \left\{ m = l + k\varphi(p) \;\middle|\; \mathrm{num}\left(\frac{B_m}{m}\right) \Big/ \mathrm{num}\left(\frac{B_m}{m(m-1)}\right) \;=\; p \right\}.$$

Then $A(p, l) = (l-1)p + 1$ if and only if one of the following cases holds that

(1) the factor $l-1$ has no irregular prime factors,

(2) for all irregular prime divisors q of $l-1$ we have $q \nmid B_{(l-1)p+1}/((l-1)p+1)$.

Otherwise $A(p, l) > (l-1)p + 1$ or $A(p, l)$ has no solution.

Proof. First of all, we show that $A(p, l) \geq (l-1)p + 1$. To solve the equation

$$\mathrm{num}\left(\frac{B_m}{m}\right) \Big/ \mathrm{num}\left(\frac{B_m}{m(m-1)}\right) \;=\; p,$$

the factor $m-1$ must have the form $m-1=pc$ with some positive integer c to reduce the p-power of the second numerator. In other words, we must have

$$\operatorname{ord}_p \text{ num}\left(\frac{B_m}{m}\right) = s \quad \text{and} \quad \operatorname{ord}_p \text{ num}\left(\frac{B_m}{m(m-1)}\right) = s-1$$

with some integer $s \geq 1$. Let m' be the smallest possible value we are searching for. By (1.2) we then have $m' = l + k(p-1)$ and $m'-1 = pc$. This yields

$$l - 1 + k(p-1) = pc \quad \text{resp.} \quad k \equiv l-1 \pmod{p}.$$

By definition we have $1 < l < p-2$. Thus $k = l-1$ is the smallest possible value and finally

$$A(p,l) \geq m' = l + (l-1)(p-1) = (l-1)p + 1.$$

Now, we have to take care that $m'-1 = (l-1)p$ does not delete other irregular prime factors of the numerator of $B_{m'}/m'$. In the case (1) nothing happens. In the case (2) an irregular prime divisor q of $l-1$ must not appear in the numerator of $B_{m'}/m'$. If case (1) or case (2) is satisfied then $A(p,l) = m'$. □

Using Kummer congruences (1.1) and the property (1.2) again, we can now reformulate Conjecture 1.2 to an extended equivalent conjecture which is described only by irregular pairs.

Conjecture 2.2. *Let (p,l) be an irregular pair. If q is an irregular prime divisor of $l-1$ then for all irregular pairs (q,l') the following holds that*

$$(l-1)p \not\equiv l'-1 \pmod{q-1}.$$

But this conjecture is **not** true. We have done some calculations for all irregular pairs (p,l) with $p < 1\,000\,000$ using a database of irregular pairs calculated in [1]. In that range there are 39 181 irregular pairs all together, 16 540 of them have irregular prime divisors of the corresponding $l-1$ and 149 exceptions occur. The first five exceptions and the last calculated exception are listed below.

(p,l)	$m=(l-1)p+1$	$l-1$	(q,l')
$(6449, 4884)$	31 490 468	$19 \cdot 257$	$(257, 164)$
$(8677, 2658)$	23 054 790	2657	$(2657, 710)$
$(11351, 1044)$	11 839 094	$7 \cdot 149$	$(149, 130)$
$(12527, 2122)$	26 569 768	$3 \cdot 7 \cdot 101$	$(101, 68)$
$(15823, 482)$	7 610 864	$13 \cdot 37$	$(37, 32)$
...	...	...	...
$(999599, 649768)$	649 506 443 434	$3 \cdot 59 \cdot 3671$	$(59, 44)$

Note that there are two irregular pairs $(6449, 4884)$ and $(6449, 5830)$. The first of them disproves the suggested conjecture with minimal $l = 4884$. The smallest index for which such an exception occurs is 7 610 864. This index is the smallest of our calculated exceptions for $p < 1\,000\,000$. For an irregular pair (p,l) with $p > 1\,000\,000$ we then obtain an index $m = (l-1)p + 1 > 37 \cdot 10^6$ for a possible exception, because 37 is the first irregular prime.

3 Extending the results to prime powers

In order to extend the results to irregular prime powers, we need some further definitions and generalizations. First, the Kummer congruences generally state for $r \geq 1$, even n, n', p prime with $p-1 \nmid n$, and $n \equiv n' \pmod{\varphi(p^r)}$ that

$$(1-p^{n-1})\frac{B_n}{n} \equiv (1-p^{n'-1})\frac{B_{n'}}{n'} \pmod{p^r}. \tag{3.1}$$

The definition of irregular pairs can be extended to irregular prime powers which was introduced by the author [4]. Here we shall recall necessary facts.

Definition 3.1. Let p be an odd prime and n, l be positive integers. A pair (p, l) is called an *irregular pair of order* n if $p^n \mid B_l/l$ with $2 \leq l < \varphi(p^n)$ and even l. Let

$$\Psi_n^{\mathrm{irr}} := \{(p,l) : \, p^n \mid B_l/l, \, p \text{ is an odd prime}, \, 2 \leq l < \varphi(p^n), \, 2 \mid l\}$$

be the set of irregular pairs of order n. For an odd prime p the *index* of irregular pairs of order n is defined by

$$i_n(p) := \#\{(p,l) : \, (p,l) \in \Psi_n^{\mathrm{irr}}\}.$$

Let $(p, l_n) \in \Psi_n^{\mathrm{irr}}$ and $(p, l_m) \in \Psi_m^{\mathrm{irr}}$ be irregular pairs of order n resp. m where $n > m \geq 1$. We say that (p, l_n) is *related* to (p, l_m) if $l_n \equiv l_m \pmod{\varphi(p^m)}$. For $(p, l) \in \Psi_n^{\mathrm{irr}}$ we p-adically write

$$(p, s_1, s_2, \ldots, s_n) \in \widehat{\Psi}_n^{\mathrm{irr}} \quad \text{where} \quad l = \sum_{\nu=1}^{n} s_\nu \, \varphi(p^{\nu-1})$$

with $0 \leq s_\nu < p$ for $\nu = 1, \ldots, n$ and $2 \leq s_1 \leq p-3$, $2 \mid s_1$. The corresponding set is denoted as $\widehat{\Psi}_n^{\mathrm{irr}}$. The pair (p, l) and the element $(p, s_1, s_2, \ldots, s_n)$ are called *associated*. For an irregular pair (p, l) we finally define

$$\Delta_{(p,l)} \equiv p^{-1}\left(\frac{B_{l+\varphi(p)}}{l+\varphi(p)} - \frac{B_l}{l}\right) \pmod{p}$$

with $0 \leq \Delta_{(p,l)} < p$.

Note that this definition includes for $n = 1$ the former definition of irregular pairs with $i(p) = i_1(p)$. By (3.1) we have the property that if $(p, l) \in \Psi_n^{\mathrm{irr}}$ then

$$p^n \mid B_{l+k\varphi(p^n)}/(l + k\varphi(p^n)) \tag{3.2}$$

for all $k \in \mathbb{N}_0$. We also call $(p, s_1, s_2, \ldots, s_n)$ an *irregular pair*, since $(s_1, s_2, \ldots, s_n)$ is the second parameter given p-adically. The main result of irregular pairs of higher order can be stated as follows, see [4, Theorem 3.1].

Theorem 3.2. *Let (p, l_1) be an irregular pair. If $\Delta_{(p,l_1)} \neq 0$ then for each $n > 1$ there exists exactly one related irregular pair of order n. There is a unique sequence $(l_n)_{n \geq 1}$ resp. $(s_n)_{n \geq 1}$ with*

$$(p, l_n) \in \Psi_n^{\mathrm{irr}} \quad \textit{resp.} \quad (p, s_1, \ldots, s_n) \in \widehat{\Psi}_n^{\mathrm{irr}}.$$

If $\Delta_{(p,l_{1,\nu})} \neq 0$ for all $i(p)$ irregular pairs $(p, l_{1,\nu}) \in \Psi_1^{\mathrm{irr}}$, then

$$i(p) = i_2(p) = i_3(p) = \ldots .$$

So far, no irregular pair (p,l) with $\Delta_{(p,l)} = 0$ has yet been found; calculations of Buhler, Crandall, Ernvall, Metsänkylä, and Shokrollahi [1] ensure this result for all irregular $p < 12\,000\,000$. Since the case $\Delta_{(p,l)} = 0$ would possibly imply a strange behavior of irregular pairs of higher order without any regularity, it is conjectured that this will never happen.

Theorem 3.3. *Let $r \geq 1$ be an integer. Let (p,l) be an irregular pair with $\Delta_{(p,l)} \neq 0$. Let $(p,l_r) \in \Psi_r^{\rm irr}$ resp. $(p,s_1,\ldots,s_r) \in \widehat{\Psi}_r^{\rm irr}$ be the related irregular pair of order r. Define*

$$A(p^r,l_r) = \min_{k \in \mathbb{N}_0} \left\{ m = l_r + k\varphi(p^r) \;\middle|\; \operatorname{num}\left(\frac{B_m}{m}\right) \Big/ \operatorname{num}\left(\frac{B_m}{m(m-1)}\right) \;=\; p^r \right\}.$$

Then the condition $(p,s_1,s_2,\ldots,s_r) = (p,l,l-1,\ldots,l-1)$ resp. $l_r - 1 = (l-1)p^{r-1}$ is necessary that $A(p^r,l_r)$ has possibly a solution. Furthermore $A(p^r,l_r) = (l_r-1)p+1 = (l-1)p^r+1$ if and only if one of the following cases holds that

(1) the factor $l-1$ has no irregular prime factors,

(2) for all irregular prime divisors q of $l-1$: all irregular pairs (q,l') must satisfy

$$(l-1)p^r \;\not\equiv\; l'-1 \pmod{q-1}.$$

Otherwise $A(p^r,l_r) > (l-1)p^r+1$ or $A(p^r,l_r)$ has no solution.

Lemma 3.4. *Let $n \geq 1$ and $s_1,\ldots,s_{n+1}$ be integers with $0 \leq s_\nu < p$ for all $\nu = 1,\ldots,n+1$. If*

$$\sum_{\nu=1}^{n} s_\nu\, \varphi(p^{\nu-1}) = s_{n+1}\, p^{n-1},$$

then $s_1 = s_2 = \ldots = s_{n+1}$.

Proof. Reordering the terms yields

$$0 = \sum_{\nu=1}^{n} s_\nu\, \varphi(p^{\nu-1}) - s_{n+1}\, p^{n-1} = \sum_{\nu=1}^{n} (s_\nu - s_{\nu+1})\, p^{\nu-1}$$

which deduces the result p-adically by induction. □

Proof of Theorem 3.3. The case $r=1$ is already covered by Theorem 2.1 with $(p,l) = (p,l_1) = (p,s_1)$. For now let $r \geq 2$. First we shall show the proposed formula for $A(p^r,l_r)$. To solve

$$\operatorname{num}\left(\frac{B_m}{m}\right) \Big/ \operatorname{num}\left(\frac{B_m}{m(m-1)}\right) \;=\; p^r,$$

factor $m-1$ must have the form $m-1 = p^r c$ with some positive integer c. Then $m-1$ must reduce the p-power of the second numerator in order that

$$\operatorname{ord}_p \operatorname{num}\left(\frac{B_m}{m}\right) = u \quad \text{and} \quad \operatorname{ord}_p \operatorname{num}\left(\frac{B_m}{m(m-1)}\right) = u - r$$

with some integer $u \geq r$, since $(p, l_r) \in \Psi_r^{\text{irr}}$. Let m' be the smallest possible value. By (3.2) we have $m' = l_r + k\varphi(p^r)$ and $m' - 1 = p^r c$ which yields

$$l_r - 1 + kp^{r-1}(p-1) = p^r c \quad \text{and} \quad l_r - 1 \equiv 0 \pmod{p^{r-1}}. \tag{3.3}$$

Remember that

$$l_r = \sum_{\nu=1}^{r} s_\nu \varphi(p^{\nu-1}) < \varphi(p^r).$$

Thus we obtain

$$0 < l_r - 1 = p^{r-1}\, t < p^{r-1}(p-1)$$

with $0 < t < p - 1$. By rewriting (3.3) we get

$$p^{r-1}\, t + kp^{r-1}(p-1) = p^r c \quad \text{and} \quad kp^{r-1} \equiv tp^{r-1} \pmod{p^r}$$

which provides $k \equiv t \pmod{p}$ and finally $k = t$ as smallest value. Note that $l = s_1$ and $2 \leq l \leq p - 3$. Now, using Lemma 3.4 with $l_r - 1 = tp^{r-1}$ yields $s_1 - 1 = s2 = \ldots = s_r = t$. Thus, we derive the following conditions

$$(p, s_1, s_2, \ldots, s_r) = (p, l, l-1, \ldots, l-1) \quad \text{and} \quad l_r - 1 = (l-1)p^{r-1}.$$

After all, we obtain

$$A(p^r, l_r) - 1 \geq m' - 1 = l_r - 1 + (l-1)\varphi(p^r) = (l-1)p^r = (l_r - 1)p.$$

To avoid that an irregular prime divisor q of the remaining factor $l-1$ of $m'-1$ divides $B_{m'}/m'$, we must have

$$m' \not\equiv l' \pmod{q-1}$$

for all irregular pairs (q, l'). Then $A(p^r, l_r) = m'$. □

Corollary 3.5. *Let (p, l) be an irregular pair with $\Delta_{(p,l)} \neq 0$. If $(p, l, l-1) \notin \widehat{\Psi}_2^{\text{irr}}$ then $A(p^r, l_r)$ as defined in Theorem 3.3 has no solution for all $r \geq 2$.*

Proof. As a result of Theorem 3.2, if $\Delta_{(p,l)} \neq 0$ then a unique sequence $(s_\nu)_{\nu \geq 1}$ exists that describes all irregular pairs of higher order related to (p, l). Then one has $(p, s_1, \ldots, s_r) \neq (p, l, l-1, \ldots, l-1)$ for all $r \geq 2$. □

The condition $(p, s_1, s_2, \ldots, s_r) = (p, l, l-1, \ldots, l-1)$ is a very strange condition. Note that no $(p, l, l-1) \in \widehat{\Psi}_2^{\text{irr}}$ has been found yet. It is quite remarkable that the conditions $\Delta_{(p,l)} \neq 0$ and $(p, l, l-1) \notin \widehat{\Psi}_2^{\text{irr}}$ play an important role in Iwasawa theory of cyclotomic fields over $\mathbb{Q}$, see [6] and particularly [4, Section 6]. Again, calculations in [1] ensure that $(p, l, l-1) \notin \widehat{\Psi}_2^{\text{irr}}$ for $p < 12\,000\,000$.

Remark 3.6. Although the more complicated case $\Delta_{(p,l)} = 0$ should not happen, Corollary 3.5 is also valid in that case. If $(p, l, l-1) \notin \widehat{\Psi}_2^{\text{irr}}$ then there are no related irregular pairs $(p, l, l-1, \ldots, l-1) \in \widehat{\Psi}_r^{\text{irr}}$ for $r > 2$. This can be shown by [4, Theorem 3.2].

4 The composite case

For completeness we shall examine the composite case. For now, we consider composite integers c where

$$c = \prod_{\nu=1}^{n} p_\nu^{e_\nu}$$

with irregular primes p_ν and $n > 1$. For now, p will only denote an irregular prime. To determine the minimal index for the composite case, define

$$\Lambda(d) = \min_{m \in 2\mathbb{N}} \left\{ m \;\middle|\; \operatorname{num}\left(\frac{B_m}{m}\right) \Big/ \operatorname{num}\left(\frac{B_m}{m(m-1)}\right) \equiv 0 \pmod{d} \right\};$$

in case of no solution define $\Lambda(d) = \infty$. Then, by Theorem 2.1, we always have

$$\Lambda(p) = \min_{(p,l) \in \Psi_1^{\mathrm{irr}}} (l-1)p + 1.$$

Theorem 3.3 asserts for $r \geq 2$ that

$$\Lambda(p^r) = \min_{(p,l,l-1,\ldots,l-1) \in \widehat{\Psi}_r^{\mathrm{irr}}} (l-1)p^r + 1,$$

but there is no solution for $p < 12\,000\,000$. Note that $m = 12$ is the smallest index for which $\operatorname{num}(B_m/m) > 1$. Hence, for $p > 12\,000\,000$ and $r \geq 2$ we have the estimate

$$\Lambda(p^r) > 1.58 \cdot 10^{15}. \tag{4.1}$$

Lemma 4.1. *Let $c = \prod_\nu p_\nu^{e_\nu}$ with irregular primes p_ν. Then*

$$\Lambda(c) \geq \max_\nu \Lambda(p_\nu^{e_\nu}).$$

Proof. Assume that $\Lambda(c) < \Lambda(p_\nu^{e_\nu})$ for a fixed ν. But this contradicts the definition of Λ, because $p_\nu^{e_\nu} \mid c$. The case of no solution is handled similarly. □

Let $\mathcal{M}$ be the smallest index for composite numbers c such that

$$\mathcal{M} = \min_c \Lambda(c).$$

By our formerly calculated exceptions, we have an upper bound:

$$\mathcal{M} \leq 7\,610\,864.$$

The estimate (4.1) for prime powers above and Lemma 4.1 imply that we now have to examine composite numbers which are squarefree. Therefore, define the minimal value of Λ for composite squarefree numbers having $n \geq 2$ irregular prime factors by

$$\mathcal{M}_n = \min_{c = p_1 \cdots p_n} \Lambda(c).$$

Then, by definition we have

$$\mathcal{M} = \mathcal{M}_2 \leq \mathcal{M}_3 \leq \ldots .$$

For further results we need the well-known Chinese remainder theorem (CRT), see [3, p. 34], and its generalization (CRT').

Theorem 4.2 (CRT)**.** *Let $w_1, \ldots, w_n$ be positive integers which are pairwise relatively prime. Define $W = \prod_{\nu=1}^{n} w_\nu$. For a given system of simultaneous congruences*

$$x \equiv a_\nu \pmod{w_\nu}, \qquad \nu = 1, \ldots, n,$$

there always exists a unique integer $x \pmod W$ with

$$x \equiv \sum_{\nu=1}^{n} a_\nu \, b_\nu \frac{W}{w_\nu} \pmod W$$

and b_ν defined by

$$b_\nu \frac{W}{w_\nu} \equiv 1 \pmod{w_\nu}, \qquad \nu = 1, \ldots, n.$$

Theorem 4.3 (CRT')**.** *Let $w_1, \ldots, w_n$ be positive integers. A system of simultaneous congruences*

$$x \equiv a_\nu \pmod{w_\nu}, \qquad \nu = 1, \ldots, n$$

has a solution if and only if

$$a_i \equiv a_j \pmod{\gcd(w_i, w_j)}$$

for all $i \neq j$. Define $W = \mathrm{lcm}(w_1, \ldots, w_n)$, then x has a unique solution $\pmod W$.

To state our next theorem, we introduce a new definition to characterize a set of irregular pairs.

Definition 4.4. Irregular pairs $(p_1, l_1), \ldots, (p_n, l_n)$ are called *friendly* if

$$l_i \equiv l_j \pmod{\gcd(p_i - 1, p_j - 1)}$$

for all $i \neq j$. They are called *strong friendly* if, in addition,

$$p_i \not\equiv 1 \pmod{p_j} \qquad \text{or} \qquad (p_i, l_i) \equiv (1, 1) \pmod{p_j}$$

for all $i \neq j$.

For example, the irregular pairs $(37, 32)$, $(59, 44)$ and $(101, 68)$ are strong friendly. The sets $\{(101, 68), (607, 592)\}$ and $\{(131, 22), (263, 100)\}$ are sets of friendly irregular pairs, but they are not strong friendly.

Theorem 4.5. *Let $n \geq 2$ and $c = p_1 \cdots p_n$ be a composite number of distinct irregular primes. Then $\Lambda(c)$ has only a solution if there exists a set of strong friendly irregular pairs $S = \{(p_1, l_1), \ldots, (p_n, l_n)\}$. In case of existence there is a unique integer m_S with*

$$c \leq m_S - 1 \leq \mathrm{lcm}(c, p_1 - 1, \ldots, p_n - 1)$$

which simultaneously solves the congruences

$$m_S - 1 \equiv p_\nu(l_\nu - 1) \pmod{p_\nu(p_\nu - 1)}, \quad \nu = 1, \ldots, n.$$

Then $\Lambda(c)$ is given by

$$\Lambda(c) = \min_S m_S,$$

whereby S passes all such sets of strong friendly irregular pairs.

Proof. To derive conditions let m be an integer solving

$$\operatorname{num}\left(\frac{B_m}{m}\right) \Big/ \operatorname{num}\left(\frac{B_m}{m(m-1)}\right) \equiv 0 \pmod{c}.$$

Thus, $c \mid B_m/m$ and $c \mid m-1$ provide the existence of irregular pairs (p_ν, l_ν) with

$$\begin{aligned} m-1 &\equiv 0 && \pmod{p_\nu}, \\ m-1 &\equiv l_\nu - 1 && \pmod{p_\nu - 1} \end{aligned} \tag{4.2}$$

for $\nu = 1, \ldots, n$. The system (4.2) of simultaneous congruences has only a solution if conditions of CRT' are satisfied. Therefore we have to recognize two cases that

$$\begin{aligned} l_i - 1 &\equiv l_j - 1 && \pmod{\gcd(p_i - 1, p_j - 1)}, \\ l_i - 1 &\equiv 0 && \pmod{\gcd(p_i - 1, p_j)} \end{aligned} \tag{4.3}$$

which must be valid for all $i \neq j$. The first congruence of (4.3) implies that all considered irregular pairs must be friendly. Additionally by the second congruence they must be strong friendly. This property must hold for a solution and defines the set S. Combining (4.2) by CRT, we get

$$m - 1 \equiv p_\nu(l_\nu - 1) \pmod{p_\nu(p_\nu - 1)}, \quad \nu = 1, \ldots, n. \tag{4.4}$$

Let $W = \operatorname{lcm}(p_1(p_1-1), \ldots, p_n(p_n-1))$, then system (4.2) resp. (4.4) has a unique solution $\pmod{W}$ by CRT' and given set S. Requiring that $1 \leq m_S - 1 \leq W$, we obtain a minimal solution $m_S - 1$ with the desired properties. If $i(p_\nu) \geq 2$ holds for one index ν, then probably other sets S can exist corresponding to irregular primes $p_1, \ldots, p_n$. Therefore all such sets must be considered to get

$$\Lambda(c) = \min_S m_S.$$

□

Theorem 4.5 implies the following easy algorithm.

Algorithm 4.6. Let $n \geq 2$, U be positive integers. Given an existing upper bound U of $\mathcal{M}_n$, define $u = \lfloor U^{1/n} \rfloor$. Otherwise set $U = u = \infty$. Consider irregular primes

$$p_1 < \ldots < p_n \quad \text{with} \quad p_1 \cdots p_n < U, \quad p_1 < u. \tag{4.5}$$

Start with smallest primes. For each tuple of primes do

- Step 1. Check for sets $S = \{(p_1, l_1), \ldots, (p_n, l_n)\}$ of strong friendly irregular pairs. For each existing set S calculate m_S using Theorem 4.5. Let $m = \min_S m_S$. If $m < U$ update $U \leftarrow m$ and u.
- Step 2. If possible go to next primes satisfying (4.5), otherwise stop with $\mathcal{M}_n = U$.

Starting with $n = 2$ and $U = 7\,610\,864$ yields $\mathcal{M}_2 = 107\,430$ with $c = 103 \cdot 149$. Thus $\mathcal{M} = 107\,430$ is the smallest index for composite numbers regarding Λ. The result for $n = 3$ is a quite large number with $\mathcal{M}_3 = 3\,754\,314\,782$ for $c = 157 \cdot 401 \cdot 1217$, see table below. To check this result, irregular pairs (p, l) up to $p < 2\,000\,000$ must be considered for the first small primes.

n	S	U	u
2	$\{(37,32),\ (59,44)\}$	272 876	522
2	$\{(103,24),\ (149,130)\}$	107 430	327
3	$\{(37,32),\ (59,44),\ (101,68)\}$	3 979 497 668	1584
3	$\{(157,62),\ (401,382),\ (1217,1118)\}$	3 754 314 782	1554

All results were calculated by several **C++** programs and finally checked with **Mathematica**.

Acknowledgement

The author wishes to thank Tony D. Noe for advising the problem and sequence **A092291**.

References

[1] J. Buhler, R. Crandall, R. Ernvall, T. Metsänkylä, and M. A. Shokrollahi, Irregular primes and cyclotomic invariants to 12 million, *J. Symb. Comput.* **31** (2001), no. 1–2, 89–96.

[2] R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete Mathematics*, Addison-Wesley, 1994.

[3] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Graduate Texts in Mathematics, vol. 84, Springer-Verlag, 2nd edition, 1990.

[4] B. C. Kellner, On irregular prime power divisors of the Bernoulli numbers, *Math. Comp.*, to appear, 1–42. (Preprint at arXiv:math.NT/0409223).

[5] N. J. A. Sloane, The Online Encyclopedia of Integer Sequences (OEIS), 2005.

[6] L. C. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics, vol. 83, Springer-Verlag, 2nd edition, 1997.

Reitstallstr. 7, 37073 Göttingen, Germany
E-mail address: **bk@bernoulli.org**