A conjecture about numerators of Bernoulli numbers related to Integer Sequence A092291

Bernd C. Kellner

5th October 2004*

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. Finally, 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 the power series

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

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

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

which occur, e.g., in approximation formulas of harmonic numbers H_n resp. Stirling's approximation of $\log \Gamma(x)$, see [GKP94, pp. 480–482].

Now, we need some basic facts about Bernoulli numbers which can be found in [IR90, Chapter 15]. In 1850 Kummer introduced the following definition.

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 p is a *regular* prime.

*2. version of 11.04.04, slightly revised

Let φ be the Euler φ-function, then the classical Kummer congruences state for n, n' even, p prime, and $p-1 \nmid n$

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

with $n \equiv n' \pmod{\varphi(p)}$. An easy consequence of the Kummer congruences supplies that the numerator of B_n/n consists only of irregular primes and that infinitely many irregular primes exist. Let (p, l) be an irregular pair. Using congruence (1.1) provides for all $k \in \mathbb{N}_0$

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

The following conjecture about numerators of B_n/n and $B_n/n(n-1)$ was suggested by Roland Bacher, see The On-Line Encyclopedia of Integer Sequences [Slo04], Sequence **A092291**. First values are given by 574, 1269, 1910, 3384, 1185, 1376, 9611. The statements will differ by a factor 2, because we will use only even indices n instead of $2n$. Define $\mathrm{num}(r)$ as the numerator of a rational number r.

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

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

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

Actually, let p_n be the n-th irregular prime, then $A(p_n)/2$ gives Integer Sequence **A092291**.

2 Counterexamples

Because the conjecture does not cover all irregular pairs, we will 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*

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

Then $A(p) = (l-1)p + 1$ is valid and has smallest possible value if and only if one of the following cases holds

(1) $l-1$ has no irregular prime factors.

(2) If q is an irregular prime divisor of $l-1$, then $q \nmid B_{(l-1)p+1}/((l-1)p+1)$.

Proof. First of all, we will prove that $A(p) = (l-1)p + 1$ is the smallest possible value. To solve

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

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

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

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

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

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 case (1) nothing happens. In case (2) an irregular prime divisor q of $l-1$ must not appear in the numerator of $B_{m'}/m'$. □

Using Kummer congruences (1.1) and property (1.2) again, we can now reformulate Conjecture 1.2 to an extended equivalent conjecture 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*

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

But this conjecture is **not** valid. We have done some calculations for all irregular pairs (p,l) with $p < 1\,000\,000$ using a database of irregular pairs calculated in [BCE+01]. 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 $(6449, 5830)$. But 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 irregular pairs (p,l) with $p > 1\,000\,000$ we obtain index $m = (l-1)p + 1 > 37 \cdot 10^6$ for a possible exception, because 37 is the first irregular prime.

3 Extending results to prime powers

In order to extend the results to irregular prime powers, we need some further definitions and generalization. First, the Kummer congruences generally state for $r \geq 1$, n, n' even, p prime, and $p - 1 \nmid n$

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

with $n \equiv n' \pmod{\varphi(p^r)}$.

The definition of irregular pairs can be extended to irregular prime powers which was first introduced by the author [Kel02, Section 2.5], see also [Kel04] for details and new results. Here we will recall necessary facts.

Definition 3.1 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

$$\Psi_n^{\mathrm{irr}} := \{(p, l) : \; p^n \mid B_l/l, \; 2 \leq l < \varphi(p^n), \; 2 \mid l\}$$

be the set of irregular pairs of order n. For a 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 $(p, l) \in \Psi_n^{\mathrm{irr}}$ be an irregular pair of order n. Let

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

be the p-adic notation of (p, l) with $0 \leq s_\nu < p$ for $\nu = 1, \ldots, n$ and $2 \mid s_1$, $2 \leq s_1 \leq p-3$. The corresponding set will be denoted as $\widehat{\Psi}_n^{\mathrm{irr}}$. The pairs (p, l) and $(p, s_1, s_2, \ldots, s_n)$ will be called associated. Define for an irregular pair (p, l)

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

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

Note that this definition includes for $n = 1$ the usual definition of irregular pairs with $i(p) = i_1(p)$. By Kummer congruences (3.1) the interval $[2, \varphi(p^n) - 2]$ is given for irregular pairs of order n if they exist. Moreover, 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 $k \in \mathbb{N}_0$. Note that $(p, s_1, s_2, \ldots, s_n)$ is also called a *pair* keeping in mind that $(s_1, s_2, \ldots, s_n)$ is the second parameter in a p-adic manner. The main result of irregular pairs of higher order can be stated as follows, see [Kel04, Theorem 3.1, p. 8].

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 irregular pair of order n corresponding to (p, l_1). Therefore a unique sequence $(l_n)_{n\geq 1}$ resp. $(s_n)_{n\geq 1}$ exists 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 been found for $p < 12\,000\,000$ by calculations in [BCE+01]. Because the case $\Delta_{(p,l)} = 0$ would imply a strange behavior, 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 $\Delta_{(p,l)} \neq 0$. Then let $(p, l_r) \in \Psi_r^{\mathrm{irr}}$ resp. $(p, s_1, \ldots, s_r) \in \widehat{\Psi}_r^{\mathrm{irr}}$ be the corresponding irregular pair of order r. Define*

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

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

(1) $l - 1$ has no irregular prime factors.

(2) If q is an irregular prime divisor of $l-1$, then all irregular pairs (q, l') must satisfy

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

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 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. Case $r = 1$ is handled by Theorem 2.1, because $(p, l) = (p, l_1) = (p, s_1)$. For now let $r \geq 2$. First we will show the proposed formula for $A(p^r)$. 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 integer c. Then $m-1$ must reduce the p-power of the second numerator in order that

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

is valid with some integer $u \geq r$ which is granted by irregular pair (p, l_r) of order r. 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

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

Keeping in mind that $l_r = \sum_{\nu=1}^{r} s_\nu \varphi(p^{\nu-1}) < \varphi(p^r)$, we obtain

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

with $0 < t < p-1$. 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

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

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 $A(p^r)$ is valid with the derived value. □

Corollary 3.5 *Let (p,l) be an irregular pair with $\Delta_{(p,l)} \neq 0$. Let $r \geq 2$ be an integer, $(p, s_1, \ldots, s_r) \in \widehat{\Psi}_r^{\text{irr}}$, and $A(p^r)$ be defined as in Theorem 3.3. Assume $(p, s_1, s_2, \ldots, s_r)$ $\neq (p, l, l-1, \ldots, l-1)$ then $A(p^u)$ related to (p,l) has no solution for all $u \geq r$.*

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 $(p, s_1, \ldots, s_r, \ldots, s_u) \neq (p, l, l-1, \ldots, l-1)$ for all $u > r$. □

The condition $(p, s_1, s_2, \ldots, s_r) = (p, l, l-1, \ldots, l-1)$ is a very strange condition. No such irregular pair $(p, s_1, s_2) \in \widehat{\Psi}_2^{\text{irr}}$ of order two with $s_2 = s_1 - 1$ has been found yet. For irregular primes $p < 1000$ the smallest difference $|s_1 - s_2|$ is 4 which happens for the following elements

$$(353, 186, 190),\ (647, 554, 558) \in \widehat{\Psi}_2^{\text{irr}}\,.$$

Therefore $A(p^r)$ has no solution for $p < 1000$ and $r \geq 2$. Calculated irregular pairs of order 10 for $p < 1000$ can be found in [Kel04, Table A.3].

Remark 3.6 Although the more complicated case $\Delta_{(p,l)} = 0$ should not happen, Theorem 3.3 is also valid in that case. We only need an irregular pair $(p, l_r) \in \Psi_r^{\mathrm{irr}}$ and its associated pair $(p, s_1, \ldots, s_r) \in \widehat{\Psi}_r^{\mathrm{irr}}$ which are related to (p, l). Corollary 3.5 remains to be valid in a similar way. A strong condition must hold that further irregular pairs of order $r + 1$ related to (p, l_r) exist. In case of existence they all have the form $(p, s_1, \ldots, s_r, t) \in \widehat{\Psi}_{r+1}^{\mathrm{irr}}$ with $0 \leq t < p$, see [Kel04, Theorem 3.2, p. 8].

4 The composite case

For completeness we will examine the composite case. For now, we will recognize composite integers c

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

having only irregular primes p_ν in its factorization with $n > 1$. Therefore, p will only denote irregular primes. To determine the minimal index of the composite case, define

$$\Lambda(c) = \min_m \left\{ m \;\Big|\; \operatorname{num}\left(\frac{B_m}{m}\right) \Big/ \operatorname{num}\left(\frac{B_m}{m(m-1)}\right) \equiv 0 \pmod{c} \right\},$$

in case of no solution define $\Lambda(c) = \infty$. 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 $r \geq 2$

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

but there is no solution for $p < 1000$. Note that $m = 12$ is the smallest index for which $\operatorname{num}(B_m/m) > 1$. Hence, for $p > 1000$, $r \geq 2$, and $\Lambda(p^r) < \infty$, we have a weak estimate

$$\Lambda(p^r) > 11 \cdot 10^6\,. \tag{4.1}$$

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 $\Lambda(c) < \Lambda(p_\nu^{e_\nu})$ 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 which a composite number appears. By our formerly calculated exceptions, we have an upper bound

$$\mathcal{M} \;=\; \min_c \Lambda(c) \;\leq\; 7\,610\,864\,. \tag{4.2}$$

Regarding estimate (4.1) for prime powers above and using Lemma 4.1, for now, we only 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 obviously have

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

For further results we need the well-known Chinese remainder theorem (CRT), s. [IR90, p. 34], and its generalization.

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

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

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

To state our next theorem, we will 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

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

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

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

holds for all $i \neq j$.

For example, the irregular pairs (37,32), (59,44), (101,68) are strong friendly. $\{(101,68), (607,592)\}$ 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*

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

which simultaneously solves the congruences

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

$\Lambda(c)$ is then given by

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

whereas 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

$$\begin{aligned} m - 1 &\equiv 0 && \pmod{p_\nu} \\ m - 1 &\equiv l_\nu - 1 && \pmod{p_\nu - 1} \end{aligned} \tag{4.3}$$

for $\nu = 1, \ldots, n$. The system (4.3) of simultaneous congruences has only a solution if conditions of CRT' are satisfied. Therefore we have to recognize two cases

$$\begin{aligned} l_i - 1 &\equiv l_j - 1 && \pmod{\gcd(p_i - 1, p_j - 1)} \\ l_i - 1 &\equiv 0 && \pmod{\gcd(p_i - 1, p_j)} \end{aligned} \tag{4.4}$$

which must be valid for all $i \neq j$. The first congruence of (4.4) 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 set S. Combining (4.3) by CRT, we get

$$m - 1 \equiv p_\nu(l_\nu - 1) \pmod{p_\nu(p_\nu - 1)}\,, \quad \nu = 1, \ldots, n\,. \tag{4.5}$$

Let $W = \operatorname{lcm}(p_1(p_1 - 1), \ldots, p_n(p_n - 1))$, then system (4.3) resp. (4.5) has a unique solution $\pmod{W}$ by CRT' and given set S. Taking $1, \ldots, W$ as residue classes, 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 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

$$p_1 < \ldots < p_n \quad \text{with} \quad p_1 \cdots p_n < U \,, \quad p_1 < u \,. \tag{4.6}$$

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 (4.6), 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 which a composite value occurs. The result for $n = 3$ is a quite large number with $\mathcal{M}_3 = 3\,754\,314\,782$, 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.

5 A connection with Iwasawa theory

In Section 4 we have seen that Theorem 3.3 asserts for $r \geq 2$

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

noting that there is no solution for $p < 1000$. For a solution with $r \geq 2$ we basically need the existence of an irregular pair $(p, l, l-1) \in \widehat{\Psi}_2^{\mathrm{irr}}$ of order two.

Now, the remarkable fact is that conditions $\Delta_{(p,l)} \neq 0$ and $(p, l, l-1) \notin \widehat{\Psi}_2^{\mathrm{irr}}$ play an important role in Iwasawa theory of cyclotomic fields over $\mathbb{Q}$, see [Kel04, Section 6]. Here we give a brief summary.

Let $\mathbb{Q}(\mu_{p^n})$ be the cyclotomic field and $\mathbb{Q}(\mu_{p^n})^+$ its maximal real subfield with μ_{p^n} as the set of p^n-th roots of unity Define the class number $h_p = h(\mathbb{Q}(\mu_p))$ and its factoring $h_p = h_p^- \, h_p^+$ with $h_p^+ = h(\mathbb{Q}(\mu_p)^+)$ and h_p^- as the relative class number introduced by Kummer. For details of the following theorem, see [Was97, Corollary 10.17, p. 202]. Note that conditions (2) and (3) are equivalently exchanged by our definitions.

Theorem 5.1 *Let p be an irregular prime. Assume the following conditions*

(1) The conjecture of Kummer–Vandiver holds: $p \nmid h_p^+$

(2) The Δ-Conjecture holds: $\Delta_{(p,l)} \neq 0$

(3) A special irregular pair of order two does not exist: $(p, l, l-1) \notin \widehat{\Psi}_2^{\mathrm{irr}}$

for all irregular pairs (p, l). Then $\operatorname{ord}_p h(\mathbb{Q}(\mu_{p^n})) = i(p)\, n$ is valid for all $n \geq 1$.

Buhler, Crandall, Ernvall, Metsänkylä, and Shokrollahi [BCE+01] have calculated not only irregular pairs, but also associated cyclotomic invariants up to $p < 12\,000\,000$. These calculations ensure that no irregular pair $(p, l, l-1) \in \widehat{\Psi}_2^{\mathrm{irr}}$ exists in that range.

Therefore we have a much stronger estimate than (4.1)

$$\Lambda(p^r) > 1.729 \cdot 10^{15}$$

which can be obviously improved by choosing a greater value $l > 12$ examining the numerators of the first divided Bernoulli numbers B_m/m.

Acknowledgement

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

Bernd C. Kellner
address: Reitstallstr. 7, 37073 Göttingen, Germany
email: bk@bernoulli.org

References

[BCE+01] J. Buhler, R. Crandall, R. Ernvall, T. Metsänkylä, and M. A. Shokrollahi. Irregular primes and cyclotomic invariants to 12 million. *Journal of Symbolic Computation*, 31(1/2):89–96, January 2001.

[GKP94] R. L. Graham, D. E. Knuth, and O. Patashnik. *Concrete Mathematics*. Addison-Wesley, Reading, MA, USA, 1994.

[IR90] K. Ireland and M. Rosen. *A Classical Introduction to Modern Number Theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, 2nd edition, 1990.

[Kel02] B. C. Kellner. Über irreguläre Paare höherer Ordnungen. *Diplomarbeit. Mathematisches Institut der Georg August Universität zu Göttingen, Germany. Also available at http://www.bernoulli.org/∼bk/irrpairord.pdf*, 2002.

[Kel04] B. C. Kellner. On irregular prime powers of Bernoulli numbers. *Preprint, to appear*, 1–29, 2004. arXiv:math.NT/0409223

[Slo04] N. J. A. Sloane. The On-Line Encyclopedia of Integer Sequences. *Published electronically at http://www.research.att.com/∼njas/sequences/*, 2004.

[Was97] L. C. Washington. *Introduction to Cyclotomic Fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, 2nd edition, 1997.