SUMS OF RECIPROCALS MODULO COMPOSITE INTEGERS

JOHN B. COSGRAVE AND KARL DILCHER

Abstract. In 1938, as part of a wider study, Emma Lehmer derived a set of four related congruences for certain sums of reciprocals over various ranges, modulo squares of odd primes. These were recently extended to congruences modulo squares of positive integers n, with certain restrictions on n. In this paper we characterize those excluded n for which the congruences still hold, and find the correct reduced moduli in the cases in which the congruences do not hold.

1. Introduction

Sums of reciprocals of consecutive integers modulo a prime or prime power have attracted a great deal of interest in the past. Possibly the first occurrence in the literature is in a paper of 1850 by Eisenstein [10] who showed, essentially, that for an odd prime p we have

$$\sum_{j=1}^{\frac{p-1}{2}} \frac{1}{j} \equiv -2\, q_p(2) \pmod{p}, \tag{1.1}$$

where $q_p(a)$ is the *Fermat quotient* to base a ($p \nmid a$), defined for odd primes p by

$$q_p(a) := \frac{a^{p-1}-1}{p}. \tag{1.2}$$

The congruence (1.1) was later extended by several authors in various directions, including congruences modulo higher powers of p, such as

$$\sum_{j=1}^{\frac{p-1}{2}} \frac{1}{j} \equiv -2\, q_p(2) + p\, q_p(2)^2 \pmod{p^2} \tag{1.3}$$

(due to Emma Lehmer [14]), or to different ranges, such as

$$\sum_{j=1}^{\lfloor \frac{p}{4} \rfloor} \frac{1}{j} \equiv -3\, q_p(2) \pmod{p}, \tag{1.4}$$

a special case of congruences modulo higher powers of p (see, e.g., [18]). Typically there exist explicit expressions for such congruences for sums from 1 to $\lfloor \frac{p}{2} \rfloor$, $\lfloor \frac{p}{3} \rfloor$, $\lfloor \frac{p}{4} \rfloor$, and $\lfloor \frac{p}{6} \rfloor$, which comes from the fact that these congruences are usually derived with the use of Bernoulli polynomials; see, e.g., the beginning of [14], which is perhaps the most important and influential paper on this subject.

Key words and phrases. Lehmer's congruences, Fermat quotients, Euler quotients, Bernoulli numbers, Bernoulli polynomials.

Research supported in part by the Natural Sciences and Engineering Research Council of Canada.

In the present paper we will consider extensions of a set of four congruences of Emma Lehmer [14, p. 358], one of which is

$$\sum_{j=1}^{\lfloor\frac{p}{4}\rfloor}\frac{1}{p-4j}\equiv\frac{3}{4}q_p(2)-\frac{3}{8}p\,q_p(2)^2\pmod{p^2}, \tag{1.5}$$

valid for $p>3$. This congruence immediately implies (1.4) when taken modulo p.

The main reason for the great interest all through the 20th century in sums of reciprocals and their congruences has been the close connection to the first case of Fermat's Last Theorem; see, e.g., [14, pp. 358–360] or [17], or [9] for a more recent publication.

A number of congruences of the above type were in recent years extended to composite moduli. While related congruences of a somewhat different type were obtained as early as 1906 independently by H. F. Baker and M. Lerch (see [1, p. 34] for details and references), it appears that the first analogue for composite moduli of a "Lehmer type" congruence was published by T. Cai [2] in 2002: For any odd $n>1$,

$$\sum_{\substack{j=1\\(j,n)=1}}^{\frac{n-1}{2}}\frac{1}{j}\equiv-2\,q_n(2)+n\,q_n(2)^2\pmod{n^2}, \tag{1.6}$$

where (j,n) stands for the greatest common divisor of j and n, and $q_n(a)$ is the *Euler quotient* of n with base a defined by

$$q_n(a):=\frac{a^{\varphi(n)}-1}{n} \tag{1.7}$$

for relatively prime positive integers a,n with $n>1$. These quotients were first studied by Lerch [15] in 1905; numerous further properties were obtained much later in [1] and [4]. It is clear that (1.3) is a special case of (1.6); a weaker version of (1.6) for $n=p^\alpha$ (p an odd prime) had earlier been obtained in [1].

Extensions of the four congruences of Emma Lehmer of the type (1.5) were recently obtained by Cai, Fu and Zhou [3] and Cao and Pan [4]: For any positive odd integer n with $n\not\equiv 0\pmod 3$ we have

$$\sum_{\substack{j=1\\(j,n)=1}}^{\lfloor\frac{n}{2}\rfloor}\frac{1}{n-2j}\equiv q_n(2)-\frac{1}{2}nq_n(2)^2\pmod{n^2}, \tag{1.8}$$

$$\sum_{\substack{j=1\\(j,n)=1}}^{\lfloor\frac{n}{3}\rfloor}\frac{1}{n-3j}\equiv\frac{1}{2}q_n(3)-\frac{1}{4}n\,q_n(3)^2\pmod{n^2}, \tag{1.9}$$

$$\sum_{\substack{j=1\\(j,n)=1}}^{\lfloor\frac{n}{4}\rfloor}\frac{1}{n-4j}\equiv\frac{3}{4}q_n(2)-\frac{3}{8}n\,q_n(2)^2\pmod{n^2}, \tag{1.10}$$

$$\sum_{\substack{j=1\\(j,n)=1}}^{\lfloor\frac{n}{6}\rfloor}\frac{1}{n-6j}\equiv\frac{1}{3}q_n(2)+\frac{1}{4}q_n(3)-n\left(\frac{1}{6}q_n(2)^2+\frac{1}{8}q_n(3)^2\right)\pmod{n^2}. \tag{1.11}$$

These four congruences were first obtained by Cai, Fu and Zhou [3], and independently Cao and Pan [4] proved (1.9), (1.10), and (1.11), but with fewer restrictions on n than was the case in [3]. More recently Kuzumaki and Urbanowicz [13] extended these congruences, and by extension also Emma Lehmer's congruences, to results for all sums

$$U_r(n) := \sum_{\substack{j=1\\(j,n)=1}}^{[n/r]} \frac{1}{n-rj} \pmod{n^s}, \tag{1.12}$$

for $s \in \{1,2,3\}$ and $r \mid 24$ with $n > r$ and relatively prime to r. These are related to similar generalizations of congruences of the type (1.6), recently studied by Kanemitsu, Kuzumaki, and Urbanowicz [12]. We return to these generalizations later, in Section 4

Concerning (1.9) Cao and Pan remark that it “fails when $n = 4$, 8, 14, 16, 22, 28, 32, 38, 44, 46, …”, and they further remark that (1.10) “fails when $n = 9$, 15, 27, 33, 45, 51, 69, 75, 81, 87, …”.

In the case of the congruence (1.11) it is entirely natural to restrict n to being odd and not divisible by 3 (because of the denominator on the left side), while for the other three congruences this wide restriction doesn't generally apply. Specifically — as Cao and Pan observed above — the restriction that n be odd does not apply to (1.9), the restriction that n be not divisible by 3 does not apply to (1.10), nor, for that matter, does the restriction that n be odd apply to Cai, Fu and Zhou's (1.8).

It is the purpose of this paper to investigate the congruences (1.8), (1.9) and (1.10) freed from these restrictions. Section 2 will be devoted to (1.8) and (1.10), and Section 3 to (1.9). In each case we will classify those of the originally excluded n for which the relevant congruence still holds, and give a modified correct form when it does not hold. We conclude this paper with some additional remarks in Section 4.

2. The congruences (1.8) and (1.10) in the case $3 \mid n$

In this section we will explain Cao and Pan's list of exceptions (9, 15, 27, …) for (1.10) and prove the correct congruence in this case. Furthermore, the congruence (1.8), not mentioned by Cao and Pan, can be treated in parallel with (1.10).

Theorem 1. *For odd positive integers n with $3 \mid n$ the congruences* (1.8) *and* (1.10) *hold if and only if n has a prime divisor p with $p \equiv 1 \pmod 6$. If n has no such prime divisor, then* (1.8) *and* (1.10) *hold modulo $\frac{1}{3}n^2$.*

In the proof of (1.10) by Cao and Pan [4], with the original condition $(n, 6) = 1$, the authors use the following property of Euler quotients which they state and prove as Lemma 4: If $n > 1$ and a are integers with $(n, 6a) = 1$, then

$$q_{n^2}(a) \equiv q_n(a) - \tfrac{1}{2} n\, q_n(a)^2 \pmod{n^2}. \tag{2.1}$$

For the proof of Theorem 1 we need the following variant of this congruence.

Lemma 1. *For any $\alpha \geq 1$ we have*

$$q_{3^{2\alpha}}(2) \equiv q_{3^\alpha}(2) - \tfrac{1}{2} 3^\alpha q_{3^\alpha}(2)^2 + 3^{2\alpha-1} \pmod{3^{2\alpha}}. \tag{2.2}$$

Proof. We follow the proof of Lemma 4 in [4] by using a binomial expansion, carrying one more term than in [4]:

$$\begin{aligned} a^{\varphi(n^2)}-1 &= \left(\left(a^{\varphi(n)}-1\right)+1\right)^n-1 \\ &\equiv n\left(a^{\varphi(n)}-1\right)+\binom{n}{2}\left(a^{\varphi(n)}-1\right)^2+\binom{n}{3}\left(a^{\varphi(n)}-1\right)^3 \pmod{n^4}, \end{aligned}$$

so that

$$n^2q_{n^2}(a)\equiv n^2q_n(a)-\tfrac{1}{2}n^3q_n(a)^2+\tfrac{1}{3}n^4q_n(a)^3 \pmod{n^4}. \tag{2.3}$$

If we set $a=2$ and $n=3^\alpha$, we get

$$q_{3^{2\alpha}}(2)\equiv q_{3^\alpha}(2)-\tfrac{1}{2}3^\alpha q_{3^\alpha}(2)^2+3^{2\alpha-1}q_{3^\alpha}(2)^3 \pmod{3^{2\alpha}}. \tag{2.4}$$

To complete the proof, we need to determine $q_{3^\alpha}(2) \pmod 3$. To do this, we expand

$$2^{\varphi(3^\alpha)}=2^{2\cdot 3^{\alpha-1}}=(1+3)^{3^{\alpha-1}}\equiv 1+3^{\alpha-1}\cdot 3 \pmod{3^{\alpha+1}},$$

and thus

$$q_{3^\alpha}(2)=\frac{2^{\varphi(3^\alpha)}-1}{3^\alpha}\equiv 1 \pmod 3$$

for all $\alpha\ge 1$. This, with (2.4), immediately gives (2.2). □

The next lemma is analogous to, and extends, Lemma 3 in [4].

Lemma 2. *Let n be an odd integer with $n=3^\alpha m$, where $\alpha\ge 1$ and $3\nmid m$. Then*

$$\sum_{\substack{j=1\\3\nmid j}}^{\lfloor\frac{n}{2}\rfloor}\frac{1}{n-2j}\equiv q_{3^{2\alpha}}(2)+3^{2\alpha-1} \pmod{3^{2\alpha}}, \tag{2.5}$$

$$\sum_{\substack{j=1\\3\nmid j}}^{\lfloor\frac{n}{4}\rfloor}\frac{1}{n-4j}\equiv \frac{3}{4}q_{3^{2\alpha}}(2)-3^{2\alpha-1} \pmod{3^{2\alpha}}. \tag{2.6}$$

For the proof of Lemma 2 and an equivalent lemma in the next section we require another result which is an extension of Lemma 2 in [4].

Lemma 3. *For any prime p and positive integer β we have*

$$pB_{\varphi(p^\beta)}\equiv p-1 \pmod{p^\beta}, \tag{2.7}$$

with the exception of the pair $p=2$, $\beta=2$, where we have $2B_2\equiv -1 \pmod{2^2}$.

Here B_n is the nth Bernoulli number, defined by the generating function

$$\frac{t}{e^t-1}=\sum_{n=0}^{\infty}B_n\frac{t^n}{n!} \qquad (|t|<2\pi).$$

Also required in this section and the next are the Bernoulli polynomials, defined by

$$\frac{te^{tx}}{e^t-1}=\sum_{n=0}^{\infty}B_n(x)\frac{t^n}{n!} \qquad (|t|<2\pi),$$

connected with the Bernoulli numbers by

$$B_n(x)=\sum_{k=0}^{n}\binom{n}{k}B_{n-k}x^k; \tag{2.8}$$

see, e.g., [16, Ch. 24] for further properties, or [14] for details on how the Bernoulli numbers and polynomials enter into the theory of the congruences studied here.

The congruence (2.7) was proved in [4] for $p \geq 5$ and $\beta = 2\alpha$, which was all that was needed there. However, it has already been known for some time; in fact, for $\beta = 1$ this is a variant of the von Staudt-Clausen theorem; see, e.g., [17, p. 102]. For $\beta > 1$ and $\varphi(p^\beta) > 2$, see [11, p. 158], where the author credits two papers of Carlitz of 1953 and 1960. We quote this result here since it will be needed in the next proof:

Let $n > 1$ and p any prime such that $(p-1)p^h \mid 2n$. Then

$$pB_{2n} \equiv p - 1 \pmod{p^{h+1}}. \tag{2.9}$$

Finally, the exceptional case in Lemma 3 is obtained through direct computation: We have $2B_2 = \frac{1}{3} \equiv -1 \pmod 4$. We are now ready to prove Lemma 2.

Proof of Lemma 2. We use the method of proof of Lemma 3 in [4], and let $d \in \{2, 4\}$. Using the fact that $\varphi(3^{2\alpha}) - 1 > 2\alpha$ for all $\alpha \geq 1$ and setting

$$S_n := \sum_{\substack{j=1 \\ 3\nmid j}}^{\lfloor \frac{n}{d} \rfloor} \frac{1}{n - dj}, \qquad d \in \{2, 4\}, \tag{2.10}$$

then we get, just as in [4, p. 1816],

$$\begin{aligned} S_n &\equiv \frac{d^{\varphi(3^{2\alpha})-1}}{\varphi(3^{2\alpha})} \left(B_{\varphi(3^{2\alpha})}(\tfrac{n}{d}) - B_{\varphi(3^{2\alpha})}(\tfrac{s}{d})\right) \\ &\equiv \frac{d^{\varphi(3^{2\alpha})-1}}{\varphi(3^{2\alpha})} \left(\sum_{i=0}^{\varphi(3^{2\alpha})} \binom{\varphi(3^{2\alpha})}{i} \left(\frac{n}{d}\right)^i B_{\varphi(3^{2\alpha})-i} - B_{\varphi(3^{2\alpha})}(\tfrac{s}{d}) \right) \pmod{3^{2\alpha}}, \end{aligned}$$

where s is the least nonnegative residue of n modulo d. Now in our case we need to carry along one more term from the summation above than was the case in [4]. Using the facts that $3^\alpha \mid n$ and $B_{\varphi(3^{2\alpha})-1} = 0$, as well as the von Staudt-Clausen theorem, we get from the last congruence,

$$S_n \equiv \frac{d^{\varphi(3^{2\alpha})-1}}{\varphi(3^{2\alpha})} \left(B_{\varphi(3^{2\alpha})} + C(n) - B_{\varphi(3^{2\alpha})}(\tfrac{s}{d})\right) \pmod{3^{2\alpha}}, \tag{2.11}$$

where

$$C(n) := \frac{1}{2}\varphi(3^{2\alpha})(\varphi(3^{2\alpha}) - 1) \left(\frac{3^\alpha m}{d}\right)^2 B_{\varphi(3^{2\alpha})-2}.$$

Using the fact that $\varphi(3^{2\alpha}) = 2 \cdot 3^{2\alpha-1}$, we now have

$$\frac{d^{\varphi(3^{2\alpha})-1}}{\varphi(3^{2\alpha})} C(n) = \left(\frac{1}{2} d^{2\cdot 3^{2\alpha-1}-3} (2 \cdot 3^{2\alpha-1} - 1) m^2 3B_{2(3^{2\alpha-1}-1)}\right) 3^{2\alpha-1}, \tag{2.12}$$

and we see that the term in large parentheses only needs to be evaluated modulo 3. Since $d \equiv \pm 1 \pmod 3$ and $m \equiv \pm 1 \pmod 3$, we have

$$d^{2\cdot 3^{2\alpha-1}-3} \equiv d \pmod 3, \qquad (2 \cdot 3^{2\alpha-1} - 1)m^2 \equiv 2 \pmod 3,$$

and (2.9) gives

$$3B_{2(3^{2\alpha-1}-1)} \equiv 2 \pmod 3.$$

Hence the right-hand side of (2.12) is congruent to $-d3^{2\alpha-1} \pmod{3^{2\alpha}}$, and with (2.11) we get

$$S_n \equiv \frac{d^{\varphi(3^{2\alpha})-1}}{\varphi(3^{2\alpha})}\left(B_{\varphi(3^{2\alpha})} - B_{\varphi(3^{2\alpha})}(\tfrac{s}{d})\right) - d3^{2\alpha-1} \pmod{3^{2\alpha}}. \tag{2.13}$$

In the case $d = 4$ the main term on the right-hand side of (2.13) can be evaluated, just as in [4], to $\frac{3}{4}q_{3^{2\alpha}}(2) \pmod{3^{2\alpha}}$, which immediately gives (2.6).

When $d = 2$, we have $s = 1$ and we use the well-known fact that for even $\nu \geq 2$ we have $B_\nu(\frac{1}{2}) = (2^{1-\nu} - 1)B_\nu$ (see, e.g., [14, p. 352] or [16, Ch. 24]), so that

$$B_\nu - B_\nu(\tfrac{1}{2}) = 2\left(1 - 2^{-\nu}\right)B_\nu.$$

Using this and (2.7) with $\beta = 2\alpha$, we get with (2.13) for $d = 2$,

$$S_n \equiv \frac{2^{\varphi(3^{2\alpha})} - 1}{\varphi(3^{2\alpha})} \cdot \frac{2}{3} - 2 \cdot 3^{2\alpha-1} \pmod{3^{2\alpha}}.$$

Finally, the fact that $\varphi(3^{2\alpha}) = 2 \cdot 3^{2\alpha-1}$ and the definition (1.7) lead to (2.5), which completes the proof of Lemma 2. $\square$

For the sake of completeness in the case of the sum on the left of (2.5), which was not covered in [4], we note that the proof of Lemma 2 can be adapted to give the following congruence.

Lemma 4. *Let $p \geq 5$ be a prime and n be an odd integer with $n = p^\alpha m$, where $\alpha \geq 1$ and $p \nmid m$. Then*

$$\sum_{\substack{j=1 \\ p\nmid j}}^{\lfloor \frac{n}{2} \rfloor} \frac{1}{n-2j} \equiv q_{p^{2\alpha}}(2) \pmod{p^{2\alpha}}. \tag{2.14}$$

The proof of this lemma is almost identical with that of (2.5), with the exception of the fact that for $p \geq 5$ we have $C(n) \equiv 0 \pmod{p^{2\alpha}}$ since by the von Staudt-Clausen theorem p does not divide the denominator of $B_{\varphi(p^{2\alpha})-2}$.

We are now ready to prove Theorem 1. Following the beginning of the proof of Theorem 1 in [4], which uses an inclusion/exclusion argument, we first get with (2.5) and (2.2),

$$\begin{aligned}\sum_{\substack{j=1 \\ (j,n)=1}}^{\lfloor \frac{n}{2} \rfloor} \frac{1}{n-2j} &\equiv \frac{\varphi(m)}{m}\left(q_{3^{2\alpha}}(2) + 3^{2\alpha-1}\right) \\ &\equiv \frac{\varphi(m)}{m}\left(q_{3^\alpha}(2) - \tfrac{1}{2}3^\alpha q_{3^\alpha}(2)^2 + 2 \cdot 3^{2\alpha-1}\right) \pmod{3^{2\alpha}}.\end{aligned}$$

Now by Lemma 5 of [4], which holds also for $p = 3$, we have

$$\frac{\varphi(m)}{m}\left(q_{3^\alpha}(2) - \tfrac{1}{2}3^\alpha q_{3^\alpha}(2)^2\right) \equiv q_n(2) - \frac{1}{2}nq_n(2)^2 \pmod{3^{2\alpha}}. \tag{2.15}$$

This and the previous congruence now give

$$\sum_{\substack{j=1 \\ (j,n)=1}}^{\lfloor \frac{n}{2} \rfloor} \frac{1}{n-2j} \equiv q_n(2) - \frac{1}{2}nq_n(2)^2 - \frac{\varphi(m)}{m}3^{2\alpha-1} \pmod{3^{2\alpha}}, \tag{2.16}$$

and similarly, for primes $p \geq 5$ we get with (2.14) and (2.1),

$$\sum_{\substack{j=1 \\ (j,n)=1}}^{\lfloor \frac{n}{2} \rfloor} \frac{1}{n-2j} \equiv q_n(2) - \frac{1}{2} n q_n(2)^2 \pmod{p^{2\alpha}}. \tag{2.17}$$

We now turn to the sum in (1.10). In a similar way as before, using again the argument in [4], followed by (2.6) and (2.2), we get

$$\begin{aligned}\sum_{\substack{j=1 \\ (j,n)=1}}^{\lfloor \frac{n}{4} \rfloor} \frac{1}{n-4j} &\equiv \frac{\varphi(m)}{m} \left(\tfrac{3}{4} q_{3^{2\alpha}}(2) - 3^{2\alpha-1}\right) \\ &\equiv \frac{\varphi(m)}{m} \left(\tfrac{3}{4} q_{3^\alpha}(2) - \tfrac{3}{8} 3^\alpha q_{3^\alpha}(2)^2 - \tfrac{1}{4} 3^{2\alpha-1}\right) \pmod{3^{2\alpha}}.\end{aligned}$$

Using (2.15) again, we obtain

$$\sum_{\substack{j=1 \\ (j,n)=1}}^{\lfloor \frac{n}{4} \rfloor} \frac{1}{n-4j} \equiv \tfrac{3}{4} q_n(2) - \frac{3}{8} n q_n(2)^2 - \tfrac{1}{4} \cdot \frac{\varphi(m)}{m} 3^{2\alpha-1} \pmod{3^{2\alpha}}. \tag{2.18}$$

To conclude the proof of Theorem 1, we note that $3 \mid \varphi(m)$ if and only if m has a prime divisor $p \equiv 1 \pmod 6$. In this case the last term on the right of both (2.16) and (2.18) vanishes. Then (2.16) and (2.17) together with the Chinese Remainder Theorem give the first statement of Theorem 1 for (1.8). Similarly, (2.18) and the corresponding congruences modulo $p^{2\alpha}$ ($p \geq 5$), obtained in [4], give the first statement of Theorem 1 for (1.10). Finally, if m has no prime divisor $p \equiv 1 \pmod 6$, then the last terms in (2.16) and (2.18) vanish only modulo $p^{2\alpha-1}$. The Chinese Remainder Theorem then gives the second part of Theorem 1. The proof is now complete.

3. The congruence (1.9) when n is even

In this section we will explain Cao and Pan's list of exceptions (9, 15, 27, ...) for (1.9) and prove the correct congruence in this case. Specifically we will prove a criterion for when (1.9) holds in the cases $n \equiv \pm 2 \pmod 6$, and give modified congruences for the cases where (1.9) does not hold. The main result of this section is as follows.

Theorem 2. *For positive integers $n \equiv \pm 2 \pmod 6$ the congruence (1.9) holds if and only if n has a prime divisor p with $p \equiv 1 \pmod 4$ or two distinct odd prime divisors. If this condition fails, then (1.9) holds*

(a) *modulo $n/2$ when $n = 2^\alpha q^\beta$ for a prime $q \equiv 3 \pmod 4$ and $\alpha, \beta \geq 1$;*
(b) *modulo $n/4$ when $n = 2^\alpha$, $\alpha \geq 2$.*

To prove this result, we once again follow the development in [4], as we did in the previous section. Our goal is to use the Chinese Remainder Theorem with an additional congruence modulo a power of 2. We begin with a crucial lemma which is analogous to Lemma 2 above and extends Lemma 3 in [4].

Lemma 5. *Let n be an integer with $n = 2^\alpha m$, $(m, 6) = 1$. Then for $\alpha \geq 2$ we have*

$$\sum_{\substack{j=1\\ 2\nmid j}}^{\lfloor \frac{n}{3} \rfloor} \frac{1}{n-3j} \equiv \frac{1}{2} q_{2^{2\alpha}}(3) + 2^{2\alpha-2} \pmod{2^{2\alpha}}, \tag{3.1}$$

while for $\alpha = 1$ there is a "$-$" instead of a "$+$" on the right-hand side.

Before continuing we remark that in spite of the factors $\frac{1}{2}$ and $\frac{1}{4}$ in (1.9) and the factor $\frac{1}{2}$ in (3.1), the congruences make sense due to the following fact.

Lemma 6. *For any odd integer b and $\alpha \geq 2$, the Euler quotient $q_{2^\alpha}(b)$ is even.*

Proof. We apply Proposition 4.1(a) in [1], namely

$$q_{2^{\alpha+1}}(b) = q_{2^\alpha}(b) + 2^{\alpha-1} q_{2^\alpha}(b)^2, \tag{3.2}$$

and use induction on α. By the definition (1.7) we have

$$q_{2^2}(b) = \frac{1}{4}(b^2 - 1) = \frac{b-1}{2} \cdot \frac{b+1}{2},$$

which is always even. Next, from (3.2) it is clear that, when $\alpha \geq 2$, $q_{2^{\alpha+1}}(b)$ is even when $q_{2^\alpha}(b)$ is. This completes the proof by induction. □

By slightly modifying the proof of this lemma we could also show that, if $\alpha \geq 2$ and $b \equiv \pm 3 \pmod 8$, then $q_{2^\alpha}(b) \equiv 2 \pmod 4$. This could easily be extended to other congruences modulo higher powers of two. However, this would lead too far in this setting; here we are only interested in knowing that $q_{2^\alpha}(3)$ is even for $\alpha \geq 2$ and, incidentally, $q_2(3) = 1$.

Proof of Lemma 5. We follow the method of proof of Lemma 2 above and Lemma 3 in [4], assuming now that $n = 2^\alpha m$, with $(m, 6) = 1$ and (for now) $\alpha \geq 2$. Then $\varphi(2^{2\alpha}) - 1 > 2\alpha$, and just as in [4] we obtain, with T_n the sum on the left of (3.1),

$$T_n \equiv \frac{3^{2^{2\alpha-1}-1}}{2^{2\alpha-1}} \left(\sum_{i=0}^{2^{2\alpha-1}} \binom{2^{2\alpha-1}}{i} \left(\frac{n}{3}\right)^i B_{2^{2\alpha-1}-i} - B_{2^{2\alpha-1}}(\tfrac{s}{3}) \right) \pmod{2^{2\alpha}} \tag{3.3}$$

where s is the least nonnegative residue of n modulo 3, so $s = 1$ or $s = 2$. As we did in the proof of Lemma 2, we need to carry along one more term from the summation on the right of (3.3) than was the case in [4]. Using the facts that $2^\alpha \mid n$ and $B_{2^{2\alpha-1}-1} = 0$, as well as the von Staudt-Clausen theorem, we get from (3.3),

$$T_n \equiv \frac{3^{2^{2\alpha-1}-1}}{2^{2\alpha-1}} \left(B_{2^{2\alpha-1}} + D(n) - B_{2^{2\alpha-1}}(\tfrac{s}{3}) \right) \pmod{2^{2\alpha}}, \tag{3.4}$$

where

$$D(n) := \frac{2^{2\alpha-1}(2^{2\alpha-1}-1)}{2} \left(\frac{2^\alpha m}{3}\right)^2 B_{2^{2\alpha-1}-2}.$$

Now we consider

$$\frac{3^{2^{2\alpha-1}-1}}{2^{2\alpha-1}} D(n) = \left(3^{2^{2\alpha-1}-3} \left(2^{2\alpha-1}\right) m^2 2 B_{2^{2\alpha-1}-2} \right) 2^{2\alpha-2} \tag{3.5}$$

and we see that the part in large parentheses only needs to be evaluated modulo 4. Now clearly, since m is odd and $3 \equiv -1 \pmod 4$, we have with $\alpha \geq 2$,

$$3^{2^{2\alpha-1}-3} \equiv -1 \pmod 4, \qquad \left(2^{2\alpha-1}\right) m^2 \equiv -1 \pmod 4,$$

and (2.9) gives

$$2B_{2^{2\alpha-1}-2} \equiv 1 \pmod{4}.$$

So, altogether, with (3.5) and (3.4),

$$T_n \equiv \frac{3^{2^{2\alpha-1}-1}}{2^{2\alpha-1}} \left(B_{2^{2\alpha-1}} - B_{2^{2\alpha-1}}(\tfrac{s}{3})\right) + 2^{2\alpha-2} \pmod{2^{2\alpha}}. \tag{3.6}$$

Now the first summand on the right evaluates exactly as in [4], and we obtain

$$T_n \equiv \frac{3^{2^{2\alpha-1}}-1}{2^{2\alpha}} B_{2^{2\alpha-1}} + 2^{2\alpha-2} \pmod{2^{2\alpha}}, \tag{3.7}$$

and finally with Lemma 3 and the definition (1.7) of the Euler quotient we get (3.1) for $\alpha \geq 2$.

To deal with the case $\alpha = 1$, we first evaluate the left-hand side of (3.1), namely $T_n \pmod 4$. Since $n \equiv 2 \pmod 4$ and j has to be odd, say $j = 2k-1$, we have

$$\frac{1}{n-3j} \equiv \frac{1}{2+(2k-1)} = \frac{1}{1+2k} \equiv 1-2k \pmod{4}. \tag{3.8}$$

We now count the number of terms in the sum T_n. Since $n \equiv \pm 2 \pmod 6$ and $n \equiv 2 \pmod 4$, we have $n \equiv \pm 2 \pmod{12}$, say $n = 12\nu \pm 2$. But then $\lfloor \frac{n}{3} \rfloor = 4\nu$ or $4\nu - 1$, and in either case the number of odd integers from 1 to $\lfloor \frac{n}{3} \rfloor$ is even. Therefore (3.8) gives

$$T_n \equiv -1+1-1+\cdots-1+1 = 0 \pmod{4}.$$

On the other hand, for $\alpha = 1$ we have

$$\tfrac{1}{2}q_4(3) - 1 = \frac{3^2-1}{2\cdot 4} - 1 = 0,$$

Having used the exceptional sign on the right of (3.1). This verifies (3.1) for $\alpha = 1$, and the proof of Lemma 5 is complete. □

Before proving Theorem 2, we remark that Lemma 4 in [4] also holds for even n with $3 \nmid n$, and Lemma 5 holds for $p = 2$. Now, proceeding exactly as in the previous section and in the proof of Theorem 1 in [4], we get with Lemma 5 above, recalling that $n = 2^\alpha m$,

$$\begin{aligned}\sum_{\substack{j=1\\(j,n)=1}}^{\lfloor \frac{n}{3} \rfloor} \frac{1}{n-3j} &\equiv \frac{\varphi(m)}{m}\left(\frac{1}{2}q_{2^{2\alpha}}(3) + 2^{2\alpha-2}\right)\\ &\equiv \frac{1}{2}q_n(3) - \frac{1}{4}n\,q_n(3)^2 + \frac{\varphi(m)}{m}2^{2\alpha-2} \pmod{2^{2\alpha}}.\end{aligned}$$

Here we have used Lemmas 4 and 5 from [4] for the last congruence. To complete the proof of Theorem 2, we first note that $\varphi(m) \equiv 0 \pmod 4$ if m has a prime factor $p \equiv 1 \pmod 4$, or m has at least two distinct odd prime factors. In these cases we immediately get

$$\sum_{\substack{j=1\\(j,n)=1}}^{\lfloor \frac{n}{3} \rfloor} \frac{1}{n-3j} \equiv \frac{1}{2}q_n(3) - \frac{1}{4}n\,q_n(3)^2 \pmod{2^{2\alpha}}. \tag{3.9}$$

If n is of the form $n = 2^\alpha q^\beta$ with a prime $q \equiv 3 \pmod 4$, then $\varphi(m) \equiv 2 \pmod 4$, and (3.9) holds only modulo $2^{2\alpha-1}$. Finally, if n is a power of 2 then $m = 1$, and

(3.9) holds only modulo $2^{2\alpha-2}$. The statement of Theorem 2 is then obtained by the Chinese Remainder Theorem, again as in the corresponding proof in [4].

4. Further remarks

1. The congruences (1.6), (1.8) and Theorem 1 can be combined to give a different (but related) kind of congruence. To set the stage for the following corollary, we note that as a special case of the congruence (18) in [14] we have for primes $p \geq 5$,

$$\sum_{j=1}^{\frac{p-1}{2}} \frac{1}{j^2} \equiv 0 \pmod{p}.$$

We can now extend this to arbitrary odd moduli.

Corollary 1. *For any odd integer $n \geq 3$ we have*

$$\sum_{\substack{j=1 \\ (j,n)=1}}^{\frac{n-1}{2}} \frac{1}{j^2} \equiv 0 \pmod{n}, \tag{4.1}$$

unless $3 \mid n$ and n does not have a prime divisor $p \equiv 1 \pmod 6$, in which case (4.1) holds modulo $n/3$.

Proof. Following the example of a congruence modulo p^2 in [14, p. 359], we expand, for odd positive n and $(j,n)=1$,

$$\frac{1}{n-2j} = \frac{-1}{2j}\left(\frac{1}{1-\frac{n}{2j}}\right) \equiv \frac{-1}{2j}\left(1+\frac{n}{2j}\right) = \frac{-1}{2j} - \frac{n}{4j^2} \pmod{n^2},$$

and thus

$$\frac{n}{j^2} \equiv -\frac{2}{j} - \frac{4}{n-2j} \pmod{n^2}.$$

Therefore

$$n \sum_{\substack{j=1 \\ (j,n)=1}}^{\lfloor n/2 \rfloor} \frac{1}{j^2} \equiv -2 \sum_{\substack{j=1 \\ (j,n)=1}}^{\lfloor n/2 \rfloor} \frac{1}{j} - 4 \sum_{\substack{j=1 \\ (j,n)=1}}^{\lfloor n/2 \rfloor} \frac{1}{n-2j} \equiv 0 \pmod{n^2},$$

unless $3 \mid n$ and n does not have a prime divisor $p \equiv 1 \pmod 6$, in which case this last congruence holds modulo $n^2/3$, a congruence which follows from (1.6) and (1.8) with Theorem 1. If we divide both sides of the congruence above by n, we get the statement of the corollary. □

A congruence of the type (4.1), but with the summation from 1 to $\lfloor n/4 \rfloor$, is the main object of [7].

2. This paper originated from the need for an extension of the congruence (1.4) in some unrelated work of the authors. To be more specific, in our recent paper [6] on the multiplicative orders of certain factorial-like products, the congruence (1.4) plays an important role. Similarly, in work in progress extending the results from [6], an analogue of (1.4) modulo arbitrary odd integers is required. Specializing the congruence (1.10), as proved in [3] and [4], to a congruence modulo n, we do indeed get the desired congruence

$$\sum_{\substack{j=1\\(j,n)=1}}^{\lfloor\frac{n}{4}\rfloor}\frac{1}{j}\equiv -3\,q_n(2)\pmod{n},$$

but with the restriction $3\nmid n$. Theorem 1 then extends this further to all odd moduli n.

3. Another application of congruences for sums of reciprocals is to the study of certain binomial coefficients modulo powers of primes. This connection is made explicit in Emma Lehmer's paper [14, p. 360]. The most important congruences of the type (1.1), (1.3), (1.4) are catalogued, with references or proofs, in Lemmas 1–4 in [5] where they are required in the proofs of extensions of the binomial coefficient theorems of Gauss and Jacobi.

4. Returning to the sums in (1.12), we note that the main result in [13] is also restricted to odd n not divisible by 3. Of the three new cases $r=8,12$, and 24, in the case $r=8$ the corresponding sum would also make sense when $3\mid n$. We therefore state this case explicitly, as a fifth congruence in the sequence (1.8)–(1.11):

$$\begin{aligned}\sum_{\substack{j=1\\(j,n)=1}}^{\lfloor\frac{n}{8}\rfloor}\frac{1}{n-8j}\equiv\frac{1}{2}q_n(2)-\frac{1}{4}n\,q_n(2)^2-\frac{1}{4n\varphi(n)}(-1)^{(n^2-1)/8}B_{n\varphi(n),\chi_8}\\ \times\prod_{p\mid n}\left(1-(-1)^{(p^2-1)/8}p^{n\varphi(n)-1}\right)\pmod{n^2},\end{aligned}\tag{4.2}$$

where the *generalized Bernoulli numbers* $B_{m,\chi}$ are defined as follows. For a Dirichlet character χ modulo M, the numbers $B_{m,\chi}$ are given by the generating function

$$\sum_{a=1}^{M}\frac{\chi(a)te^{at}}{e^{Mt}-1}=\sum_{m=0}^{\infty}B_{m,\chi}\frac{t^m}{m!}.\tag{4.3}$$

This and numerous other properties and references can be found, e.g., in [8] or [20]. For properties that were used in [12] and [13] to obtain congruences such as (4.2), see [19]. The character χ_8 in (4.2) is the (unique) primitive quadratic character modulo 8, i.e., it is given by $\chi_8(a)=1$ for $a\equiv\pm1\pmod{8}$, $\chi_8(a)=-1$ for $a\equiv\pm3\pmod{8}$, and $\chi_8(a)=0$ for all even integers a. The corresponding generalized Bernoulli numbers can then be computed using the generating function (4.3), or the following special case of a well-known recurrence relation, which is computationally more efficient:

$$B_{2n,\chi_8}=-\sum_{j=1}^{n-1}\binom{2n}{2j-1}\frac{B_{2j,\chi_8}}{2j}64^{n-j}+\frac{1}{8}\left(1-9^n-25^n+49^n\right)\tag{4.4}$$

(for $n\geq1$, where the empty sum is considered to be 0). The first few values are shown in Table 1.

m	2	4	6	8	10	12
B_{m,χ_8}	2	-44	2 166	$-196\,888$	28 730 410	$-6\,148\,123\,332$

Table 1: The first six nonzero generalized Bernoulli numbers B_{m,χ_8}.

Since χ_8 is a nontrivial even character, we have $B_{m,\chi_8} = 0$ for all odd m and for $m = 0$. Other standard properties explain the fact that nonzero generalized Bernoulli numbers have alternating signs, and that we have asymptotically

$$|B_{n,\chi_8}| \sim \frac{1}{2\sqrt{\pi n}} \left(\frac{4n}{\pi e}\right)^n \quad \text{as } n \to \infty \quad (n \text{ even}). \tag{4.5}$$

This explains the very rapid growth of the generalized Bernoulli numbers, as observed in Table 1.

We computed both sides of (4.2) modulo n^2 for those $n < 200$ for which the congruence is still meaningful, but which are not covered by the main theorem in [13], namely $n \equiv 3 \pmod 6$. Surprisingly, it turns out that, in contrast to (1.8)–(1.10), the congruence (4.2) also holds in the exceptional cases, at least for $n < 200$. For the relevant $n < 200$ the largest subscript of the generalized Bernoulli number in (4.2) is $183\varphi(183) = 21960$; this and the relations (4.5) and (4.4) indicate that evaluating the right-hand side of (4.2) up to this limit is computationally very intensive.

A further investigation of this case would go beyond the scope of this paper.

Acknowledgments

We would like to thank a referee for bringing the papers [12] and [13] to our attention.

References

[1] T. Agoh, K. Dilcher, and L. Skula, *Fermat quotients for composite moduli*, J. Number Theory **66** (1997), no. 1, 29–50.

[2] Cai, Tianxin, *A congruence involving the quotients of Euler and its applications (I)*, Acta Arith. **103** (2002), no. 4, 313–320.

[3] Cai, T. X., Fu, X. D., and Zhou, X., *A congruence involving the quotients of Euler and its applications (II)*, Acta Arith. **130** (2007), no. 3, 203–214.

[4] Cao, Hui-Qin and Pan, Hao, *Note on some congruences of Lehmer*, J. Number Theory **129** (2009), no. 8, 1813–1819.

[5] J. B. Cosgrave and K. Dilcher, *Mod p^3 analogues of theorems of Gauss and Jacobi on binomial coefficients*, Acta Arith. **142** (2010), 103–118.

[6] J. B. Cosgrave and K. Dilcher, *The multiplicative orders of certain Gauss factorials*, Int. J. Number Theory **7** (2011), no. 1, 145–171.

[7] J. B. Cosgrave and K. Dilcher, *On a congruence of Emma Lehmer related to Euler numbers*, preprint, 2012.

[8] K. Dilcher, *Zeros of Bernoulli, generalized Bernoulli and Euler polynomials*, Memoirs Amer. Math. Soc., **73** (1988), no. 386.

[9] K. Dilcher and L. Skula, *A new criterion for the first case of Fermat's last theorem*, Math. Comp. **64** (1995), 363–392.

[10] G. Eisenstein, *Eine neue Gattung zahlentheoretischer Funktionen welche von zwei Elementen abhaengen und durch gewisse lineare Funktional-Gleichungen definiert werden*. In: Bericht ueber die zur Bekanntmachung geeigneten Verhandlungen der Koenigl. Preuss. Akademie der Wissenschaften zu Berlin, 1850, pp. 36–42. *Mathematische Werke* (2nd ed.), Gotthold Eisenstein, Band II, Chelsea, New York, 1989, pp. 705–711.

[11] F. T. Howard, *Applications of a recurrence for the Bernoulli numbers*, J. Number Theory **52** (1995), no. 1, 157–172.

[12] S. Kanemitsu, T. Kuzumaki, and J. Urbanowicz, *On congruences for the sums $\sum_{i=1}^{[n/r]} \frac{\chi_n(i)}{i^k}$ of E. Lehmer's type*, IM PAN Preprint No. 735, 2012. `http://www.impan.pl/Preprints/p735.pdf`.

[13] T. Kuzumaki and J. Urbanowicz, *On congruences for the sums $\sum_{i=1}^{[n/r]} \frac{\chi_n(i)}{n-ri}$ of E. Lehmer's type*, IM PAN Preprint No. 736, 2012. `http://www.impan.pl/Preprints/p736.pdf`.

[14] E. Lehmer, *On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson*, Ann. of Math. Oxford Ser. **39** (1938), 350–360.
[15] M. Lerch, *Zur Theorie des Fermatschen Quotienten* $(a^{p-1}-1)/p = q(a)$, Math. Annalen **60** (1905), 471–490.
[16] F. W. J. Olver et al. (eds.), *NIST Handbook of Mathematical Functions*, Cambridge Univ. Press, New York, 2010.
[17] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*. Springer-Verlag, New York, 1979.
[18] Sun, Zhi-Hong, *Congruences involving Bernoulli and Euler numbers*. J. Number Theory **128** (2008), 280–312.
[19] J. Szmidt, J. Urbanowicz, and D. Zagier, *Congruences among generalized Bernoulli numbers*, Acta Arith. **71** (1995), 273–278.
[20] J. Urbanowicz and K. S. Williams, Congruences for L-functions, Kluwer Academic Publishers, Dordrecht/Boston/London, 2000.

79 Rowanbyrn, Blackrock, County Dublin, Ireland
E-mail address: jbcosgrave@gmail.com

Department of Mathematics and Statistics, Dalhousie University, Halifax, Nova Scotia, B3H 3J5, Canada
E-mail address: dilcher@mathstat.dal.ca