ACTA ARITHMETICA
161.1 (2013)

On a congruence of Emma Lehmer related to Euler numbers

by

John B. Cosgrave (Dublin) and Karl Dilcher (Halifax)

1. Introduction. Congruences for sums of reciprocals modulo a prime or prime power have been of considerable interest throughout the 20th century, mainly because of their close connection to the first case of Fermat's Last Theorem; see, e.g., [17, pp. 155 ff.] or [11]. Even though this motivation is now only of historical interest, such congruences have continued to attract attention, and have recently been extended to composite moduli; see [1], [2] or [3]. A brief historical overview is given in [7], where some of the earlier results, relating sums of reciprocals with Fermat and Euler quotients, have been further extended.

All these papers are based on methods and results of Emma Lehmer, whose 1938 paper [11] remains the most important and influential paper on this topic, although it built on earlier work of Glaisher, Lerch and others. One of the more remarkable congruences in Lehmer's paper [11] is the following one for sums of reciprocals of squares:

$$\sum_{j=1}^{\lfloor p/4\rfloor} \frac{1}{j^2} \equiv (-1)^{(p-1)/2} 4E_{p-3} \pmod{p}, \tag{1.1}$$

valid for all primes $p \geq 5$, where E_n is the nth Euler number, which can be defined by the exponential generating function

$$\frac{2}{e^t + e^{-t}} = \sum_{n=0}^{\infty} \frac{E_n}{n!} t^n \quad (|t| < \pi). \tag{1.2}$$

Recently Cai, Fu and Zhou [2] extended (1.1) to prime powers by proving the following congruence for odd primes p and integers $\alpha \geq 1$:

$$\sum_{\substack{j=1 \\ p\nmid j}}^{\lfloor p^\alpha/4\rfloor} \frac{1}{j^2} \equiv (-1)^{(p^\alpha-1)/2} 4E_{\varphi(p^\alpha)-2} \begin{cases} \pmod{p^\alpha} & \text{when } p \geq 5, \\ \pmod{3^{\alpha-1}} & \text{when } p = 3. \end{cases} \tag{1.3}$$

2010 *Mathematics Subject Classification*: Primary 11A07; Secondary 11B68.
Key words and phrases: sums of reciprocals, congruences, Euler numbers.

DOI: 10.4064/aa161-1-4

It is the main purpose of this paper to extend (1.3) to arbitrary moduli n. We begin with odd moduli in Section 3, after we prove some auxiliary results on Euler numbers in Section 2. Our main result in Section 3 relies on a certain arithmetic function which we study further in Section 4, along with some computational results. In Section 5 we consider the question of the extended sum vanishing modulo n (or modulo $n/3$ when $3 \mid n$), and give a complete characterization for odd n. In Section 6 we deal with even n; finally, Section 7 contains an application to a sum of reciprocals modulo n^2.

2. Congruences for Euler numbers. The Euler numbers, defined in (1.2), have also been studied extensively because of their connection with Fermat's Last Theorem and the arithmetic of cyclotomic fields; see, e.g., [17, p. 202] or [9]. The Euler numbers are integers, and it is immediate from (1.2) that $E_{2k+1} = 0$ for all $k \geq 0$ since the generating function is even. Also, it can be shown that even-index Euler numbers have alternating signs, and the first few numbers are $1, -1, 5, -61, 1385, -50521$.

One of the more remarkable properties of the Euler numbers is the Kummer congruence, which in its simplest form can be written as

$$E_{2k+(p-1)} \equiv E_{2k} \pmod{p} \tag{2.1}$$

for integers $k \geq 1$ and primes $p \geq 3$; see, e.g., [15, Ch. 24]. Numerous generalizations are known; see, e.g., [4], [5], [6], [19], or [20]. In particular, the congruence (2.1) has been extended to prime power moduli (see [10, p. 226] or [6]):

$$E_{\varphi(p^\alpha)+2k} \equiv (1 - (-1)^{(p-1)/2} p^{2k}) E_{2k} \pmod{p^\alpha}. \tag{2.2}$$

It is the purpose of this section to extend (2.1) to an arbitrary odd modulus. While (2.2) could easily be used for this purpose, we choose a different approach which we consider interesting. We begin with the congruence

$$E_m \equiv \sum_{j=0}^{n-1} (-1)^j (2j+1)^m \pmod{n}, \tag{2.3}$$

valid for arbitrary integers $m \geq 1$ and odd integers $n \geq 1$. This congruence can be found in [10, Lemma 2.5], but similar congruences have been known for a long time; see, e.g., [4, p. 36].

We also require the following extension of Euler's generalization of Fermat's Little Theorem. Generalizing the concept of a square free integer, we say that an integer n is $(k+1)$*th-power free* if no prime power higher than the kth power divides n.

LEMMA 1. *Let n and k be positive integers. Then*

$$a^{\varphi(n)+k} \equiv a^k \pmod{n} \quad \text{for all } a \in \mathbb{Z} \tag{2.4}$$

if and only if n is a $(k+1)$th-power free integer.

Proof. Let $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, with $p_1, \ldots, p_r$ distinct primes and $1 \le \alpha_j \le k$ for $j = 1, \ldots, r$. Now fix one such j. By Euler's theorem we have

$$a^{\varphi(p_j^{\alpha_j})} \equiv 1 \pmod{p_j^{\alpha_j}} \quad \text{if } p_j \nmid a.$$

Raising both sides to the power $\varphi(p_1^{\alpha_1}) \cdots \varphi(p_r^{\alpha_r})$ (but without $\varphi(p_j^{\alpha_j})$), we get

$$a^{\varphi(p_1^{\alpha_1}) \cdots \varphi(p_r^{\alpha_r})} \equiv 1 \pmod{p_j^{\alpha_j}}. \tag{2.5}$$

Now, if we multiply both sides of (2.5) by a^k then, recalling that $\alpha_j \le k$, we see that the congruence

$$a^{\varphi(p_1^{\alpha_1} \cdots p_r^{\alpha_r})+k} \equiv a^k \pmod{p_j^{\alpha_j}} \tag{2.6}$$

holds for *all* integers a. But j is arbitrary, and thus by the Chinese Remainder Theorem (or in this case simply by the definition of the congruences) we get

$$a^{\varphi(p_1^{\alpha_1} \cdots p_r^{\alpha_r})+k} \equiv a^k \pmod{p_1^{\alpha_1} \cdots p_r^{\alpha_r}},$$

which is (2.4). Conversely, suppose that $\alpha_j > k$ for some j. Then for $a = p_j$ the exponent of a on the left of (2.4) is some $K > k$, so that $p_j^{\alpha_j} \mid p_j^K - p_j^k$, which is a contradiction. ∎

The desired extension of the Kummer congruence (2.1) now follows immediately from (2.3) and Lemma 1:

LEMMA 2. *Let $k \ge 1$ be an integer and $n \ge 1$ an odd $(k+1)$th-power free integer. Then*

$$E_{\varphi(n)+k} \equiv E_k \pmod{n}. \tag{2.7}$$

Proof. Using (2.3) and Lemma 1, we have

$$\begin{aligned} E_{\varphi(n)+k} &\equiv \sum_{j=0}^{n-1} (-1)^j (2j+1)^{\varphi(n)+k} \pmod{n} \\ &\equiv \sum_{j=0}^{n-1} (-1)^j (2j+1)^k \equiv E_k \pmod{n}, \end{aligned}$$

which was to be shown. ∎

3. The main result. In this section we are going to extend the generalization (1.3) of Lehmer's congruence (1.1) to arbitrary odd moduli n. For the statement of our result we require the following expression that depends on the prime factorization of n.

Given the odd integer n, write it in its prime power decomposition

$$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}. \tag{3.1}$$

Then define the integer $A(n)$ by $A(n) = 1$ when $r = 1$, and for $r \geq 2$,

$$A(n) := \sum_{j=1}^{r} \prod_{\substack{i=1 \\ i \neq j}}^{r} p_i^{\alpha_i \varphi(p_j^{\alpha_j})} \left(1 - \frac{(-1)^{(p_i-1)/2}}{p_i^2}\right). \tag{3.2}$$

With this expression we have the following result for the sum

$$S_4(n) := \sum_{\substack{j=1 \\ (j,n)=1}}^{\lfloor n/4 \rfloor} \frac{1}{j^2}. \tag{3.3}$$

THEOREM 1. *Let n be an odd positive integer. Then*

(3.4)

$$S_4(n) \equiv \begin{cases} (-1)^{(n-1)/2} 4A(n) E_{\varphi(n)-2} \pmod{n} & \text{when } 3 \nmid n, \\ (-1)^{(n-1)/2} 4A(n) E_{\varphi(n)-2} \pmod{n/3} & \text{when } n \equiv 0 \pmod 9, \\ (-1)^{(n-1)/2} \frac{40}{9} A(\frac{n}{3}) E_{\varphi(n)-2} \pmod{n/3} & \text{when } n \equiv \pm 3 \pmod 9. \end{cases}$$

To simplify notation, we use the following convention for the remainder of this paper:

$$A \pmod{\overline{p^\alpha}} \text{ means } \begin{cases} A \pmod{p^\alpha} & \text{when } p \geq 5, \\ A \pmod{3^{\alpha-1}} & \text{when } p = 3. \end{cases} \tag{3.5}$$

The main ingredient in the proof of Theorem 1 is the following lemma.

LEMMA 3. *Let n be an odd positive integer and p a prime divisor of n. If p^α is the highest power of p dividing n, then*

$$\sum_{\substack{j=1 \\ p \nmid j}}^{\lfloor n/4 \rfloor} \frac{1}{j^2} \equiv (-1)^{(n-1)/2} 4 E_{\varphi(n)-2} \pmod{\overline{p^\alpha}}. \tag{3.6}$$

The idea of proof of Lemma 3 is as follows. We write $n = mp^\alpha$, $p \nmid m$, and divide $\lfloor n/4 \rfloor$ into multiples of p^α and a (positive or negative) remainder $\lfloor p^\alpha/4 \rfloor$. To evaluate the corresponding sums, we use the congruence (1.3) of Cai et al. [2] and the following lemma due to Cai [1, Lemma 1].

LEMMA 4. *Let $n \geq 2$ be an integer. Then*

$$S_1(n) := \sum_{\substack{j=1 \\ (j,n)=1}}^{n-1} \frac{1}{j^2} \equiv 0 \begin{cases} \pmod n & \text{when } 3 \nmid n,\ n \neq 2^a, \\ \pmod{n/3} & \text{when } 3 \mid n, \\ \pmod{n/2} & \text{when } n = 2^a. \end{cases} \tag{3.7}$$

REMARK. In passing we note that $S_1(n) \equiv 0 \pmod n$ when $3 \mid n$ and n has a prime divisor $p \equiv 1 \pmod 6$ (see, [7, Corollary 1]). While this refinement and the case n even will not be needed here, we will return to it later in Section 6.

Proof of Lemma 3. With $n = mp^\alpha$, $p \nmid m$ as above, we let

$$n \equiv \varepsilon \pmod 4, \qquad m \equiv \overline{\varepsilon} \pmod 4, \qquad p^\alpha \equiv \varepsilon_1 \pmod 4,$$

with $\varepsilon, \overline{\varepsilon}, \varepsilon_1 = \pm 1$. Then $\varepsilon = \overline{\varepsilon}\varepsilon_1$, and we have

$$\frac{mp^\alpha - 2 + \varepsilon}{4} = \frac{m - \overline{\varepsilon}}{4} p^\alpha + \overline{\varepsilon}\frac{p^\alpha - 2 + \varepsilon_1}{4} - \frac{1 - \overline{\varepsilon}}{2}, \tag{3.8}$$

which is easy to verify by direct calculation. Now (3.8) can be rewritten as

$$\left\lfloor \frac{n}{4} \right\rfloor = \frac{m - \overline{\varepsilon}}{4} p^\alpha + \overline{\varepsilon}\left\lfloor \frac{p^\alpha}{4} \right\rfloor - \frac{1 - \overline{\varepsilon}}{2}. \tag{3.9}$$

When $\overline{\varepsilon} = 1$, we have a positive remainder upon division by p^α; in this case Lemma 4 (with $n = p^\alpha$) and (1.3) give

$$\sum_{\substack{j=1 \\ p \nmid j}}^{\lfloor n/4 \rfloor} \frac{1}{j^2} \equiv (-1)^{(p^\alpha - 1)/2} 4E_{\varphi(p^\alpha)-2} \pmod{\overline{p^\alpha}} \tag{3.10}$$

(for $m \equiv \overline{\varepsilon} = 1 \pmod 4$). When $\overline{\varepsilon} = -1$, then (3.9) indicates that we sum over $(m - \overline{\varepsilon})/4$ full ranges of p^α, and then subtract a "quarter range" from the last p^α-range. The additional $(1 - \overline{\varepsilon})/2$ accounts for the final term $((m - \overline{\varepsilon})/4)p^\alpha$. Hence again with Lemma 4 (with $n = p^\alpha$) and (1.3), combined with the fact that

$$\frac{1}{(p^\alpha - j)^2} \equiv \frac{1}{j^2} \pmod{p^\alpha},$$

we have again (3.10), but with the right-hand side multiplied by -1. That is, altogether we have

$$\sum_{\substack{j=1 \\ p \nmid j}}^{\lfloor n/4 \rfloor} \frac{1}{j^2} \equiv (-1)^{(m-1)/2}(-1)^{(p^\alpha - 1)/2} 4E_{\varphi(p^\alpha)-2} \pmod{\overline{p^\alpha}}. \tag{3.11}$$

To continue, we first note that by a standard argument (see, e.g., [14, p. 144]) we have

$$\frac{m-1}{2} + \frac{p^\alpha - 1}{2} \equiv \frac{mp^\alpha - 1}{2} = \frac{n-1}{2} \pmod 2. \tag{3.12}$$

Next we use Lemma 2 with $n = p^\alpha$ and $k = \varphi(p^\alpha) - 2$. Since for all odd prime p and integers $\alpha \geq 1$ we clearly have $\varphi(p^\alpha) - 1 = (p-1)p^{\alpha-1} - 1 > \alpha$, the modulus p^α is $(k+1)$th-power free. Since

$$\varphi(n) = \varphi(mp^\alpha) = \varphi(m)\varphi(p^\alpha),$$

an iterated application of Lemma 2 shows that

$$E_{\varphi(n)-2} \equiv E_{\varphi(p^\alpha)-2} \pmod{p^\alpha}. \tag{3.13}$$

Finally, this and (3.12) applied to (3.11) gives (3.6). ∎

To obtain Theorem 1 from Lemma 3, we could use an "inclusion-exclusion" argument. However, we find it more convenient to use an equivalent approach via the Möbius function as was done, for instance, in [3, p. 1818]. Below we will use the definition of the Möbius function, namely

$$\mu(n) = \begin{cases} (-1)^r & \text{when } n = p_1 \cdots p_r, \\ 0 & \text{otherwise,} \end{cases} \tag{3.14}$$

where $p_1, \dots, p_r$ are distinct primes. We also require the basic property

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n > 1; \end{cases} \tag{3.15}$$

see, e.g., [14, p. 193]. Let p be a prime divisor of the odd modulus n in Theorem 1, and write $n = mp^\alpha$, $p \nmid m$. If $m = 1$, then Theorem 1 is just (1.3) and there is nothing more to show; so we assume that $m > 1$. Using (3.15), we write

$$\begin{aligned} \sum_{\substack{j=1 \\ (j,n)=1}}^{\lfloor n/4 \rfloor} \frac{1}{j^2} &= \sum_{\substack{j=1 \\ p\nmid j,\,(j,m)=1}}^{\lfloor n/4 \rfloor} \frac{1}{j^2} = \sum_{\substack{j=1 \\ p\nmid j}}^{\lfloor n/4 \rfloor} \frac{1}{j^2} \sum_{k|(j,m)} \mu(k) \\ &= \sum_{k|m} \mu(k) \sum_{\substack{j=1 \\ p\nmid j,\,k|j}}^{\lfloor n/4 \rfloor} \frac{1}{j^2} = \sum_{k|m} \mu(k) \sum_{\substack{j=1 \\ p\nmid j}}^{\lfloor n/(4k) \rfloor} \frac{1}{(kj)^2} = \sum_{k|m} \frac{\mu(k)}{k^2} \sum_{\substack{j=1 \\ p\nmid j}}^{\lfloor n/(4k) \rfloor} \frac{1}{j^2}. \end{aligned}$$

To continue, we label the primes in the decomposition (3.13) such that $p = p_1$ and $m = p_2^{\alpha_2} \cdots p_r^{\alpha_r}$. Then with (3.14) the last identity becomes

$$\sum_{\substack{j=1 \\ (j,n)=1}}^{\lfloor n/4 \rfloor} \frac{1}{j^2} = \sum_{\nu=0}^{r-1} \sum_{2 \le j_1 < \cdots < j_\nu \le r} \frac{(-1)^\nu}{(p_{j_1} \cdots p_{j_\nu})^2} \sum_{\substack{j=1 \\ p\nmid j}}^{\lfloor n^*/4 \rfloor} \frac{1}{j^2}, \tag{3.16}$$

where for simplicity of notation n^* stands for

$$n^* := \frac{n}{p_{j_1} \cdots p_{j_\nu}}. \tag{3.17}$$

To finish the proof, we apply Lemma 3 to the right-most sum in (3.16), with n^* instead of n in (3.6). Then, applying (3.12) repeatedly to (3.17), we get

$$(-1)^{(n^*-1)/2} = (-1)^{(n-1)/2} (-1)^{(p_{j_1}-1)/2} \cdots (-1)^{(p_{j_\nu}-1)/2}. \tag{3.18}$$

Also, with the same argument as in (3.13) we have

$$E_{\varphi(n^*)-2} \equiv E_{\varphi(p^\alpha)-2} \equiv E_{\varphi(n)-2} \pmod{p^\alpha}, \tag{3.19}$$

so (3.18) and (3.19) together with (3.6) show that

$$\sum_{\substack{j=1\\ p\nmid j}}^{\lfloor n^*/4\rfloor} \frac{1}{j^2} \equiv (-1)^{(p_{j_1}-1)/2}\cdots(-1)^{(p_{j_\nu}-1)/2}(-1)^{(n-1)/2}4E_{\varphi(n)-2} \pmod{\overline{p^\alpha}}. \tag{3.20}$$

Thus, with (3.16) we have

$$\sum_{\substack{j=1\\ (j,n)=1}}^{\lfloor n/4\rfloor} \frac{1}{j^2} \equiv \left(\prod_{i=2}^{r}\left(1-\frac{(-1)^{(p_i-1)/2}}{p_i^2}\right)\right)(-1)^{(n-1)/2}4E_{\varphi(n)-2} \pmod{\overline{p^\alpha}}. \tag{3.21}$$

To complete the proof of Theorem 1, we first assume that $3 \nmid n$. We let p run through all prime divisors of n, and use the Chinese Remainder Theorem in the following form (see, e.g., [14, pp. 64–65]): Given the $r \geq 2$ congruences

$$x \equiv a_j \pmod{p_j^{\alpha_j}}, \quad j = 1, \ldots, r,$$

there is a unique simultaneous solution x_0 modulo $n = p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ given by

$$x_0 = \sum_{j=1}^{r} \frac{n}{p_j^{\alpha_j}} b_j a_j, \tag{3.22}$$

where $b_j \equiv (n/p_j^{\alpha_j})^{-1} \pmod{p_j^{\alpha_j}}$. Now, by Euler's generalization of Fermat's Little Theorem we can take

$$b_j = \left(\frac{n}{p_j^{\alpha_j}}\right)^{\varphi(p_j^{\alpha_j})-1}. \tag{3.23}$$

If we substitute (3.23) into (3.22) and take a_j to be the right-hand side of (3.21) (with p replaced by p_j), then we immediately get the first part of (3.4), with $A(n)$ given by (3.2).

The case $9 \mid n$ requires a more careful analysis. Since the exceptional prime $p = 3$ is involved, the congruence (3.21) holds only modulo $p^{\alpha-1}$ (for $p = 3$), and the combined modulus is

$$\frac{n}{3} = 3^{\alpha_1-1}p_2^{\alpha_2}\cdots p_r^{\alpha_r} \quad (\alpha_1 \geq 2).$$

We proceed as before, but the analogue of (3.22) is now

$$x_0 = \frac{n/3}{3^{\alpha_1-1}} b_1 a_1 + \sum_{j=2}^{r} \frac{n/3}{p_j^{\alpha_j}} b_j a_j. \tag{3.24}$$

First, to determine b_1, we note that

$$\left(\frac{n}{3^{\alpha_1}}\right)^{-1} \equiv \left(\frac{n}{3^{\alpha_1}}\right)^{\varphi(3^{\alpha_1})-1} \pmod{3^{\alpha_1}},$$

and thus

$$b_1 \equiv \left(\frac{n/3}{3^{\alpha_1-1}}\right)^{-1} \equiv \left(\frac{n}{3^{\alpha_1}}\right)^{\varphi(3^{\alpha_1})-1} \pmod{3^{\alpha_1-1}}, \tag{3.25}$$

as required by the Chinese Remainder Theorem. For $j \ge 2$ we have

$$b_j \equiv \left(\frac{n/3}{p_j^{\alpha_j}}\right)^{-1} = 3\left(\frac{n}{p_j^{\alpha_j}}\right)^{-1} \equiv 3\left(\frac{n}{p_j^{\alpha_j}}\right)^{\varphi(p_j^{\alpha_j})-1} \pmod{p_j^{\alpha_j}}. \tag{3.26}$$

If we substitute (3.25) and (3.26) into (3.24), we see that, with $p_1 = 3$,

$$x_0 \equiv \sum_{j=1}^{r}\left(\frac{n}{p_j^{\alpha_j}}\right)^{\varphi(p_j^{\alpha_j})} a_j \pmod{n/3}$$

is the solution given by the Chinese Remainder Theorem. This, along with the definition (3.2), leads to the second part of (3.4).

Finally, when $3 \mid n$ but $9 \nmid n$ (in other words, $n \equiv \pm 3 \pmod 9$), then $\overline{p^\alpha} = 1$ for $p = 3$, and the congruence (3.21) is meaningless and can be deleted from consideration. However, the factor

$$1 - \frac{(-1)^{(p_1-1)/2}}{p_1^2} = 1 + \frac{1}{9}$$

(for $p_1 = 3$) still appears on the right-hand side of (3.22) for all other primes p. This accounts for the extra factor $10/9$ in the third part of the right-hand side of (3.4), while the Chinese Remainder Theorem has been used as in the previous parts.

The proof of Theorem 1 is now complete.

4. Some results on the function $A(n)$. Although the function $A(n)$, as defined in (3.2), is rather complicated, it is possible to derive a few simple properties. The following theorem is the main result of this section; it will be applied in the following section.

THEOREM 2. *Let n be an odd positive integer. Then:*

(a) *if $A(n) \equiv 0 \pmod n$, then $3 \mid n$ but $9 \nmid n$;*
(b) *if $9 \mid n$ and $A(n) \equiv 0 \pmod{n/3}$, then $n = 45$.*

To prove this, we first note that $A(n) \equiv 0 \pmod n$, resp. $A(n) \equiv 0 \pmod{n/3}$, if and only if

$$A(n) \equiv 0 \pmod{p_j^{\alpha_j}}, \quad \text{resp.} \quad A(n) \equiv 0 \pmod{\overline{p_j^{\alpha_j}}}, \quad j = 1, \dots, r, \tag{4.1}$$

where we have used the notation of (3.5). We need the following two lemmas.

LEMMA 5. *For an odd positive integer n we have $A(n) \equiv 0 \pmod{n}$ if and only if*

$$\prod_{\substack{i=1\\ i\neq j}}^{r}(p_i^2 - (-1)^{(p_i-1)/2}) \equiv 0 \pmod{p_j^{\alpha_j}} \quad \text{for all } j = 1, \dots, r \tag{4.2}$$

unless $n \equiv \pm 3 \pmod 9$. Similarly, if $9 \mid n$ then $A(n) \equiv 0 \pmod{n/3}$ if and only if (4.2) *holds modulo $\overline{p_j^{\alpha_j}}$.*

Proof. The hypothesis means that $p_j^{\alpha_j} \geq 5$ and thus $\varphi(p_j^{\alpha_j}) \geq 4$. This implies that $\alpha_i\varphi(p_j^{\alpha_j}) - 2 \geq \alpha_i$ for all $\alpha_i \geq 1$, which is easy to verify. This in turn means that for all $i = 1, \dots, r$ we have

$$p_i^{\alpha_i} \mid p_i^{\alpha_i\varphi(p_j^{\alpha_j})-2},$$

and for a given index ν all summands in (3.2) vanish modulo $p_\nu^{\alpha_\nu}$, with the exception of the summand for $j = \nu$. In this case we note that by Euler's generalization of Fermat's Little Theorem we have

$$\Big(\prod_{\substack{i=1\\ i\neq\nu}}^{r} p_i^{\alpha_i}\Big)^{\varphi(p_\nu^{\alpha_\nu})} \equiv 1 \pmod{p_\nu^{\alpha_\nu}}.$$

Hence the congruence (4.1) implies

$$\prod_{\substack{i=1\\ i\neq\nu}}^{r}\left(1 - \frac{(-1)^{(p_i-1)/2}}{p_i^2}\right) \equiv 0 \pmod{p_\nu^{\alpha_\nu}},$$

and upon multiplying both sides by the appropriate products of squares of the p_i and renaming ν to j, we get (4.2). The opposite direction follows from the Chinese Remainder Theorem. If $9 \mid n$ and $A(n) \equiv 0 \pmod{n/3}$, the proof remains the same. ∎

LEMMA 6. *Suppose that either* (i) $n \not\equiv \pm 3 \pmod 9$ *and* $A(n) \equiv 0 \pmod n$, *or* (ii) $9 \mid n$ *and* $A(n) \equiv 0 \pmod{n/3}$. *Then the largest prime factor of n satisfies $q \equiv 1 \pmod 4$, and there is another prime factor $p \equiv 3 \pmod 4$ such that*

$$p^2 + 1 \equiv 0 \pmod q, \tag{4.3}$$

$$q^2 - 1 \equiv 0 \pmod p. \tag{4.4}$$

Proof. First we note that a necessary condition for (4.2) to hold is that the congruences must hold modulo p_j. This means that the remainder of the proof is identical for the cases (i) and (ii). Assume that the prime factors of n are ordered by size: $p_1 < \cdots < p_r$. Consider the last one of the modified

congruences (4.2), namely

$$\prod_{i=1}^{r-1}(p_i^2-(-1)^{(p_i-1)/2})\equiv 0 \pmod{p_r}. \tag{4.5}$$

Now p_r has to divide one of the factors in (4.5), say the one for $i=\nu$. If $p_\nu \equiv 1 \pmod 4$ then the corresponding quadratic term factors, and we have $p_r \mid p_\nu - 1$ or $p_r \mid p_\nu + 1$, which is impossible since p_r is the largest prime factor. If, on the other hand, $p_\nu \equiv 3 \pmod 4$ then we have $p_\nu^2+1 \equiv 0 \pmod{p_r}$, and by quadratic reciprocity this is impossible when $p_r \equiv 3 \pmod 4$. Therefore we require $p_r \equiv 1 \pmod 4$, while there has to be at least one other prime factor $p_\nu \equiv 3 \pmod 4$. This proves the lemma, with $p := p_\nu$ and $q := p_r$. ∎

To finish the proof of Theorem 2, we note that by Theorem 1 in [8], the pair of quadratic congruences (4.3), (4.4) has $p=3$, $q=5$ as its only prime solution. Then by Lemma 6 the only n which can possibly satisfy conditions (i) or (ii) are of the form $n = 3^\alpha 5^\beta$ with $\alpha \ge 2$ and $\beta \ge 1$. However, in case (a) of Theorem 2 we have

$$5^2 - 1 \not\equiv 0 \pmod{3^\alpha} \quad \text{for } \alpha \ge 2,$$

which contradicts (4.2). Similarly, for case (b) we have

$$5^2 - 1 \equiv 0 \pmod{3^{\alpha-1}} \quad \text{and} \quad 3^2+1 \equiv 0 \pmod{5^\beta}$$

if and only if $\alpha = 2$ and $\beta = 1$, i.e., $n = 45$. This, by Lemma 5, completes the proof of Theorem 2.

Table 1. All odd $n \le 10^8$ for which $A(n) \equiv 0 \pmod n$

n	factored	n	factored
525	$3 \cdot 5^2 \cdot 7$	4876437	$3 \cdot 23 \cdot 29 \cdot 2437$
705	$3 \cdot 5 \cdot 47$	4953165	$3 \cdot 5 \cdot 7^2 \cdot 23 \cdot 293$
1725	$3 \cdot 5^2 \cdot 23$	5928285	$3 \cdot 5 \cdot 11 \cdot 19 \cdot 31 \cdot 61$
25935	$3 \cdot 5 \cdot 7 \cdot 13 \cdot 19$	7739985	$3 \cdot 5 \cdot 11 \cdot 61 \cdot 769$
50325	$3 \cdot 5^2 \cdot 11 \cdot 61$	8019375	$3 \cdot 5^4 \cdot 7 \cdot 13 \cdot 47$
61755	$3 \cdot 5 \cdot 23 \cdot 179$	8224125	$3 \cdot 5^3 \cdot 7 \cdot 13 \cdot 241$
72345	$3 \cdot 5 \cdot 7 \cdot 13 \cdot 53$	18163299	$3 \cdot 7 \cdot 11 \cdot 61 \cdot 1289$
231735	$3 \cdot 5 \cdot 7 \cdot 2207$	24088155	$3 \cdot 5 \cdot 7^2 \cdot 13 \cdot 2521$
436821	$3 \cdot 7 \cdot 11 \cdot 31 \cdot 61$	28393365	$3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 31 \cdot 61$
473109	$3 \cdot 7 \cdot 13 \cdot 1733$	32717685	$3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 2179$
1188525	$3 \cdot 5^2 \cdot 13 \cdot 23 \cdot 53$	40981125	$3 \cdot 5^3 \cdot 103 \cdot 1061$
2308911	$3 \cdot 11 \cdot 31 \cdot 37 \cdot 61$	46830225	$3 \cdot 5^2 \cdot 13 \cdot 43 \cdot 1117$
3353025	$3 \cdot 5^2 \cdot 13 \cdot 19 \cdot 181$	89995191	$3 \cdot 11 \cdot 13 \cdot 19 \cdot 61 \cdot 181$

Theorem 2(a) is illustrated by Table 1. In addition to the 26 integers $n \le 10^8$, there are 57 more $n \le 10^{10}$ for which $A(n) \equiv 0 \pmod{n}$. Table 1 also suggests that such n have at least three distinct prime factors. This is indeed the case:

COROLLARY 1. *If an odd positive integer n satisfies $A(n) \equiv 0 \pmod{n}$, then n has at least three distinct prime factors.*

Proof. To obtain a contradiction, we assume that n has only two prime factors. By Theorem 2 it is of the form $n = 3p^\alpha$ with $p \ge 5$ and $\alpha \ge 1$. The definition (3.2) gives

$$A(n) = p^{2\alpha}\left(1 - \frac{(-1)^{(p-1)/2}}{p^2}\right) + 3^{\varphi(p^\alpha)}\left(1 + \frac{1}{3^2}\right). \tag{4.6}$$

Since $p^2 \equiv 1 \pmod 3$ and $\varphi(p^\alpha) \ge 4$, we have

$$A(n) \equiv 1 - (-1)^{(p-1)/2} \pmod 3. \tag{4.7}$$

Next, when $\alpha \ge 2$, then (4.6) with Euler's theorem gives

$$A(n) \equiv 1 + 3^{-2} \equiv 3^{-2} \cdot 10 \not\equiv 0 \pmod{p^\alpha},$$

which proves the corollary for $\alpha \ge 2$. If $\alpha = 1$ then (4.6) gives

$$A(n) \equiv (-1)^{(p+1)/2} + 1 + 3^{-2} \pmod p.$$

When $p \equiv 1 \pmod 4$, then this expression cannot vanish modulo p. When $p \equiv 3 \pmod 4$, we use (4.7) which shows that $A(n) \not\equiv 0 \pmod 3$. ∎

5. Vanishing sums modulo n. As mentioned in the Introduction, sums of the type (1.1) and the corresponding congruences involving Bernoulli numbers or, as in this case, Euler numbers have been of historical interest in connection with Fermat's Last Theorem. In analogy to irregular primes (see, e.g., [17]), Ernvall and Metsänkylä [9] studied E-irregular primes. In particular, if the prime p divides the Euler number E_{p-3}, then $(p, p-3)$ is called an "E-irregular pair". For easier reference we introduce the following terminology.

DEFINITION 1. An odd prime p will be called an *E-prime* if $p \mid E_{p-3}$, or in other words, if $(p, p-3)$ is an E-irregular pair.

The first such primes, $p = 149$ and $p = 241$, were found in [9], and using PARI [16] and the congruence (1.1), we found three more such primes up to 50 million. These calculations were verified by D. Staple with a custom C program, and extended up to 200 million. Finally, independently of this

paper and using an algorithm due to Peter Montgomery, R. McIntosh [13] had recently computed three further E-primes up to $3 \cdot 10^9$; see Table 2.

Table 2. All E-primes $p < 3 \cdot 10^9$

p	$p^2 - (-1)^{(p-1)/2}$ factored
149	$2^3 \cdot 3 \cdot 5^2 \cdot 37$
241	$2^5 \cdot 3 \cdot 5 \cdot 11^2$
2946901	$2^3 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 19 \cdot 37 \cdot 47 \cdot 5689$
16467631	$2 \cdot 70657 \cdot 1919009233$
17613227	$2 \cdot 5 \cdot 13 \cdot 37 \cdot 2557 \cdot 25223309$
327784727	$2 \cdot 5 \cdot 409 \cdot 127637 \cdot 69697 \cdot 2953$
426369739	$2 \cdot 157 \cdot 757 \cdot 1546057 \cdot 494677$
1062232319	$2 \cdot 13 \cdot 281 \cdot 397 \cdot 353653 \cdot 1099997$

While the E-primes are exactly the prime values n for which $S_4(n)$ in (3.3) vanishes modulo n, we will now extend this question to all odd integers n. The following result shows that once again the E-primes play an important role in this.

COROLLARY 2. *Let n be an odd positive integer.*

(a) *If $S_4(n) \equiv 0 \pmod{n}$, then $n = 45$, or n is divisible by an E-prime.*
(b) *If $3 \mid n$ and $S_4(n) \equiv 0 \pmod{n/3}$, then $n = 3, 15, 45$, or n is divisible by an E-prime.*

Proof. We begin by distinguishing between three cases, corresponding to the cases of Theorem 1. First, if $3 \nmid n$, then by Theorem 2(a) we have $A(n) \not\equiv 0 \pmod{n}$, and consequently by Theorem 1 there must be a prime $p > 3$, $p \mid n$, such that

$$E_{\varphi(n)-2} \equiv 0 \pmod{p}. \tag{5.1}$$

Next, let $n \equiv \pm 3 \pmod 9$. If $n = 3$, then (3.4) holds trivially, and for $n = 15$, the factor 40 in (3.4) means that the congruence also holds trivially, both modulo $n/3$; this is not the case modulo n. Otherwise we have, again by Theorem 2(a), $A(n/3) \not\equiv 0 \pmod{n/3}$, and by Theorem 1, as before, there is a prime $p > 3$, $p \mid n$, that satisfies (5.1). Finally, it is easy to verify that $n = 45$ satisfies the congruence in question. However, if $9 \mid n$ and $n \neq 45$, then by Theorem 2(b) we have $A(n) \not\equiv 0 \pmod{n/3}$, and by Theorem 1 there must once again exist a prime $p > 3$, $p \mid n$, that satisfies (5.1).

Now, if we write $n = p^\alpha m$ with $p \nmid m$, then

$$\varphi(n) - 2 = (p-1)p^{\alpha-1}\varphi(m) - 2 = (p^{\alpha-1}\varphi(m) - 1)(p-1) + (p-3), \tag{5.2}$$

and thus, by Kummer's congruence (2.1),

$$E_{\varphi(n)-2} \equiv E_{p-3} \pmod{p}, \tag{5.3}$$

which vanishes modulo p if and only if p is an E-prime. This, with (5.1), completes the proof. ∎

Table 3. All odd $n \le 2 \cdot 10^7$, $3 \nmid n$, for which $S_4(n) \equiv 0 \pmod{n}$

n	factored	n	factored
149	149	897725	$5^2 \cdot 149 \cdot 241$
241	241	1328633	$37 \cdot 149 \cdot 241$
745	$5 \cdot 149$	1778821	$11^2 \cdot 61 \cdot 241$
1205	$5 \cdot 241$	1974995	$5 \cdot 11 \cdot 149 \cdot 241$
2651	$11 \cdot 241$	2618675	$5^2 \cdot 19 \cdot 37 \cdot 149$
3725	$5^2 \cdot 149$	2946901	2946901
5513	$37 \cdot 149$	4042775	$5^2 \cdot 11 \cdot 61 \cdot 241$
13255	$5 \cdot 11 \cdot 241$	4344989	$11^2 \cdot 149 \cdot 241$
27565	$5 \cdot 37 \cdot 149$	4488625	$5^3 \cdot 149 \cdot 241$
29161	$11^2 \cdot 241$	5013041	$11 \cdot 31 \cdot 61 \cdot 241$
35909	$149 \cdot 241$	6643165	$5 \cdot 37 \cdot 149 \cdot 241$
104747	$19 \cdot 37 \cdot 149$	8894105	$5 \cdot 11^2 \cdot 61 \cdot 241$
137825	$5^2 \cdot 37 \cdot 149$	9874975	$5^2 \cdot 11 \cdot 149 \cdot 241$
145805	$5 \cdot 11^2 \cdot 241$	14614963	$11 \cdot 37 \cdot 149 \cdot 241$
161711	$11 \cdot 61 \cdot 241$	14734505	$5 \cdot 2946901$
179545	$5 \cdot 149 \cdot 241$	16467631	16467631
394999	$11 \cdot 149 \cdot 241$	17613227	17613227
523735	$5 \cdot 19 \cdot 37 \cdot 149$	18959207	$19 \cdot 37 \cdot 149 \cdot 181$
808555	$5 \cdot 11 \cdot 61 \cdot 241$		

This result is illustrated by Tables 3, 4, and 5. The next result provides explanations for the other prime factors of the solutions n shown in these tables; in fact, we obtain complete characterizations. On account of the three different cases in Theorem 1, we need to distinguish between these cases also here.

To state this result, we use the notation

$$\nu_p(n) = \alpha \quad \text{if and only if} \quad p^\alpha \parallel n,$$

where p is a prime. Also, p_j will denote an odd prime, and $\delta_{p,q}$ the Kronecker delta defined by $\delta_{p,q} = 1$ when $p = q$ and 0 otherwise.

Corollary 3. *Let* $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} p_{r+1} \cdots p_{r+s}$, *where* $s \ge 1$ *and* $p_{r+1}, \ldots, p_{r+s}$ *are distinct E-primes.*

(a) *If* $3 \nmid n$, *then* $S_4(n) \equiv 0 \pmod{n}$ *if and only if*

$$1 \le \alpha_j \le \nu_{p_j}\Big(\prod_{i=1}^{r+s}(p_i^2 - (-1)^{(p_i-1)/2})\Big), \quad j = 1, \dots, r. \tag{5.4}$$

(b) *If* $p_1 = 3$ *and* $\alpha_1 \ge 2$, *then* $S_4(n) \equiv 0 \pmod{n/3}$ *if and only if*

$$1 \le \alpha_j \le \nu_{p_j}\Big(\prod_{i=1}^{r+s}(p_i^2 - (-1)^{(p_i-1)/2})\Big) + \delta_{3,p_j}, \quad j = 1, \dots, r. \tag{5.5}$$

(c) *If* $p_1 = 3$ *and* $\alpha_1 = 1$, *then* $S_4(n) \equiv 0 \pmod{n/3}$ *if and only if*

$$1 \le \alpha_j \le \nu_{p_j}\Big(\prod_{i=2}^{r+s}(p_i^2 - (-1)^{(p_i-1)/2})\Big) + \delta_{5,p_j}, \quad j = 2, \dots, r. \tag{5.6}$$

If $r = 0$ *in* (a) *or* $r = 1$ *in* (c), *we consider the conditions* (5.4), *resp.* (5.6), *to be vacuously satisfied.*

Proof. (a) In order to apply the first part of Theorem 1, we first note that by (5.2) and (5.3) we have

$$E_{\varphi(n)-2} \equiv 0 \pmod{p_{r+k}}, \quad k = 1, \dots, s. \tag{5.7}$$

Next, by (4.1) and the proof of Lemma 5 we have

$$A(n) \equiv 0 \pmod{p_j^{\alpha_j}}, \quad j = 1, \dots, r, \tag{5.8}$$

if and only if the condition (5.4) holds. The result now follows from the first congruence in (3.4) and the Chinese Remainder Theorem.

(b) Since Theorem 1, (4.1), and Lemma 5 still hold when $9 \mid n$, the proof of this part is almost identical to that of part (a), but using the second congruence in (3.4). Another difference is that for $p_1 = 3$ the congruence (4.2) holds only modulo 3^{α_1-1}, which, however, does not change the assertion of part (b). Finally, since we are dealing with a congruence modulo $n/3$, the power of 3 occurring in n can be 1 higher than given by the factors in Lemma 5. This accounts for the summand δ_{3,p_j} in (5.5).

(c) Here we use the third part of (3.4), and in place of (5.8) we have $A(n/3) \equiv 0 \pmod{p_j^{\alpha_j}}$, $j = 2, \dots, r$, since Lemma 5 applies just as in part (a), with n replaced by $n/3$. Hence the prime $p_1 = 3$ does not occur in (5.6). On the other hand, special attention must be paid to the prime 5: The factor 40 in (3.4) provides an extra power of 5, in addition to those coming from Lemma 5. This accounts for the summand δ_{5,p_j} in (5.6). ∎

Table 4. All odd $n \le 2 \cdot 10^7$, $9 \mid n$ for which $S_4(n) \equiv 0 \pmod{n/3}$

n	factored	n	factored
45	$3^2 \cdot 5$	1312245	$3^2 \cdot 5 \cdot 11^2 \cdot 241$
1341	$3^2 \cdot 149$	1455399	$3^2 \cdot 11 \cdot 61 \cdot 241$
2169	$3^2 \cdot 241$	1615905	$3^2 \cdot 5 \cdot 149 \cdot 241$
6705	$3^2 \cdot 5 \cdot 149$	1789425	$3^3 \cdot 5^2 \cdot 11 \cdot 241$
10845	$3^2 \cdot 5 \cdot 241$	2232765	$3^4 \cdot 5 \cdot 37 \cdot 149$
20115	$3^3 \cdot 5 \cdot 149$	2828169	$3^3 \cdot 19 \cdot 37 \cdot 149$
23859	$3^2 \cdot 11 \cdot 241$	3554991	$3^2 \cdot 11 \cdot 149 \cdot 241$
32535	$3^3 \cdot 5 \cdot 241$	3721275	$3^3 \cdot 5^2 \cdot 37 \cdot 149$
33525	$3^2 \cdot 5^2 \cdot 149$	3936735	$3^3 \cdot 5 \cdot 11^2 \cdot 241$
49617	$3^2 \cdot 37 \cdot 149$	4366197	$3^3 \cdot 11 \cdot 61 \cdot 241$
54225	$3^2 \cdot 5^2 \cdot 241$	4713615	$3^2 \cdot 5 \cdot 19 \cdot 37 \cdot 149$
100575	$3^3 \cdot 5^2 \cdot 149$	4847715	$3^3 \cdot 5 \cdot 149 \cdot 241$
119295	$3^2 \cdot 5 \cdot 11 \cdot 241$	6202125	$3^2 \cdot 5^3 \cdot 37 \cdot 149$
148851	$3^3 \cdot 37 \cdot 149$	6561225	$3^2 \cdot 5^2 \cdot 11^2 \cdot 241$
162675	$3^3 \cdot 5^2 \cdot 241$	6698295	$3^5 \cdot 5 \cdot 37 \cdot 149$
167625	$3^2 \cdot 5^3 \cdot 149$	7276995	$3^2 \cdot 5 \cdot 11 \cdot 61 \cdot 241$
248085	$3^2 \cdot 5 \cdot 37 \cdot 149$	8079525	$3^2 \cdot 5^2 \cdot 149 \cdot 241$
262449	$3^2 \cdot 11^2 \cdot 241$	8484507	$3^4 \cdot 19 \cdot 37 \cdot 149$
323181	$3^2 \cdot 149 \cdot 241$	10664973	$3^3 \cdot 11 \cdot 149 \cdot 241$
357885	$3^3 \cdot 5 \cdot 11 \cdot 241$	11163825	$3^4 \cdot 5^2 \cdot 37 \cdot 149$
446553	$3^4 \cdot 37 \cdot 149$	11957697	$3^2 \cdot 37 \cdot 149 \cdot 241$
502875	$3^3 \cdot 5^3 \cdot 149$	14140845	$3^3 \cdot 5 \cdot 19 \cdot 37 \cdot 149$
596475	$3^2 \cdot 5^2 \cdot 11 \cdot 241$	14543145	$3^4 \cdot 5 \cdot 149 \cdot 241$
744255	$3^3 \cdot 5 \cdot 37 \cdot 149$	16009389	$3^2 \cdot 11^2 \cdot 61 \cdot 241$
942723	$3^2 \cdot 19 \cdot 37 \cdot 149$	17774955	$3^2 \cdot 5 \cdot 11 \cdot 149 \cdot 241$
969543	$3^3 \cdot 149 \cdot 241$	18606375	$3^3 \cdot 5^3 \cdot 37 \cdot 149$
1240425	$3^2 \cdot 5^2 \cdot 37 \cdot 149$	19683675	$3^3 \cdot 5^2 \cdot 11^2 \cdot 241$

EXAMPLES. (1) Consider the smallest E-prime 149, and note that

$$149^2 - 1 = 2^3 \cdot 3 \cdot 5^2 \cdot 37, \quad 37^2 - 1 = 2^3 \cdot 3^2 \cdot 19, \quad 19^2 + 1 = 2 \cdot 181.$$

If we set $n = 149 \cdot 37 \cdot 19 \cdot 181$, then Corollary 3(a) shows that $S_4(n) \equiv 0 \pmod{n}$. In particular, this example shows that the largest prime factor of such an n may not be an E-prime; see the final entry in Table 3.

(2) If we further note that $181^2 - 1 = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$, as well as $5^2 - 1 = 2^3 \cdot 3$, $7^2 + 1 = 2 \cdot 5^2$, and $13^2 - 1 = 2^3 \cdot 3 \cdot 7$, then Corollary 3(a) shows that

$$n = 149 \cdot 37 \cdot 19 \cdot 181 \cdot 13 \cdot 7^2 \cdot 5^3 = 1\,509\,626\,857\,375$$

is the largest odd integer n, not divisible by 3 and having $n = 149$ as sole E-prime factor, which satisfies $S_4(n) \equiv 0 \pmod{n}$.

(3) Since $241^2 - 1 = 2^5 \cdot 3 \cdot 5 \cdot 11^2$, $3^2 + 1 = 2 \cdot 5$, and $5^2 - 1 = 2^3 \cdot 3$, Corollary 3(b) shows that for

$$n = 3^\alpha \cdot 5^\beta \cdot 241, \quad 2 \le \alpha \le 3, \quad 1 \le \beta \le 2,$$

we have $S_4(n) \equiv 0 \pmod{n/3}$. Furthermore, $\beta = 0$ forces $\alpha = 2$ for the congruence to hold. These are all possibilities for α and β in this case; see also Table 4.

(4) Given the factorizations in Table 2, Corollary 3(c) shows that for

$$n = 3 \cdot 5^\beta \cdot 149 \cdot 241, \quad 0 \le \beta \le 4,$$

we have $S_4(n) \equiv 0 \pmod{n/3}$, and this congruence holds for no larger β. Although the prime $p_1 = 3$ does not contribute to the "allowable" powers of 5, the Kronecker delta in (5.6) does add to it, giving a maximum of $\beta = 4$.

Table 5. All odd $n \le 2 \cdot 10^7$, $n \equiv \pm 3 \pmod 9$, with $S_4(n) \equiv 0 \pmod{n/3}$

n	factored	n	factored
3	3	485133	$3 \cdot 11 \cdot 61 \cdot 241$
15	$3 \cdot 5$	538635	$3 \cdot 5 \cdot 149 \cdot 241$
447	$3 \cdot 149$	1184997	$3 \cdot 11 \cdot 149 \cdot 241$
723	$3 \cdot 241$	1571205	$3 \cdot 5 \cdot 19 \cdot 37 \cdot 149$
2235	$3 \cdot 5 \cdot 149$	2067375	$3 \cdot 5^3 \cdot 37 \cdot 149$
3615	$3 \cdot 5 \cdot 241$	2187075	$3 \cdot 5^2 \cdot 11^2 \cdot 241$
7953	$3 \cdot 11 \cdot 241$	2425665	$3 \cdot 5 \cdot 11 \cdot 61 \cdot 241$
11175	$3 \cdot 5^2 \cdot 149$	2693175	$3 \cdot 5^2 \cdot 149 \cdot 241$
16539	$3 \cdot 37 \cdot 149$	3985899	$3 \cdot 37 \cdot 149 \cdot 241$
18075	$3 \cdot 5^2 \cdot 241$	5336463	$3 \cdot 11^2 \cdot 61 \cdot 241$
39765	$3 \cdot 5 \cdot 11 \cdot 241$	5924985	$3 \cdot 5 \cdot 11 \cdot 149 \cdot 241$
55875	$3 \cdot 5^3 \cdot 149$	7856025	$3 \cdot 5^2 \cdot 19 \cdot 37 \cdot 149$
82695	$3 \cdot 5 \cdot 37 \cdot 149$	8840703	$3 \cdot 2946901$
87483	$3 \cdot 11^2 \cdot 241$	12128325	$3 \cdot 5^2 \cdot 11 \cdot 61 \cdot 241$
107727	$3 \cdot 149 \cdot 241$	13034967	$3 \cdot 11^2 \cdot 149 \cdot 241$
198825	$3 \cdot 5^2 \cdot 11 \cdot 241$	13465875	$3 \cdot 5^3 \cdot 149 \cdot 241$
314241	$3 \cdot 19 \cdot 37 \cdot 149$	15039123	$3 \cdot 11 \cdot 31 \cdot 61 \cdot 241$
413475	$3 \cdot 5^2 \cdot 37 \cdot 149$	19929495	$3 \cdot 5 \cdot 37 \cdot 149 \cdot 241$
437415	$3 \cdot 5 \cdot 11^2 \cdot 241$		

6. Even moduli n. In this section we consider the sum $S_4(n)$, defined in (3.3), for *even* integers n. As we shall see, the cases $n \equiv 0 \pmod 4$ and $n \equiv 2 \pmod 4$ are fundamentally different. We begin with the first case.

THEOREM 3. *Let $n = 4m$, where m is a positive integer.*

(a) *If $3 \nmid n$ and $n \neq 2^\alpha$, then $S_4(n) \equiv 0 \pmod{N_1}$, where $N_1 \in \{m, 2m, 4m\}$. In particular, if m is odd and $8 \mid \varphi(m)$, then $S_4(n) \equiv 0 \pmod{n}$.*

(b) *If $3 \mid n$, then $S_4(n) \equiv 0 \pmod{N_2}$, where $N_2 \in \{m/3, 2m/3, 4m/3, m, 2m, 4m\}$. In particular, if m is odd, has a prime divisor $p \equiv 1 \pmod 6$, and $8 \mid \varphi(m)$, then $S_4(n) \equiv 0 \pmod{n}$.*

(c) *If $n = 2^\alpha$, $\alpha \geq 3$, then $S_4(n) \equiv 0 \pmod{n/8}$.*

The smallest example for the special case in (b) is $n = 4 \cdot 39$; note that $13 \equiv 1 \pmod 6$ and $\varphi(39) = 24 \equiv 0 \pmod 8$.

For the proof of Theorem 3 we require Lemma 4 in Section 3 above, as well as the following lemma which also uses the sum $S_1(n)$ defined in (3.7).

LEMMA 7. *Let $m \geq 2$ be an integer. Then*

$$S_4(4m) \equiv \begin{cases} S_1(m) \pmod m & \text{when } m \text{ is even,} \\ \frac{7}{8} S_1(m) \pmod m & \text{when } m \text{ is odd,} \end{cases} \tag{6.1}$$

and

$$S_4(4m) \equiv \begin{cases} \varphi(m) \pmod 4 & \text{when } m \text{ is even,} \\ \frac{1}{2}\varphi(m) \pmod 4 & \text{when } m \text{ is odd.} \end{cases} \tag{6.2}$$

Proof. If m is even, then an integer j satisfies $(j, 4m) = 1$ if and only if $(j, m) = 1$. Hence by comparing the definitions of the sums $S_4(4m)$ and $S_1(m)$ in (3.3) and (3.7), respectively, we see that $S_4(4m) = S_1(m)$. This immediately gives the first part of (6.1). If we note that for all odd j we have $1/j^2 \equiv 1 \pmod 4$, we see, again by the definition of $S_1(m)$, that $S_1(m) \equiv \varphi(m) \pmod 4$. This proves the first part of (6.2).

Now let m be odd. Then

$$S_4(4m) = \sum_{\substack{j=1 \\ (j,4m)=1}}^{m} \frac{1}{j^2} = \sum_{\substack{j=1 \\ (j,m)=1}}^{m} \frac{1}{j^2} - \sum_{\substack{j=1 \\ (j,m)=1 \\ j \text{ even}}}^{m} \frac{1}{j^2} = S_1(m) - \frac{1}{4} \sum_{\substack{j=1 \\ (j,m)=1}}^{\lfloor m/2 \rfloor} \frac{1}{j^2}. \tag{6.3}$$

It is straightforward to show by a symmetry argument (see also identity (10) in [1]) that

$$\sum_{\substack{j=1 \\ (j,m)=1}}^{\lfloor m/2 \rfloor} \frac{1}{j^2} \equiv \frac{1}{2} \sum_{\substack{j=1 \\ (j,m)=1}}^{m} \frac{1}{j^2} = \frac{1}{2} S_1(m) \pmod m, \tag{6.4}$$

and this, with (6.3), gives the second part of (6.1).

Finally, since for each fixed $k = 1, 2, 3$ we have $(km + j, 4m) = 1$ for exactly those j for which $(j, 4m) = 1$, the definition of $S_4(n)$ implies

that $S_4(4m) \equiv \frac{1}{4}\varphi(4m) = \frac{1}{2}\varphi(m) \pmod 4$, which proves the second part of (6.2). ∎

Proof of Theorem 3. (a) Suppose that $3 \nmid n$, and that n is not a power of 2. Then by (6.1) and Lemma 4 we have $S_4(4m) \equiv 0 \pmod m$, while by (6.2), $S_4(4m)$ may be odd, or it may be congruent to 0 modulo 2 or 4, which proves the first part of (a).

If m is odd and $8 \mid \varphi(m)$, then $S_4(4m) \equiv 0 \pmod 4$ by (6.2), and then by (6.1), Lemma 4, and the Chinese Remainder Theorem we have $S_4(4m) \equiv 0 \pmod{4m}$, which proves the second part of (a).

(b) If $3 \mid n$, then by (6.1) and Lemma 4 we have $S_4(4m) \equiv 0 \pmod{m/3}$, while by (6.2), as before, we may have $S_4(4m) \equiv 0 \pmod j$ with $j \in \{1, 2, 4\}$. This gives the possible values $m/3, 2m/3, 4m/3$ for N_2. Now, if m has a prime divisor $p \equiv 1 \pmod 6$ (see the Remark following Lemma 4) then $S_4(4m) \equiv 0 \pmod m$ after all. Just like in part (a) this gives the possible values $m, 2m, 4m$ for N_2, and also the second part of (b).

(c) If $n = 2^\alpha$, $\alpha \ge 3$, then (6.1) and Lemma 4, together with (6.2) and the Chinese Remainder Theorem, give the desired result. ∎

Remark. A more detailed study might give an exact characterization of the occurrences of the different values of N_1 and N_2 in parts (a) and (b). Also, based on computations we believe that m can be eliminated from the set of values for N_2. However, this would go beyond the scope of this paper.

As mentioned at the beginning of this section, the case $n \equiv 2 \pmod 4$ is very different from the first case. In fact, it can be easily reduced to the situation of Theorem 2.

Theorem 4. *Let m be an odd positive integer. Then*

$$S_4(2m) \equiv \begin{cases} -\frac{1}{4}S_4(m) \pmod m & \text{when } 3 \nmid m, \\ -\frac{1}{4}S_4(m) \pmod{m/3} & \text{when } 3 \mid m. \end{cases} \tag{6.5}$$

Proof. Similar to the situation in (6.3), we have

$$S_4(2m) = \sum_{\substack{j=1 \\ (j,2m)=1}}^{\lfloor m/2 \rfloor} \frac{1}{j^2} = \sum_{\substack{j=1 \\ (j,m)=1}}^{\lfloor m/2 \rfloor} \frac{1}{j^2} - \sum_{\substack{j=1 \\ (j,m)=1 \\ j \text{ even}}}^{\lfloor m/2 \rfloor} \frac{1}{j^2}$$

$$\equiv \frac{1}{2}S_1(m) - \frac{1}{4}\sum_{\substack{j=1 \\ (j,m)=1}}^{\lfloor m/4 \rfloor} \frac{1}{j^2} = \frac{1}{2}S_1(m) - \frac{1}{4}S_4(m) \pmod m,$$

where we have used the congruence (6.4). Now, by Lemma 4 the term $S_1(m)$ vanishes modulo m or modulo $m/3$, according as $3 \nmid m$ or $3 \mid m$, respectively. This proves both cases of (6.5). ∎

7. A further consequence of Theorem 1. Many congruences for sums of reciprocals involve the *Fermat quotient* $q_p(a)$, defined for odd primes p by

$$q_p(a) := \frac{a^{p-1}-1}{p}, \tag{7.1}$$

with base $a \geq 2$ an integer with $p \nmid a$. For instance, Lerch [12] proved that for primes $p \geq 5$,

$$\sum_{j=1}^{\lfloor p/4 \rfloor} \frac{1}{j} \equiv -3q_p(2) \pmod{p}. \tag{7.2}$$

This was extended to a congruence modulo p^2 by Z.-H. Sun [18, Corollary 3.3], namely

$$\sum_{j=1}^{\lfloor p/4 \rfloor} \frac{1}{j} \equiv -3q_p(2) + \frac{3}{2}pq_p(2)^2 - (-1)^{(p-1)/2}pE_{p-3} \pmod{p^2}, \tag{7.3}$$

and an extension to odd composite moduli is a consequence of the following results of Cai, Fu and Zhang [2], and (independently) Cao and Pan [3]: For any positive integer n with $(n,6)=1$ we have

$$\sum_{\substack{j=1 \\ (j,n)=1}}^{\lfloor n/4 \rfloor} \frac{1}{n-4j} \equiv \frac{3}{4}q_n(2) - \frac{3}{8}nq_n(2)^2 \pmod{n^2}, \tag{7.4}$$

where $q_n(a)$ is the *Euler quotient* of n with base a, defined by

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

for positive integers a, n with $n > 1$; this obviously generalizes the Fermat quotient defined by (7.1). Taking this modulo n, we obtain

$$\sum_{\substack{j=1 \\ (j,n)=1}}^{\lfloor n/4 \rfloor} \frac{1}{j} \equiv -3q_n(2) \pmod{n}, \tag{7.5}$$

again for $(n,6)=1$.

While the congruence (7.4) alone is not sufficient to prove a modulo n^2 extension of (7.5), in this brief section we will see that Theorem 1 will enable us to do so. Following the example of a congruence modulo p^2 in [11, p. 359], we expand, for odd positive n and $(j,n)=1$,

$$\frac{1}{n-4j} = \frac{-1}{4j}\left(\frac{1}{1-n/4j}\right) \equiv \frac{-1}{4j}\left(1+\frac{n}{4j}\right) = \frac{-1}{4j} - \frac{n}{16j^2} \pmod{n^2},$$

and thus

$$\frac{1}{j} \equiv -\frac{4}{n-4j} - \frac{n}{4}\,\frac{1}{j^2} \pmod{n^2}. \tag{7.6}$$

We are now ready to state the desired extension of the congruence (7.5). For the sake of simplicity we restrict our attention to the main case where $3 \nmid n$.

COROLLARY 4. *For any positive integer with* $(n, 6) = 1$ *we have*

$$\sum_{\substack{j=1\\(j,n)=1}}^{\lfloor n/4 \rfloor} \frac{1}{j} \equiv -3q_n(2) + \frac{3}{2} n q_n(2)^2 - (-1)^{(n-1)/2} n A(n) E_{\varphi(n)-2} \pmod{n^2}. \tag{7.7}$$

This follows immediately from (7.6), with Theorem 1 and with (7.4). By appealing to the second and third parts of Theorem 1, and to results in [7], this corollary can easily be extended to all odd integers.

Acknowledgments. We would like to thank Douglas B. Staple of Dalhousie University and Richard McIntosh of the University of Regina for their computations related to Table 2.

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

References

[1] T. X. Cai, *A congruence involving the quotients of Euler and its applications (I)*, Acta Arith. 103 (2002), 313–320.

[2] T. X. Cai, X. D. Fu, and X. Zhou, *A congruence involving the quotients of Euler and its applications (II)*, Acta Arith. 130 (2007), 203–214.

[3] H.-Q. Cao and H. Pan, *Note on some congruences of Lehmer*, J. Number Theory 129 (2009), 1813–1819.

[4] L. Carlitz, *A note on Euler numbers and polynomials*, Nagoya Math. J. 7 (1954), 35–43.

[5] L. Carlitz and J. Levine, *Some problems concerning Kummer's congruences for the Euler numbers and polynomials*, Trans. Amer. Math. Soc. 96 (1960), 23–37.

[6] K. W. Chen, *Congruences for Euler numbers*, Fibonacci Quart. 42 (2004), 128–140.

[7] J. B. Cosgrave and K. Dilcher, *Sums of reciprocals modulo composite integers*, J. Number Theory 133 (2013), 3565–3577.

[8] J. B. Cosgrave and K. Dilcher, *Pairs of reciprocal quadratic congruences involving primes*, Fibonacci Quart. 51 (2013), 98–111.

[9] R. Ernvall and T. Metsänkylä, *Cyclotomic invariants and E-irregular primes*, Math. Comp. 32 (1978), 617–629.

[10] Y. He and Q. Y. Liao, *Some congruences involving Euler numbers*, Fibonacci Quart. 46/47 (2008/09), 225–234.

[11] E. Lehmer, *On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson*, Ann. of Math. 39 (1938), 350–360.

[12] M. Lerch, *Zur Theorie des Fermatschen Quotienten* $(a^{p-1}-1)/p = q(a)$, Math. Ann. 60 (1905), 471–490.
[13] R. McIntosh, private communication, December 2012.
[14] I. Niven, H. S. Zuckerman, and H. L. Montgomery, *An Introduction to the Theory of Numbers*, 5th ed., Wiley, New York, 1991.
[15] F. W. J. Olver et al. (eds.), *NIST Handbook of Mathematical Functions*, Cambridge Univ. Press, Cambridge, 2010.
[16] PARI/GP, http://pari.math.u-bordeaux.fr/.
[17] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer, New York, 1979.
[18] Z. H. Sun, *Congruences involving Bernoulli and Euler numbers*, J. Number Theory 128 (2008), 280–312.
[19] Z. H. Sun, *Euler numbers modulo* 2^n, Bull. Austral. Math. Soc. 82 (2010), 221–231.
[20] P. T. Young, *Congruences for Bernoulli, Euler, and Stirling numbers*, J. Number Theory 78 (1999), 204–227.

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

Karl Dilcher
Department of Mathematics and Statistics
Dalhousie University
Halifax, NS, B3H 3J5, Canada
E-mail: dilcher@mathstat.dal.ca

Received on 20.1.2013
and in revised form on 10.5.2013 (7321)