A congruence of Emma Lehmer related to Euler numbers

Karl Dilcher

Dalhousie University, Halifax

CMS Winter Meeting, Montréal, December, 2012

Joint work with

John B. Cosgrave

Dublin, Ireland

1. Introduction

Since $\{1, 2, \ldots, p-1\}$ forms a reduced residue system mod p (an odd prime), so does $\{1, 1/2, \ldots, 1/(p-1)\}$, and therefore we have

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

1. Introduction

Since $\{1, 2, \ldots, p-1\}$ forms a reduced residue system mod p (an odd prime), so does $\{1, 1/2, \ldots, 1/(p-1)\}$, and therefore we have

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

What can be said about *partial* sums?

1. Introduction

Since $\{1, 2, \dots, p-1\}$ forms a reduced residue system mod p (an odd prime), so does $\{1, 1/2, \dots, 1/(p-1)\}$, and therefore we have

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

What can be said about *partial* sums?
Eisenstein (1850) showed

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

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

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

This was later extended in various directions, among them:

(1) Modulo higher powers of p, e.g., (Emma Lehmer, 1938)

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

This was later extended in various directions, among them:

(1) Modulo higher powers of p, e.g., (Emma Lehmer, 1938)

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

(2) Different ranges, e.g.,

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

This was later extended in various directions, among them:

(1) Modulo higher powers of p, e.g., (Emma Lehmer, 1938)

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

(2) Different ranges, e.g.,

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

Typically there exist explicit expressions for such congruences for sums of length $\lfloor \frac{p}{2} \rfloor$, $\lfloor \frac{p}{3} \rfloor$, $\lfloor \frac{p}{4} \rfloor$, and $\lfloor \frac{p}{6} \rfloor$.

Reason: Bernoulli polynomials are usually involved.

(3) Reciprocals of squares, etc.; e.g., (E. Lehmer, 1938)

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

(3) Reciprocals of squares, etc.; e.g., (E. Lehmer, 1938)

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

for primes $p \geq 5$, where E_n is the nth Euler number (see later).

(3) Reciprocals of squares, etc.; e.g., (E. Lehmer, 1938)

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

for primes $p \geq 5$, where E_n is the nth Euler number (see later).

Why are we interested in such congruences?

(3) Reciprocals of squares, etc.; e.g., (E. Lehmer, 1938)

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

for primes $p \geq 5$, where E_n is the nth Euler number (see later).

Why are we interested in such congruences?

(1) Historical reason: Related to 1st case of Fermat's Last Theorem.

(3) Reciprocals of squares, etc.; e.g., (E. Lehmer, 1938)

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

for primes $p \geq 5$, where E_n is the nth Euler number (see later).

Why are we interested in such congruences?

(1) Historical reason: Related to 1st case of Fermat's Last Theorem.

Emma Lehmer (1938) derived criteria involving such congruences, building on work of Wieferich, Mirimanoff, and Vandiver.

Before Lehmer, similar congruences were derived by J.W.L. Glaisher and others.

(2) More recently: A mod p^3 extension of a theorem of Gauss:

Let p and a be such that $p \equiv 1 \pmod 4$, $p = a^2 + b^2, a \equiv 1 \pmod 4$. Then

$$\binom{\frac{p-1}{2}}{\frac{p-1}{4}} \equiv 2a \pmod p.$$

(Gauss, 1828).

(2) More recently: A mod p^3 extension of a theorem of Gauss:

Let p and a be such that $p \equiv 1 \pmod 4$,
$p = a^2 + b^2, a \equiv 1 \pmod 4$. Then

$$\binom{\frac{p-1}{2}}{\frac{p-1}{4}} \equiv 2a \pmod p.$$

(Gauss, 1828). Extended by Chowla, Dwork, and Evans (1986):

$$\binom{\frac{p-1}{2}}{\frac{p-1}{4}} \equiv \left(2a - \frac{p}{2a}\right)\left(1 + \frac{1}{2}pq_p(2)\right) \pmod{p^2},$$

and further by John Cosgrave and KD (2010):

$$\binom{\frac{p-1}{2}}{\frac{p-1}{4}} \equiv \left(2a - \frac{p}{2a} - \frac{p^2}{8a^3}\right) \times \left(1 + \tfrac{1}{2}pq_p(2) + \tfrac{1}{8}p^2\left(2E_{p-3} - q_p(2)^2\right)\right) \pmod{p^3}.$$

E_n is again the nth Euler number (see below).

In the proof of this last extension, numerous congruences of "Lehmer type" were needed.

2. Lehmer's congruence

Recall Emma Lehmer's congruence: for primes $p \geq 5$,

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

2. Lehmer's congruence

Recall Emma Lehmer's congruence: for primes $p \geq 5$,

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

where E_n is the nth Euler number defined by

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

2. Lehmer's congruence

Recall Emma Lehmer's congruence: for primes $p \geq 5$,

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

where E_n is the nth Euler number defined by

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

Euler numbers are integers, and the first few are

$E_0 = 1$, $E_2 = -1$, $E_4 = 5$, $E_6 = -61$, and $E_{2j+1} = 0$ for $j \geq 0$.

This congruence,

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

was extended to prime powers by Cai, Fu and Zhou (2007): for odd primes p and integers $\alpha\geq 1$,

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

This congruence,

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

was extended to prime powers by Cai, Fu and Zhou (2007): for odd primes p and integers $\alpha \geq 1$,

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

There's no obvious extension to arbitrary odd moduli.

This congruence,

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

was extended to prime powers by Cai, Fu and Zhou (2007): for odd primes p and integers $\alpha\geq 1$,

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

There's no obvious extension to arbitrary odd moduli.

First objective of this talk: To find such an extension.

3. Extension to arbitrary odd moduli

Recall: Euler numbers are defined by

$$\frac{2}{e^t + e^{-t}} = \sum_{n=0}^{\infty} \frac{E_n}{n!} t^n.$$

Odd-index Euler numbers are 0; first few even-index ones are $1, -1, 5, -61, 1385, -50521$.

3. Extension to arbitrary odd moduli

Recall: Euler numbers are defined by

$$\frac{2}{e^t + e^{-t}} = \sum_{n=0}^{\infty} \frac{E_n}{n!} t^n.$$

Odd-index Euler numbers are 0; first few even-index ones are $1, -1, 5, -61, 1385, -50521$.

An important property is the *Kummer congruence*:
for $k \geq 1$ and prime $p \geq 3$,

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

3. Extension to arbitrary odd moduli

Recall: Euler numbers are defined by

$$\frac{2}{e^t + e^{-t}} = \sum_{n=0}^{\infty} \frac{E_n}{n!} t^n.$$

Odd-index Euler numbers are 0; first few even-index ones are $1, -1, 5, -61, 1385, -50521$.

An important property is the *Kummer congruence*:
for $k \geq 1$ and prime $p \geq 3$,

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

Numerous generalizations and extensions are known.

We'll extend this to arbitrary odd moduli.

We say an integer n is $(k+1)$*th-power free* if no prime power higher than the kth power divides n.

This generalizes the concept of a square-free integer.

We say an integer n is $(k+1)$*th-power free* if no prime power higher than the kth power divides n.

This generalizes the concept of a square-free integer.

Lemma 1

Let $k \geq 1$ and $n \geq 1$ an odd $(k+1)$th-power free integer. Then

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

We say an integer n is $(k+1)$*th-power free* if no prime power higher than the kth power divides n.

This generalizes the concept of a square-free integer.

Lemma 1

Let $k \geq 1$ and $n \geq 1$ an odd $(k+1)$th-power free integer. Then

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

Method of proof: Use the congruence

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

valid for arbitrary integers $m \geq 1$ and odd integers $n \geq 1$. (Carlitz, 1954).

Then use the following extension of Euler's theorem:

Lemma 2

Let $n, k \in \mathbb{N}$. Then

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

iff n is a $(k+1)$th-power free integer.

Then use the following extension of Euler's theorem:

Lemma 2

Let $n, k \in \mathbb{N}$. Then

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

iff n is a $(k+1)$th-power free integer.

Proof is elementary and uses the Chinese Remainder Theorem.

For the main result we need the following function of n. With

$$n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$$

define $A(n) \in \mathbb{N}$ by $A(n) = 1$ when $r = 1$ and for $r \geq 2$,

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

For the main result we need the following function of n. With

$$n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$$

define $A(n) \in \mathbb{N}$ by $A(n) = 1$ when $r = 1$ and for $r \geq 2$,

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

Theorem 3

Let $n \in \mathbb{N}$ be odd. Then

$$\sum_{\substack{j=1 \\ (j,n)=1}}^{\lfloor n/4 \rfloor} \frac{1}{j^2} \equiv \begin{cases} (-1)^{\frac{n-1}{2}} 4A(n) E_{\varphi(n)-2} \pmod{n}, & 3 \nmid n, \\ (-1)^{\frac{n-1}{2}} 4A(n) E_{\varphi(n)-2} \pmod{n/3}, & n \equiv 0 \ (9), \\ (-1)^{\frac{n-1}{2}} \frac{40}{9} A(\frac{n}{3}) E_{\varphi(n)-2} \pmod{n/3}, & n \equiv \pm 3 \ (9). \end{cases}$$

Outline of proof:

- For each prime power $p^\alpha \mid n$, divide $\lfloor \frac{n}{4} \rfloor$ by p^α with remainder.
- Use inclusion/exclusion (via the Möbius function).
- Use the (known) congruence for prime powers.
- Use the extended Kummer congruence for Euler numbers.
- Combine everything with the Chinese Remainder Theorem.
- Particular care needs to be taken with powers of 3.

Can we have

$$S_4 := \sum_{\substack{j=1 \\ (j,n)=1}}^{\lfloor n/4 \rfloor} \frac{1}{j^2} \equiv 0 \pmod{n}?$$

Can we have

$$S_4 := \sum_{\substack{j=1 \\ (j,n)=1}}^{\lfloor n/4 \rfloor} \frac{1}{j^2} \equiv 0 \pmod{n}?$$

Yes! This happens for prime moduli 149, 241, and several others (see later).

Can we have

$$S_4 := \sum_{\substack{j=1 \\ (j,n)=1}}^{\lfloor n/4 \rfloor} \frac{1}{j^2} \equiv 0 \pmod{n}?$$

Yes! This happens for prime moduli 149, 241, and several others (see later).

Reason: $E_{p-3} \equiv 0 \pmod{p}$ for $p = 149$, $p = 241, \ldots$.

Can we have

$$S_4 := \sum_{\substack{j=1 \\ (j,n)=1}}^{\lfloor n/4 \rfloor} \frac{1}{j^2} \equiv 0 \pmod{n}?$$

Yes! This happens for prime moduli 149, 241, and several others (see later).

Reason: $E_{p-3} \equiv 0 \pmod{p}$ for $p = 149$, $p = 241, \ldots$.

Looking at the theorem:

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

Can we have $A(n) \equiv 0 \pmod{n}$?

Theorem 4

If for odd $n \in \mathbb{N}$ *we have* $A(n) \equiv 0 \pmod{n}$ *then* $3 \mid n$ *but* $9 \nmid n$.

Theorem 4

If for odd $n \in \mathbb{N}$ *we have* $A(n) \equiv 0 \pmod{n}$ *then* $3 \mid n$ *but* $9 \nmid n$.

For a proof, we need the following two lemmas.

Lemma 5

For an odd $n \in \mathbb{N}$ *we have* $A(n) \equiv 0 \pmod{n}$ *iff*

$$\prod_{\substack{i=1 \\ i \neq j}}^{r} \left(p_i^2 - (-1)^{(p_i-1)/2} \right) \equiv 0 \pmod{p_j^{\alpha_j}} \qquad \textit{for all} \quad j = 1, \ldots, r$$

unless $n \equiv \pm 3 \pmod{9}$.

Theorem 4

If for odd $n \in \mathbb{N}$ we have $A(n) \equiv 0 \pmod{n}$ then $3 \mid n$ but $9 \nmid n$.

For a proof, we need the following two lemmas.

Lemma 5

For an odd $n \in \mathbb{N}$ we have $A(n) \equiv 0 \pmod{n}$ iff

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

unless $n \equiv \pm 3 \pmod{9}$.

Sketch of proof:

- Consider congruences $\pmod{p_j^{\alpha_j}}$ separately.
- Euler's generalization of Fermat's Little Theorem.
- Count/estimate exponents of p_j.

Lemma 6

Suppose that $n \not\equiv \pm 3 \pmod 9$ *and* $A(n) \equiv 0 \pmod n$*.*
Then n *has two prime factors* $p < q$ *with*
$p \equiv 3 \pmod 4$, $q \equiv 1 \pmod 4$, *and*

$$p^2 + 1 \equiv 0 \pmod q,$$
$$q^2 - 1 \equiv 0 \pmod p.$$

Lemma 6

Suppose that $n \not\equiv \pm 3 \pmod 9$ *and* $A(n) \equiv 0 \pmod n$*.*
Then n *has two prime factors* $p < q$ *with*
$p \equiv 3 \pmod 4$, $q \equiv 1 \pmod 4$, *and*

$$p^2 + 1 \equiv 0 \pmod q,$$
$$q^2 - 1 \equiv 0 \pmod p.$$

This follows from previous lemma, using quadratic residues.

Lemma 6

Suppose that $n \not\equiv \pm 3 \pmod 9$ *and* $A(n) \equiv 0 \pmod n$*. Then* n *has two prime factors* $p < q$ *with* $p \equiv 3 \pmod 4$*,* $q \equiv 1 \pmod 4$*, and*

$$\begin{aligned} p^2 + 1 &\equiv 0 \pmod q, \\ q^2 - 1 &\equiv 0 \pmod p. \end{aligned}$$

This follows from previous lemma, using quadratic residues.

The function $A(n)$ has other interesting properties; see later.

Lemma 6

Suppose that $n \not\equiv \pm 3 \pmod 9$ *and* $A(n) \equiv 0 \pmod n$*.*
Then n *has two prime factors* $p < q$ *with*
$p \equiv 3 \pmod 4$*,* $q \equiv 1 \pmod 4$*, and*

$$\begin{aligned} p^2 + 1 &\equiv 0 \pmod q, \\ q^2 - 1 &\equiv 0 \pmod p. \end{aligned}$$

This follows from previous lemma, using quadratic residues.

The function $A(n)$ has other interesting properties; see later.

The following result shows that this is impossible.
It is of interest in its own right:

Theorem 7

For $\delta = \pm 1$ and $\varepsilon = \pm 1$, consider the pair of congruences

$$\begin{cases} p^2 & \equiv \delta \pmod{q}, \\ q^2 & \equiv \varepsilon \pmod{p}, \end{cases}$$

in odd primes p and q.

Theorem 7

For $\delta = \pm 1$ and $\varepsilon = \pm 1$, consider the pair of congruences

$$\begin{cases} p^2 & \equiv \delta \pmod{q}, \\ q^2 & \equiv \varepsilon \pmod{p}, \end{cases}$$

in odd primes p and q. We have the following cases.

(a) *If $\delta = \varepsilon = 1$, then no solutions.*

Theorem 7

For $\delta = \pm 1$ and $\varepsilon = \pm 1$, consider the pair of congruences

$$\begin{cases} p^2 & \equiv \delta \pmod{q}, \\ q^2 & \equiv \varepsilon \pmod{p}, \end{cases}$$

in odd primes p and q. We have the following cases.

(a) *If $\delta = \varepsilon = 1$, then no solutions.*

(b) *If $\delta = -1, \varepsilon = 1$, then $(p, q) = (3, 5)$ is the only solution.*

Theorem 7

For $\delta = \pm 1$ and $\varepsilon = \pm 1$, consider the pair of congruences

$$\begin{cases} p^2 & \equiv \delta \pmod{q}, \\ q^2 & \equiv \varepsilon \pmod{p}, \end{cases}$$

in odd primes p and q. We have the following cases.

(a) *If $\delta = \varepsilon = 1$, then no solutions.*

(b) *If $\delta = -1, \varepsilon = 1$, then $(p, q) = (3, 5)$ is the only solution.*

(c) *If $\delta = \varepsilon = -1$, then the only solutions are*
$(p, q) = (F_n, F_{n+2})$, $n = 1, 2, \ldots$,
provided both Fibonacci number F_n, F_{n+2} are prime.

Theorem 7

For $\delta = \pm 1$ and $\varepsilon = \pm 1$, consider the pair of congruences

$$\begin{cases} p^2 \equiv \delta \pmod{q}, \\ q^2 \equiv \varepsilon \pmod{p}, \end{cases}$$

in odd primes p and q. We have the following cases.

(a) *If $\delta = \varepsilon = 1$, then no solutions.*

(b) *If $\delta = -1, \varepsilon = 1$, then $(p, q) = (3, 5)$ is the only solution.*

(c) *If $\delta = \varepsilon = -1$, then the only solutions are $(p, q) = (F_n, F_{n+2})$, $n = 1, 2, \ldots$, provided both Fibonacci number F_n, F_{n+2} are prime.*

Part (b) is the case of Lemma 6.

Theorem 7

For $\delta = \pm 1$ and $\varepsilon = \pm 1$, consider the pair of congruences

$$\begin{cases} p^2 & \equiv \delta \pmod{q}, \\ q^2 & \equiv \varepsilon \pmod{p}, \end{cases}$$

in odd primes p and q. We have the following cases.

(a) *If $\delta = \varepsilon = 1$, then no solutions.*

(b) *If $\delta = -1, \varepsilon = 1$, then $(p, q) = (3, 5)$ is the only solution.*

(c) *If $\delta = \varepsilon = -1$, then the only solutions are*
$(p, q) = (F_n, F_{n+2})$, $n = 1, 2, \ldots$,
provided both Fibonacci number F_n, F_{n+2} are prime.

Part (b) is the case of Lemma 6.

Method of proof: Pell equations and divisibility properties of generalized Lucas sequences.

4. Vanishing sums modulo n

If a prime p divides E_{2j} for some $4 \leq 2j \leq p-3$, then p is called an *E-irregular prime*, and $(p, 2j)$ is an *E-irregular pair*.

4. Vanishing sums modulo n

If a prime p divides E_{2j} for some $4 \leq 2j \leq p-3$, then p is called an *E-irregular prime*, and $(p, 2j)$ is an *E-irregular pair*.

Carlitz (1954) proved that there are infinitely many E-irregular primes.

4. Vanishing sums modulo n

If a prime p divides E_{2j} for some $4 \leq 2j \leq p-3$, then p is called an *E-irregular prime*, and $(p, 2j)$ is an *E-irregular pair*.

Carlitz (1954) proved that there are infinitely many E-irregular primes.

Definition 8

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.

4. Vanishing sums modulo n

If a prime p divides E_{2j} for some $4 \le 2j \le p-3$, then p is called an *E-irregular prime*, and $(p, 2j)$ is an *E-irregular pair*.

Carlitz (1954) proved that there are infinitely many E-irregular primes.

Definition 8

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 following E-primes are known:

$$149, \quad 241, \quad 2\,946\,901, \quad 16\,467\,631, \quad 17\,613\,227,$$
$$327\,784\,727, \quad 426\,369\,739, \quad 1\,062\,232\,319.$$

These are all up to 3×10^9. (R. McIntosh).
The first two were found by Ernvall & Metsänkylä (1978).

Recall our first main result: For odd $n \in \mathbb{N}$,

$$\sum_{\substack{j=1\\(j,n)=1}}^{\lfloor n/4\rfloor} \frac{1}{j^2} \equiv \begin{cases} (-1)^{\frac{n-1}{2}} 4A(n)E_{\varphi(n)-2} \pmod{n}, & 3 \nmid n, \\ (-1)^{\frac{n-1}{2}} 4A(n)E_{\varphi(n)-2} \pmod{n/3}, & n \equiv 0\ (9), \\ (-1)^{\frac{n-1}{2}} \frac{40}{9} A(\frac{n}{3})E_{\varphi(n)-2} \pmod{n/3}, & n \equiv \pm 3\ (9). \end{cases}$$

When does the LHS vanish (mod n), resp. (mod $n/3$)?

Consider some tables:

n	factored	n	factored
149	149	4344989	$11^2 \cdot 149 \cdot 241$
241	241	4488625	$5^3 \cdot 149 \cdot 241$
745	$5 \cdot 149$	5013041	$11 \cdot 31 \cdot 61 \cdot 241$
1205	$5 \cdot 241$	6643165	$5 \cdot 37 \cdot 149 \cdot 241$
2651	$11 \cdot 241$	8894105	$5 \cdot 11^2 \cdot 61 \cdot 241$
3725	$5^2 \cdot 149$	874975	$5^2 \cdot 11 \cdot 149 \cdot 241$
5513	$37 \cdot 149$	14614963	$11 \cdot 37 \cdot 149 \cdot 241$
13255	$5 \cdot 11 \cdot 241$	14734505	$5 \cdot 2946901$
27565	$5 \cdot 37 \cdot 149$	16467631	16467631
29161	$11^2 \cdot 241$	17613227	17613227
35909	$149 \cdot 241$	18959207	$19 \cdot 37 \cdot 149 \cdot 181$
...	...		

Table 1: Odd $n \leq 2 \cdot 10^7$, $3 \nmid n$, for which $S_4(n) \equiv 0 \pmod{n}$ (partial list).

n	factored	n	factored
45	$3^2 \cdot 5$	4366197	$3^3 \cdot 11 \cdot 61 \cdot 241$
1341	$3^2 \cdot 149$	4713615	$3^2 \cdot 5 \cdot 19 \cdot 37 \cdot 149$
2169	$3^2 \cdot 241$	4847715	$3^3 \cdot 5 \cdot 149 \cdot 241$
6705	$3^2 \cdot 5 \cdot 149$	6202125	$3^2 \cdot 5^3 \cdot 37 \cdot 149$
10845	$3^2 \cdot 5 \cdot 241$	6561225	$3^2 \cdot 5^2 \cdot 11^2 \cdot 241$
20115	$3^3 \cdot 5 \cdot 149$	6698295	$3^5 \cdot 5 \cdot 37 \cdot 149$
23859	$3^2 \cdot 11 \cdot 241$	7276995	$3^2 \cdot 5 \cdot 11 \cdot 61 \cdot 241$
32535	$3^3 \cdot 5 \cdot 241$	8079525	$3^2 \cdot 5^2 \cdot 149 \cdot 241$
33525	$3^2 \cdot 5^2 \cdot 149$	8484507	$3^4 \cdot 19 \cdot 37 \cdot 149$
49617	$3^2 \cdot 37 \cdot 149$	10664973	$3^3 \cdot 11 \cdot 149 \cdot 241$
54225	$3^2 \cdot 5^2 \cdot 241$	11163825	$3^4 \cdot 5^2 \cdot 37 \cdot 149$
100575	$3^3 \cdot 5^2 \cdot 149$	11957697	$3^2 \cdot 37 \cdot 149 \cdot 241$
...	...	14140845	$3^3 \cdot 5 \cdot 19 \cdot 37 \cdot 149$

Table 2: Odd n, $9 \mid n$, for which $S_4(n) \equiv 0 \pmod{\frac{n}{3}}$ (partial list).

n	factored	n	factored
3	3	2693175	$3 \cdot 5^2 \cdot 149 \cdot 241$
15	$3 \cdot 5$	3985899	$3 \cdot 37 \cdot 149 \cdot 241$
447	$3 \cdot 149$	5336463	$3 \cdot 11^2 \cdot 61 \cdot 241$
723	$3 \cdot 241$	5924985	$3 \cdot 5 \cdot 11 \cdot 149 \cdot 241$
2235	$3 \cdot 5 \cdot 149$	7856025	$3 \cdot 5^2 \cdot 19 \cdot 37 \cdot 149$
3615	$3 \cdot 5 \cdot 241$	8840703	$3 \cdot 2946901$
7953	$3 \cdot 11 \cdot 241$	12128325	$3 \cdot 5^2 \cdot 11 \cdot 61 \cdot 241$
11175	$3 \cdot 5^2 \cdot 149$	13034967	$3 \cdot 11^2 \cdot 149 \cdot 241$
16539	$3 \cdot 37 \cdot 149$	13465875	$3 \cdot 5^3 \cdot 149 \cdot 241$
18075	$3 \cdot 5^2 \cdot 241$	15039123	$3 \cdot 11 \cdot 31 \cdot 61 \cdot 241$
39765	$3 \cdot 5 \cdot 11 \cdot 241$	19929495	$3 \cdot 5 \cdot 37 \cdot 149 \cdot 241$
$\dots$	$\dots$		

Table 3: Odd $n \leq 2 \cdot 10^7$, $n \equiv \pm 3 \pmod 9$, for which $S_4(n) \equiv 0 \pmod{\frac{n}{3}}$ (partial list).

The following confirms our observations:

Corollary 9

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.

The following confirms our observations:

Corollary 9

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.*

The following confirms our observations:

Corollary 9

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.

The proof is based on
- $A(n) \not\equiv 0 \pmod{n}$ (resp. $\not\equiv 0 \pmod{n/3}$);
- Kummer's congruences for E_n.

The following confirms our observations:

Corollary 9

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.

The proof is based on

- $A(n) \not\equiv 0 \pmod{n}$ (resp. $\not\equiv 0 \pmod{n/3}$);
- Kummer's congruences for E_n.

For simplicity, we will restrict our attention to $3 \nmid n$ from here on.

The following confirms our observations:

Corollary 9

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.*

The proof is based on

- $A(n) \not\equiv 0 \pmod{n}$ (resp. $\not\equiv 0 \pmod{n/3}$);
- Kummer's congruences for E_n.

For simplicity, we will restrict our attention to $3 \nmid n$ from here on.

Let's look at the first table again:

n	factored	n	factored
149	149	4344989	$11^2 \cdot 149 \cdot 241$
241	241	4488625	$5^3 \cdot 149 \cdot 241$
745	$5 \cdot 149$	5013041	$11 \cdot 31 \cdot 61 \cdot 241$
1205	$5 \cdot 241$	6643165	$5 \cdot 37 \cdot 149 \cdot 241$
2651	$11 \cdot 241$	8894105	$5 \cdot 11^2 \cdot 61 \cdot 241$
3725	$5^2 \cdot 149$	874975	$5^2 \cdot 11 \cdot 149 \cdot 241$
5513	$37 \cdot 149$	14614963	$11 \cdot 37 \cdot 149 \cdot 241$
13255	$5 \cdot 11 \cdot 241$	14734505	$5 \cdot 2946901$
27565	$5 \cdot 37 \cdot 149$	16467631	16467631
29161	$11^2 \cdot 241$	17613227	17613227
35909	$149 \cdot 241$	18959207	$19 \cdot 37 \cdot 149 \cdot 181$
...	...		

What determines the other factors?

n	factored	n	factored
149	149	4344989	$11^2 \cdot 149 \cdot 241$
241	241	4488625	$5^3 \cdot 149 \cdot 241$
745	$5 \cdot 149$	5013041	$11 \cdot 31 \cdot 61 \cdot 241$
1205	$5 \cdot 241$	6643165	$5 \cdot 37 \cdot 149 \cdot 241$
2651	$11 \cdot 241$	8894105	$5 \cdot 11^2 \cdot 61 \cdot 241$
3725	$5^2 \cdot 149$	874975	$5^2 \cdot 11 \cdot 149 \cdot 241$
5513	$37 \cdot 149$	14614963	$11 \cdot 37 \cdot 149 \cdot 241$
13255	$5 \cdot 11 \cdot 241$	14734505	$5 \cdot 2946901$
27565	$5 \cdot 37 \cdot 149$	16467631	16467631
29161	$11^2 \cdot 241$	17613227	17613227
35909	$149 \cdot 241$	18959207	$19 \cdot 37 \cdot 149 \cdot 181$
...	...		

What determines the other factors? We have with

- 149: 5, 19, 37, 181;
- 241: 5, 11, 61,

in various combinations and powers.

Key to the solution lies in considering the table

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	$2^3 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 19 \cdot 37 \cdot 47 \cdot 5689$

Table 4: The first three *E*-primes

Key to the solution lies in considering the table

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	$2^3 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 19 \cdot 37 \cdot 47 \cdot 5689$

Table 4: The first three *E*-primes

Note that 5 and 37 occur with 149, and 5 and 11 with 241.

Key to the solution lies in considering the table

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	$2^3 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 19 \cdot 37 \cdot 47 \cdot 5689$

Table 4: The first three E-primes

Note that 5 and 37 occur with 149, and 5 and 11 with 241.

But what about the others?

Key to the solution lies in considering the table

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	$2^3 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 19 \cdot 37 \cdot 47 \cdot 5689$

Table 4: The first three E-primes

Note that 5 and 37 occur with 149, and 5 and 11 with 241.

But what about the others? Note further that
$19 \mid 37^2 - 1 \quad \text{and} \quad 61 \mid 11^2 + 1.$

Key to the solution lies in considering the table

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	$2^3 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 19 \cdot 37 \cdot 47 \cdot 5689$

Table 4: The first three E-primes

Note that 5 and 37 occur with 149, and 5 and 11 with 241.

But what about the others? Note further that
$19 \mid 37^2 - 1 \quad \text{and} \quad 61 \mid 11^2 + 1.$

These are instances of the following result:

Denote, for a prime p,

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

Let p_j denote an odd prime.

Denote, for a prime p,

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

Let p_j denote an odd prime.

Theorem 10

Let $n = p_1^{\alpha_1} \dots p_r^{\alpha_r} p_{r+1} \dots p_{r+s}$, where $s \geq 1$ and $p_{r+1}, \dots, p_{r+s}$ are distinct E-primes.
If $3 \nmid n$, then $S_4(n) \equiv 0 \pmod{n}$ if and only if

$$1 \leq \alpha_j \leq \nu_{p_j} \left(\prod_{i=1}^{r+s} \left(p_i^2 - (-1)^{(p_i-1)/2} \right) \right), \quad j = 1, \dots, r.$$

Note: If $r = 0$, we consider the condition to be vacuously satisfied.

Examples.

(1) Consider the smallest E-prime 149. Note that

$$\begin{aligned} 149^2 - 1 &= 2^3 \cdot 3 \cdot 5^2 \cdot 37, \\ 37^2 - 1 &= 2^2 \cdot 3^2 \cdot 19, \\ 19^2 + 1 &= 2 \cdot 181. \end{aligned}$$

If $n = 149 \cdot 37 \cdot 19 \cdot 181$, then $S_4(n) \equiv 0 \pmod{n}$.

Examples.

(1) Consider the smallest E-prime 149. Note that

$$\begin{aligned} 149^2-1 &= 2^3\cdot 3\cdot 5^2\cdot 37,\\ 37^2-1 &= 2^2\cdot 3^2\cdot 19,\\ 19^2+1 &= 2\cdot 181. \end{aligned}$$

If $n = 149\cdot 37\cdot 19\cdot 181$, then $S_4(n)\equiv 0 \pmod{n}$.

(2) Further note that

$$181^2-1 = 2^3\cdot 3^2\cdot 5\cdot 7\cdot 13,$$
$$5^2-1 = 2^3\cdot 3,\quad 7^2+1 = 2\cdot 5^2,\quad 13^2-1 = 2^3\cdot 3\cdot 7.$$

Then the theorem 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, $3\nmid n$, having $n = 149$ as sole E-prime factor, which satisfies $S_4(n)\equiv 0 \pmod{n}$.

5. Even Moduli n

When n is even, the situation is very different; the cases $n \equiv 0 \pmod 4$ and $n \equiv 2 \pmod 4$ are also fundamentally different.

5. Even Moduli n

When n is even, the situation is very different; the cases $n \equiv 0 \pmod{4}$ and $n \equiv 2 \pmod{4}$ are also fundamentally different.

Theorem 11

Let $n = 4m$, where $m \geq 1$. 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 $S_4(n) \equiv 0 \pmod{n}$.

5. Even Moduli n

When n is even, the situation is very different; the cases $n \equiv 0 \pmod{4}$ and $n \equiv 2 \pmod{4}$ are also fundamentally different.

Theorem 11

Let $n = 4m$, where $m \geq 1$. 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 $S_4(n) \equiv 0 \pmod{n}$.

Proof is based on the following congruences (for $m \geq 2$):

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

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

The case $n \equiv 2 \pmod 4$ is very different from the first case.

Theorem 12

Let m be an odd positive integer, $3 \nmid m$. Then

$$S_4(2m) \equiv -\frac{1}{4} S_4(m) \pmod{m}.$$

The case $n \equiv 2 \pmod 4$ is very different from the first case.

Theorem 12

Let m be an odd positive integer, $3 \nmid m$. Then

$$S_4(2m) \equiv -\frac{1}{4} S_4(m) \pmod{m}.$$

There are analogous results for the case $3 \mid n$.

Thank you – Merci