Sums of reciprocals modulo composite integers

Karl Dilcher

Dalhousie University, Halifax

CNTA Lethbridge, June, 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 $\{1, 2, \ldots, p-1\}$ 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?
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 lenght $\lfloor \frac{p}{2} \rfloor$, $\lfloor \frac{p}{3} \rfloor$, $\lfloor \frac{p}{4} \rfloor$, and $\lfloor \frac{p}{6} \rfloor$.

Reason: Bernoulli polynomials are usually involved.

Why are we interested in such congruences?

Why are we interested in such congruences?

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

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.

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.

Criteria are quoted in Ribenboim's "13 Lectures on Fermat's Last Theorem" (1979).

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

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.

Criteria are quoted in Ribenboim's "13 Lectures on Fermat's Last Theorem" (1979).

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).

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):

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

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):

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

and further by John Cosgrave and KD (2010):

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

Here E_n denotes the nth Euler number (see below).

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

The congruence

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

is a special case of a sum over an arithmetic progression:

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

valid for primes $p > 3$ (Emma Lehmer, 1938).

The congruence

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

is a special case of a sum over an arithmetic progression:

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

valid for primes $p > 3$ (Emma Lehmer, 1938).

This is one of a set of 4 such congruences, with a 5th one just obtained by Kuzumaki and Urbanowicz (preprint, 2012).

The congruence

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

is a special case of a sum over an arithmetic progression:

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

valid for primes $p > 3$ (Emma Lehmer, 1938).

This is one of a set of 4 such congruences, with a 5th one just obtained by Kuzumaki and Urbanowicz (preprint, 2012).

First goal of this talk:

Study extensions of these to composite moduli.

2. Composite Moduli

Congruences modulo *composite* integers first obtained independently by H. F. Baker and M. Lerch (1906).

However, it appears that the first composite analogue of a “Lehmer type" congruence was only published in 2002 (T. Cai):

2. Composite Moduli

Congruences modulo *composite* integers first obtained independently by H. F. Baker and M. Lerch (1906).

However, it appears that the first composite analogue of a “Lehmer type" congruence was only published in 2002 (T. Cai): For any odd $n > 1$,

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

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

$$q_n(a) := \frac{a^{\varphi(n)} - 1}{n} \qquad (\gcd(a, n) = 1, n > 1).$$

3. Interlude: Euler quotients

First introduced and studied by Lerch (1905).

Further properties later by Agoh, KD, and Skula (1997), and by Cao and Pan (2009).

3. Interlude: Euler quotients

First introduced and studied by Lerch (1905).

Further properties later by Agoh, KD, and Skula (1997), and by Cao and Pan (2009).

Some important properties:

(1) $q_n(ab) \equiv q_n(a) + q_n(b) \pmod{n}$;

3. Interlude: Euler quotients

First introduced and studied by Lerch (1905).

Further properties later by Agoh, KD, and Skula (1997), and by Cao and Pan (2009).

Some important properties:

(1) $q_n(ab) \equiv q_n(a) + q_n(b) \pmod{n}$;

(2) $q_n(a + kn^\alpha) \equiv q_n(a) + \frac{1}{a}\varphi(n)kn^{\alpha-1} \pmod{n^\alpha}$;

3. Interlude: Euler quotients

First introduced and studied by Lerch (1905).

Further properties later by Agoh, KD, and Skula (1997), and by Cao and Pan (2009).

Some important properties:

(1) $q_n(ab) \equiv q_n(a) + q_n(b) \pmod{n}$;

(2) $q_n(a + kn^\alpha) \equiv q_n(a) + \frac{1}{a}\varphi(n)kn^{\alpha-1} \pmod{n^\alpha}$;

(3) $q_{mn}(a) \equiv \frac{\varphi(n)}{n} q_m a \pmod{m}$.

(with reasonable restrictions on a, b, m, n).

Another interesting property:

Theorem 1 (Baker, Lerch)

Let $a \geq 1$, $n \geq 2$ with $\gcd(a, n) = 1$. Then

$$q_n(a) \equiv \sum_{\substack{r=1 \\ \gcd(r,n)=1}}^{n-1} \frac{\lambda(r)}{r} \pmod{n},$$

where $\lambda(r)$ is the least nonnegative residue of $-r/n \pmod{a}$.

Another interesting property:

Theorem 1 (Baker, Lerch)

Let $a \geq 1$, $n \geq 2$ *with* $\gcd(a, n) = 1$. *Then*

$$q_n(a) \equiv \sum_{\substack{r=1 \\ \gcd(r,n)=1}}^{n-1} \frac{\lambda(r)}{r} \pmod{n},$$

where $\lambda(r)$ *is the least nonnegative residue of* $-r/n \pmod{a}$.

Independently published by Baker and Lerch in 1906;
Special case (a, n prime) due to Sylvester (1861).

Connections with Bernoulli numbers and polynomials:

Recall: Bernoulli numbers can be defined by

$$\frac{t}{e^t - 1} = \sum_{r=0}^{\infty} \frac{B_r}{r!} t^r.$$

Then $B_0 = 1, B_1 = -1/2, B_2 = 1/6, B_{2k+1} = 0$ for $k \geq 1$.

Connections with Bernoulli numbers and polynomials:

Recall: Bernoulli numbers can be defined by

$$\frac{t}{e^t - 1} = \sum_{r=0}^{\infty} \frac{B_r}{r!} t^r.$$

Then $B_0 = 1, B_1 = -1/2, B_2 = 1/6, B_{2k+1} = 0$ for $k \geq 1$.

The Bernoulli polynomials are then defined by

$$B_n(x) = \sum_{j=0}^{n} \binom{n}{j} B_j x^{n-j}.$$

Connections with Bernoulli numbers and polynomials:

Recall: Bernoulli numbers can be defined by

$$\frac{t}{e^t - 1} = \sum_{r=0}^{\infty} \frac{B_r}{r!} t^r.$$

Then $B_0 = 1, B_1 = -1/2, B_2 = 1/6, B_{2k+1} = 0$ for $k \geq 1$.

The Bernoulli polynomials are then defined by

$$B_n(x) = \sum_{j=0}^{n} \binom{n}{j} B_j x^{n-j}.$$

Key property: For integers $k \geq 1$,

$$\sum_{j=1}^{n-1} j^k = \frac{1}{k+1} \left(B_{k+1}(n) - B_{k+1} \right).$$

The following establishes the link between sums of powers (including sums of reciprocals – by Fermat's Little theorem) and Euler quotients:

Lemma 2

Let $a \geq 1$*,* $n \geq 2$ *with* $\gcd(a,n) = 1$*. Then*

$$aq_n(a) = -\frac{a^{\varphi(m)}}{mB_{\varphi(m)}} \sum_{j=1}^{a-1} \left(B_{\varphi(m)}(\frac{j}{a}) - B_{\varphi(m)} \right).$$

The following establishes the link between sums of powers (including sums of reciprocals – by Fermat's Little theorem) and Euler quotients:

Lemma 2

Let $a \geq 1$, $n \geq 2$ *with* $\gcd(a, n) = 1$. *Then*

$$aq_n(a) = -\frac{a^{\varphi(m)}}{mB_{\varphi(m)}} \sum_{j=1}^{a-1} \left(B_{\varphi(m)}(\frac{j}{a}) - B_{\varphi(m)} \right).$$

Proof: Well-known identities for Bernoulli polynomials.

Lemma extends similar result for prime n.

4. Composite Moduli (Cont'd)

The following extensions of 4 congruences of Emma Lehmer were recently obtained by Cai, Fu and Zhou (2007) and independently by Cao and Pan (2009):

For any odd $n \geq 1$ with $n \not\equiv 0 \pmod 3$ we have

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

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

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

and

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

and

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

Note: The full restriction "n odd and $n\not\equiv 0 \pmod 3$" is only needed in (4)

(1) and (3) make sense also when $n\equiv 0 \pmod 3$, and (2) makes sense for *even n*.

and

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

Note: The full restriction "n odd and $n \not\equiv 0 \pmod 3$" is only needed in (4)

(1) and (3) make sense also when $n \equiv 0 \pmod 3$, and (2) makes sense for *even n*.

Questions:
(a) For which n are (1)–(3) correct after all?

and

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

Note: The full restriction "n odd and $n \not\equiv 0 \pmod 3$" is only needed in (4)

(1) and (3) make sense also when $n \equiv 0 \pmod 3$, and (2) makes sense for *even n*.

Questions:
(a) For which n are (1)–(3) correct after all?
(b) Otherwise, what are the correct statements for (1)–(3)?

5. Congruences (1) and (3) for $3 \mid n$

Cao and Pan (2009) wrote that (3) "fails when $n = 9, 15, 27, 33, 45, 51, 69, 75, 81, 87, \ldots$".

5. Congruences (1) and (3) for $3 \mid n$

Cao and Pan (2009) wrote that (3) “fails when $n = 9, 15, 27, 33, 45, 51, 69, 75, 81, 87, \ldots$”. The following result characterizes these exceptions.

Theorem 3

For odd $n \geq 1$ with $3 \mid n$, the congruences

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

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

hold iff n has a prime divisor p with $p \equiv 1 \pmod 6$.

5. Congruences (1) and (3) for $3 \mid n$

Cao and Pan (2009) wrote that (3) “fails when $n = 9, 15, 27, 33, 45, 51, 69, 75, 81, 87, \ldots$". The following result characterizes these exceptions.

Theorem 3

For odd $n \geq 1$ with $3 \mid n$, the congruences

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

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

hold iff n has a prime divisor p with $p \equiv 1 \pmod 6$.
If n has no such prime divisor, then they hold modulo $\frac{1}{3}n^2$.

Idea of proof:

- Inclusion/exclusion principle.
- Congruences for Euler quotients.
- A deep property of Bernoulli numbers (see below).
- The fact that $3 \mid \varphi(m)$ iff m has a prime divisor $p \equiv 1 \pmod{6}$.
- The Chinese Remainder Theorem.

The following variants/extensions of the von Staudt-Clausen theorem for Bernoulli numbers is also needed:

The following variants/extensions of the von Staudt-Clausen theorem for Bernoulli numbers is also needed:

Lemma 4 (Carlitz, 1953, 1960)

(1) For any prime p and $\beta \geq 1$ we have

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

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

The following variants/extensions of the von Staudt-Clausen theorem for Bernoulli numbers is also needed:

Lemma 4 (Carlitz, 1953, 1960)

(1) For any prime p and $\beta \geq 1$ we have

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

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

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

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

6. The Congruence (2) for even n

Cao and Pan (2009) wrote that (2) "fails when $n = 4, 8, 14, 16, 22, 28, 32, 38, 44, 46, \ldots$"

6. The Congruence (2) for even n

Cao and Pan (2009) wrote that (2) “fails when $n = 4, 8, 14, 16, 22, 28, 32, 38, 44, 46, \ldots$"
As before, we'll characterizes these exceptions.

Theorem 5

For positive integers $n \equiv \pm 2 \pmod 6$ the congruence

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

holds iff n has a prime divisor $p \equiv 1 \pmod 4$ or two distinct odd prime divisors.

6. The Congruence (2) for even n

Cao and Pan (2009) wrote that (2) "fails when $n = 4, 8, 14, 16, 22, 28, 32, 38, 44, 46, \ldots$"
As before, we'll characterizes these exceptions.

Theorem 5

For positive integers $n \equiv \pm 2 \pmod 6$ the congruence

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

holds iff n has a prime divisor $p \equiv 1 \pmod 4$ or two distinct odd prime divisors. If this condition fails, then the congruence holds

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

6. The Congruence (2) for even n

Cao and Pan (2009) wrote that (2) "fails when $n = 4, 8, 14, 16, 22, 28, 32, 38, 44, 46, \ldots$"
As before, we'll characterizes these exceptions.

Theorem 5

For positive integers $n \equiv \pm 2 \pmod 6$ the congruence

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

holds iff n has a prime divisor $p \equiv 1 \pmod 4$ or two distinct odd prime divisors. If this condition fails, then the congruence holds

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

(b) *modulo $\frac{1}{4}n^2$ when $n = 2^\alpha$, $\alpha \geq 2$.*

Outline of proof is similar to that of previous theorem.

Outline of proof is similar to that of previous theorem.

Main criterion comes from the fact 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.

A consequence: Different type of E. Lehmer's congruences:

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

valid for primes $p \geq 5$.

A consequence: Different type of E. Lehmer's congruences:

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

valid for primes $p \geq 5$.

Composite analogue:

Corollary 6

For any odd integer $n \geq 3$ we have

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

unless $3 \mid n$ and n has no prime divisor $p \equiv 1 \pmod{6}$, in which case congruence holds modulo $n/3$.

7. Another Lehmer congruence

Emma Lehmer also proved the following: for primes $p \geq 5$,

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

7. Another Lehmer congruence

Emma Lehmer also proved the following: for primes $p \geq 5$,

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

where E_n is the nth Euler number defined by

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

7. Another Lehmer congruence

Emma Lehmer also proved the following: 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 $j \geq 0$.

Lehmer's 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 $\alpha \geq 1$,

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

Lehmer's 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.

Lehmer's 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.

Goal of this part of the talk: To find such an extension.

8. Interlude: Euler numbers

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 $1, -1, 5, -61, 1385, -50521$.

8. Interlude: Euler numbers

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 $p \geq 3$,

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

8. Interlude: Euler numbers

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 7

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 7

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 8

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 8

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 again.

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 9

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

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

Can we have

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

Yes! This happens for prime moduli 149, 241, and several others.

Can we have

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

Yes! This happens for prime moduli 149, 241, and several others.

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

Can we have

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

Yes! This happens for prime moduli 149, 241, and several others.

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

Looking at the theorem:

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

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

Theorem 10

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

Theorem 10

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 11

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

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

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

Theorem 10

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 11

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

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

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 12

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 12

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 12

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.

The function $A(n)$ has other interesting properties; e.g., for which n is $A(n) \equiv \pm 1 \pmod n$?
(Work in progress).

Lemma 12

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.

The function $A(n)$ has other interesting properties; e.g., for which n is $A(n) \equiv \pm 1 \pmod n$?
(Work in progress).

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

Theorem 13

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 13

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 13

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 13

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 13

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 12.

For Part (c): How many pairs of prime F_n, F_{n+2} are there?

For Part (c): How many pairs of prime F_n, F_{n+2} are there?

33 Fibonacci numbers are known to be prime;
another 16 are probable primes.

(Computations by Williams, Dubner & Keller, several others, and most recently by H. & R. Lifschitz.)

For Part (c): How many pairs of prime F_n, F_{n+2} are there?

33 Fibonacci numbers are known to be prime;
another 16 are probable primes.

(Computations by Williams, Dubner & Keller, several others, and most recently by H. & R. Lifschitz.)

The only prime pairs F_n, F_{n+2} occur when

- $n = 5$: $(p, q) = (5, 13)$;
- $n = 11$: $(p, q) = (89, 233)$;
- $n = 431$: (p, q) have 90 and 91 decimal digits;
- $n = 569$: (p, q) both have 119 digits.

For Part (c): How many pairs of prime F_n, F_{n+2} are there?

33 Fibonacci numbers are known to be prime;
another 16 are probable primes.

(Computations by Williams, Dubner & Keller, several others, and most recently by H. & R. Lifschitz.)

The only prime pairs F_n, F_{n+2} occur when

- $n = 5$: $(p, q) = (5, 13)$;
- $n = 11$: $(p, q) = (89, 233)$;
- $n = 431$: (p, q) have 90 and 91 decimal digits;
- $n = 569$: (p, q) both have 119 digits.

If there are further solutions, then both primes will have more than 470 849 digits.

Outline of Proof of Theorem 13:

- Transform the pairs of congruences into single Pell equations.

Outline of Proof of Theorem 13:

- Transform the pairs of congruences into single Pell equations.

- Explicit solutions in terms of generalized Lucas sequences $U_n(P,Q)$, $V_n(P,Q)$ are given in a paper by J. P. Jones (2003).

Outline of Proof of Theorem 13:

- Transform the pairs of congruences into single Pell equations.

- Explicit solutions in terms of generalized Lucas sequences $U_n(P,Q)$, $V_n(P,Q)$ are given in a paper by J. P. Jones (2003).

- Use the fact that these sequences are "divisibility sequences", i.e.,

$$n \mid m \quad \Rightarrow \quad U_n(P,Q) \mid U_m(P,Q) \quad \text{and} \quad V_n(P,Q) \mid V_m(P,Q).$$

Outline of Proof of Theorem 13:

- Transform the pairs of congruences into single Pell equations.

- Explicit solutions in terms of generalized Lucas sequences $U_n(P, Q)$, $V_n(P, Q)$ are given in a paper by J. P. Jones (2003).

- Use the fact that these sequences are "divisibility sequences", i.e.,

$$n \mid m \quad \Rightarrow \quad U_n(P,Q) \mid U_m(P,Q) \quad \text{and} \quad V_n(P,Q) \mid V_m(P,Q).$$

- This shows that there are either

– no solutions, or
– just one solution (e.g., $(F_4, F_5) = (3, 5)$), or
– a class of solutions (e.g., pairs of Fibonacci primes).

Final Remark:

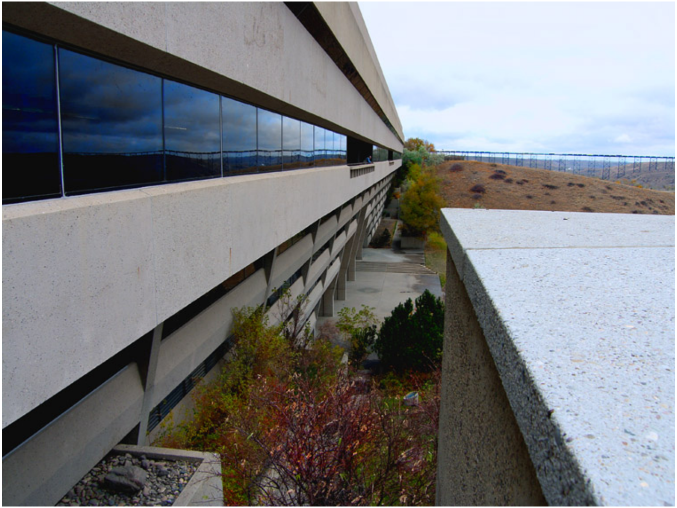
This method can be used to solve pairs of congruences

$$\begin{cases} p^2 & \equiv a \pmod{q}, \\ q^2 & \equiv b \pmod{p} \end{cases}$$

for other constants (a, b), e.g.,

- explicitly for $(\pm 2, \pm 2)$ or $(\pm 5, \pm 5)$,
- or “in principle" for any pairs (a, b).

Thank you



Lethbridge – Otto Rapp