On Multiple Zeros of Bernoulli Polynomials

Karl Dilcher

Dalhousie University, Halifax

“Special Functions in the 21st Century"
Washington, DC, April 6, 2011
Bernoulli numbers:

\[ \frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!} , \quad |t| < 2\pi. \]
Bernoulli numbers:

\[
\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}, \quad |t| < 2\pi.
\]

\[B_0 = 1, \quad B_1 = -\frac{1}{2}, \quad B_2 = \frac{1}{6}, \quad B_4 = -\frac{1}{30}, \ldots; \quad B_{2n+1} = 0 \text{ for } n \geq 1.\]
Bernoulli numbers:

\[ \frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}, \quad |t| < 2\pi. \]

\[ B_0 = 1, \quad B_1 = -\frac{1}{2}, \quad B_2 = \frac{1}{6}, \quad B_4 = -\frac{1}{30}, \ldots; \quad B_{2n+1} = 0 \text{ for } n \geq 1. \]

- \( B_n \in \mathbb{Q} \) for all \( n \).

Applications in number theory: E.g., Euler's formula 
\[ \zeta(2n) = \left(-\frac{1}{2}\right)^n n^{-1} \left(\frac{2\pi}{2n}\right)^{2n} B_{2n}. \]
Bernoulli numbers:

\[
\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}, \quad |t| < 2\pi.
\]

\[B_0 = 1, \quad B_1 = -\frac{1}{2}, \quad B_2 = \frac{1}{6}, \quad B_4 = -\frac{1}{30}, \ldots; \quad B_{2n+1} = 0 \text{ for } n \geq 1.\]

- \(B_n \in \mathbb{Q}\) for all \(n\).
- Denominators are completely determined (see later).
Bernoulli numbers:

\[
\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}, \quad |t| < 2\pi.
\]

\(B_0 = 1, \ B_1 = -\frac{1}{2}, \ B_2 = \frac{1}{6}, \ B_4 = -\frac{1}{30}, \ldots; \ B_{2n+1} = 0 \text{ for } n \geq 1.\)

- \(B_n \in \mathbb{Q}\) for all \(n\).
- Denominators are completely determined (see later)
- Numerators are quite mysterious and deep.
Bernoulli numbers:

\[
\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}, \quad |t| < 2\pi.
\]

\(B_0 = 1, \ B_1 = -\frac{1}{2}, \ B_2 = \frac{1}{6}, \ B_4 = -\frac{1}{30}, \ldots; \ B_{2n+1} = 0 \text{ for } n \geq 1.\)

- \(B_n \in \mathbb{Q} \text{ for all } n.\)
- Denominators are completely determined (see later)
- Numerators are quite mysterious and deep.

Applications in number theory: E.g.,
- Euler’s formula

\[
\zeta(2n) = (-1)^{n-1} \frac{(2\pi)^{2n}}{2(2n)!} B_{2n}, \quad (n \geq 1).
\]
• Related:

\[ \zeta(1 - n) = -\frac{B_n}{n} \quad (n \geq 2). \]

(Trivial zeros of \( \zeta(s) \)).
• Related:

\[ \zeta(1 - n) = -\frac{B_n}{n} \quad (n \geq 2). \]

(Trivial zeros of \( \zeta(s) \)).

• Kummer’s Theorem:
Let \( p \) be an odd prime. If \( p \) does not divide the numerator of one of \( B_2, B_4, \ldots, B_{p-3} \), then the equation

\[ x^p + y^p = z^p \]

has no solutions in integers \( x, y, z \) satisfying \( p \nmid xyz \).
• Related:

\[ \zeta(1 - n) = -\frac{B_n}{n} \quad (n \geq 2). \]

(Trivial zeros of \( \zeta(s) \)).

• **Kummer’s Theorem:**

Let \( p \) be an odd prime. If \( p \) does not divide the numerator of one of \( B_2, B_4, \ldots, B_{p-3} \), then the equation

\[ x^p + y^p = z^p \]

has no solutions in integers \( x, y, z \) satisfying \( p \nmid xyz \).

In other words: The First Case of FLT is true.
Bernoulli polynomials:

\[
\frac{te^tx}{e^t - 1} = \sum_{n=0}^{\infty} B_n(x) \frac{t^n}{n!}, \quad |t| < 2\pi,
\]
Bernoulli polynomials:

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

or equivalently

\[
B_n(x) = \sum_{j=0}^{n} \binom{n}{j} B_j x^{n-j}.
\]
Bernoulli polynomials:

\[
\frac{te^{xt}}{e^t - 1} = \sum_{n=0}^{\infty} B_n(x) \frac{t^n}{n!}, \quad |t| < 2\pi,
\]

or equivalently

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

Obvious connection with Bernoulli numbers:

\[
B_n(0) = B_n(1) = B_n, \quad (n \geq 2)
\]
Bernoulli polynomials:

\[
\frac{te^{xt}}{e^t - 1} = \sum_{n=0}^{\infty} B_n(x) \frac{t^n}{n!}, \quad |t| < 2\pi,
\]

or equivalently

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

Obvious connection with Bernoulli numbers:

\[
B_n(0) = B_n(1) = B_n, \quad (n \geq 2)
\]

Functional equation:

\[
B_n(x + 1) - B_n(x) = nx^{n-1}.
\]
Bernoulli polynomials:

\[
\frac{te^{xt}}{e^t - 1} = \sum_{n=0}^{\infty} B_n(x) \frac{t^n}{n!}, \quad |t| < 2\pi,
\]

or equivalently

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

Obvious connection with Bernoulli numbers:

\[
B_n(0) = B_n(1) = B_n, \quad (n \geq 2)
\]

Functional equation:

\[
B_n(x + 1) - B_n(x) = nx^{n-1}.
\]

This gives rise to numerous applications; e.g.,

\[
1^n + 2^n + \ldots + x^n = \frac{1}{n+1} (B_{n+1}(x + 1) - B_{n+1}).
\]
Let $T_n(z)$ be the $n$th degree Taylor polynomial (about 0) of $\cos z$ (when $n$ is even) and of $\sin z$ (when $n$ is odd).
Let $T_n(z)$ be the $n$th degree Taylor polynomial (about $0$) of $\cos z$ (when $n$ is even) and of $\sin z$ (when $n$ is odd).

**Theorem (K.D., 1987)**

For all $z \in \mathbb{C}$ and $n \geq 2$ we have

$$\left| (-1)^{\lfloor n/2 \rfloor} \frac{(2\pi)^n}{2n!} B_n(z + \frac{1}{2}) - T_n(2\pi z) \right| < 2^{-n} \exp(4\pi \|z\|).$$
Asymptotic Behaviour

Let $T_n(z)$ be the $n$th degree Taylor polynomial (about 0) of $\cos z$ (when $n$ is even) and of $\sin z$ (when $n$ is odd).

**Theorem (K.D., 1987)**

For all $z \in \mathbb{C}$ and $n \geq 2$ we have

$$\left|(-1)^{\lfloor n/2 \rfloor} \left(\frac{2\pi}{2n!}\right)^n B_n(z + \frac{1}{2}) - T_n(2\pi z)\right| < 2^{-n} \exp(4\pi |z|).$$

**Corollary**

We have uniformly on compact subsets of $\mathbb{C}$,

$$(-1)^{k-1} \left(\frac{2\pi}{2(2k)!}\right)^{2k} B_{2k}(z) \to \cos(2\pi z),$$

$$(-1)^{k-1} \left(\frac{2\pi}{2(2k + 1)!}\right)^{2k+1} B_{2k+1}(z) \to \sin(2\pi z).$$
As a consequence, the real zeros of the Bernoulli polynomials converge to the zeros of cos(2\pi z), resp. sin(2\pi z).

This had been known before (Lense, 1934; Inkeri, 1959). It also gives an indication (though not a proof) that the complex zeros behave like those of the polynomials T_n(z) (studied by Szegő, 1924).

What was proven, though, is the existence of a parabolic zero-free region (K.D., 1983/88).
As a consequence, the real zeros of the Bernoulli polynomials converge to the zeros of \( \cos(2\pi z) \), resp. \( \sin(2\pi z) \).

This had been known before (Lense, 1934; Inkeri, 1959).
As a consequence, the real zeros of the Bernoulli polynomials converge to the zeros of \( \cos(2\pi z) \), resp. \( \sin(2\pi z) \).

This had been known before (Lense, 1934; Inkeri, 1959).

It also gives an indication (though not a proof) that the complex zeros behave like those of the polynomials \( T_n(z) \) (studied by Szegő, 1924).
As a consequence, the real zeros of the Bernoulli polynomials converge to the zeros of \( \cos(2\pi z) \), resp. \( \sin(2\pi z) \).

This had been known before (Lense, 1934; Inkeri, 1959).

It also gives an indication (though not a proof) that the complex zeros behave like those of the polynomials \( T_n(z) \) (studied by Szegő, 1924).

What was proven, though, is the existence of a parabolic zero-free region (K.D., 1983/88).
Figure 2: Complex Zeros of $E_n(x)$ \quad 6 \leq n \leq 83.
Why study zeros of Bernoulli polynomials?

• Because they are there;
• There are actually applications:
To show that for fixed $k \geq 2$ the diophantine equation
$$1^k + 2^k + \ldots + x^k = yz$$
has at most finitely many solutions in $x, y, z$, one needs to have
some knowledge of the zeros of the polynomial (in $x$) on the
left. But this is, essentially, a Bernoulli polynomial.

This equation, and generalizations, have been extensively
studied during the past 20 years.
Why study zeros of Bernoulli polynomials?
• Because they are there;

To show that for fixed $k \geq 2$ the diophantine equation
$1^k + 2^k + \ldots + x^k = yz$
has at most finitely many solutions in $x, y, z$, one needs to have
some knowledge of the zeros of the polynomial (in $x$) on the
left. But this is, essentially, a Bernoulli polynomial.
This equation, and generalizations, have been extensively
studied during the past 20 years.
Why study zeros of Bernoulli polynomials?
- Because they are there;
- there are actually applications:
Why study zeros of Bernoulli polynomials?

- Because they are there;
- there are actually applications:

To show that for fixed $k \geq 2$ the diophantine equation

$$1^k + 2^k + \ldots + x^k = y^z$$

has at most finitely many solutions in $x, y, z$, one needs to have some knowledge of the zeros of the polynomial (in $x$) on the left.
Why study zeros of Bernoulli polynomials?  
• Because they are there;  
• there are actually applications:

To show that for fixed $k \geq 2$ the diophantine equation

$$1^k + 2^k + \ldots + x^k = y^z$$

has at most finitely many solutions in $x, y, z$, one needs to have some knowledge of the zeros of the polynomial (in $x$) on the left.

But this is, essentially, a Bernoulli polynomial.
Why study zeros of Bernoulli polynomials?
- Because they are there;
- there are actually applications:

To show that for fixed $k \geq 2$ the diophantine equation

$$1^k + 2^k + \ldots + x^k = y^z$$

has at most finitely many solutions in $x, y, z$, one needs to have some knowledge of the zeros of the polynomial (in $x$) on the left.

But this is, essentially, a Bernoulli polynomial.

This equation, and generalizations, have been extensively studied during the past 20 years.
Main topic of this talk:
Can Bernoulli polynomials have multiple zeros?

Theorem (Brillhart, 1969)
\[ B_{2n}(x) \] has no multiple zeros for any \( n \geq 0 \).

Any multiple zero of \( B_{2n}(x) \) must be a zero of \( x^2 - x - b \), with \( b \) a positive odd integer.

The main result is

Theorem (K.D., 2008)
\( B_{2n}(x) \) has no multiple zeros.
Main topic of this talk:
Can Bernoulli polynomials have multiple zeros?

This was partly answered by Brillhart:

**Theorem (Brillhart, 1969)**

1. \( B_{2n+1}(x) \) has no multiple zeros for any \( n \geq 0 \).
Main topic of this talk: Can Bernoulli polynomials have multiple zeros?

This was partly answered by Brillhart:

Theorem (Brillhart, 1969)

1. $B_{2n+1}(x)$ has no multiple zeros for any $n \geq 0$.
2. Any multiple zero of $B_{2n}(x)$ must be a zero of $x^2 - x - b$, with $b$ a positive odd integer.
Main topic of this talk:
Can Bernoulli polynomials have multiple zeros?

This was partly answered by Brillhart:

Theorem (Brillhart, 1969)

1. $B_{2n+1}(x)$ has no multiple zeros for any $n \geq 0$.
2. Any multiple zero of $B_{2n}(x)$ must be a zero of $x^2 - x - b$, with $b$ a positive odd integer.

The main result is

Theorem (K.D., 2008)

$B_{2n}(x)$ has no multiple zeros.
Some other elementary properties of Bernoulli polynomials:

\[ B_n\left(\frac{1}{2}\right) = (2^{1-n} - 1)B_n, \]
\[ B'_n(x) = nB_{n-1}(x). \]
Sketch of Proof

Some other elementary properties of Bernoulli polynomials:

\[ B_n\left(\frac{1}{2}\right) = (2^{1-n} - 1) B_n, \]
\[ B'_n(x) = nB_{n-1}(x). \]

With these, a Taylor expansion now gives

\[ B_{2m}(x) = \sum_{j=0}^{m} \binom{2m}{2j} (2^{1-2j} - 1)(x - \frac{1}{2})^{2(m-j)} B_{2j}. \] (1)
Sketch of Proof

Some other elementary properties of Bernoulli polynomials:

\[ B_n\left(\frac{1}{2}\right) = (2^{1-n} - 1)B_n, \]
\[ B'_n(x) = nB_{n-1}(x). \]

With these, a Taylor expansion now gives

\[ B_{2m}(x) = \sum_{j=0}^{m} \binom{2m}{2j} (2^{1-2j} - 1)(x - \frac{1}{2})^{2(m-j)} B_{2j}. \quad (1) \]

Let \( x_b \) be a zero of \( x^2 - x - b \). Then

\[ 4(x_b - \frac{1}{2})^2 = 4x_b^2 - 4x_b + 1 = 4b + 1, \]
Some other elementary properties of Bernoulli polynomials:

\[ B_n\left(\frac{1}{2}\right) = (2^{1-n} - 1)B_n, \]
\[ B'_n(x) = nB_{n-1}(x). \]

With these, a Taylor expansion now gives

\[ B_{2m}(x) = \sum_{j=0}^{m} \binom{2m}{2j} (2^{1-2j} - 1)(x - \frac{1}{2})^{2(m-j)} B_{2j}. \quad (1) \]

Let \( x_b \) be a zero of \( x^2 - x - b \). Then

\[ 4(x_b - \frac{1}{2})^2 = 4x_b^2 - 4x_b + 1 = 4b + 1, \]

and with (1) we get

\[ 2^{2m}B_{2m}(x_b) = \sum_{j=0}^{m} \binom{2m}{2j} (4b + 1)^{m-j}(2 - 2^{2j})B_{2j}. \quad (2) \]
Main ingredients:

**Theorem (von Staudt, 1840; Clausen, 1840)**

- *A prime $p$ divides the denominator of $B_{2n}$ if and only if $p - 1 | 2n.*

Recall:

$$2^{2m} B_{2m}(x) = m \sum_{j=0}^{m} (2m^2 j)^m (4b+1)^{m-j} \binom{2m}{2j} B_j.$$
Main ingredients:

Theorem (von Staudt, 1840; Clausen, 1840)

- A prime \( p \) divides the denominator of \( B_{2n} \) if and only if \( p - 1 \mid 2n \).
- If \( p - 1 \mid 2n \), then \( pB_{2n} \equiv -1 \pmod{p} \).
Main ingredients:

Theorem (von Staudt, 1840; Clausen, 1840)

- A prime \( p \) divides the denominator of \( B_{2n} \) if and only if \( p - 1 \mid 2n \).
- If \( p - 1 \mid 2n \), then \( pB_{2n} \equiv -1 \pmod{p} \).

Fix an \( m \geq 1 \), and consider primes \( p \) with \( p - 1 \mid 2m \).
Main ingredients:

Theorem (von Staudt, 1840; Clausen, 1840)

- A prime \( p \) divides the denominator of \( B_{2n} \) if and only if \( p - 1 \mid 2n \).
- If \( p - 1 \mid 2n \), then \( pB_{2n} \equiv -1 \) (mod \( p \)).

Fix an \( m \geq 1 \), and consider primes \( p \) with \( p - 1 \mid 2m \).

If \( p - 1 = 2m \), or if \( p - 1 < 2m \) and \( p \mid 4b + 1 \),
then easy to see: \( B_{2m}(x_b) \neq 0 \).

Recall:

\[
2^{2m}B_{2m}(x_b) = \sum_{j=0}^{m} \binom{2m}{2j} (4b + 1)^{m-j}(2 - 2^{2j})B_{2j}.
\]
Remaining case

\[ p - 1 < 2m \text{ and } p \nmid 4b + 1: \]

Set \( q := \frac{2m}{p - 1}; \) then \( q \in \mathbb{Z}, \quad 2 \leq q \leq m. \)
Remaining case

$p - 1 < 2m$ and $p \nmid 4b + 1$:

Set $q := \frac{2m}{p - 1}$; then $q \in \mathbb{Z}$, $2 \leq q \leq m$.

Multiply both sides of (2) with $p$; then

- By von Staudt - Clausen:

\[
pB_{2j} \equiv \begin{cases} 
-1 \; (\text{mod } p) & \text{for } 2j = r(p - 1), \\
0 \; (\text{mod } p) & \text{for all other } j.
\end{cases}
\]

for $r = 1, 2, \ldots, q$.
Remaining case

$p - 1 < 2m$ and $p \nmid 4b + 1$:

Set $q := \frac{2m}{p - 1}$; then $q \in \mathbb{Z}, \quad 2 \leq q \leq m$.

Multiply both sides of (2) with $p$; then

- By von Staudt - Clausen:
  \[
  pB_{2j} \equiv \begin{cases} 
    -1 \pmod{p} & \text{for } 2j = r(p - 1), \\
    0 \pmod{p} & \text{for all other } j.
  \end{cases}
  \]

- By Fermat’s Little Theorem, for $2j = r(p - 1)$,
  \[
  2 - 2^{2j} = 2 - 2^{r(p - 1)} \equiv 2 - 1 = 1 \pmod{p}.
  \]
• Since $p \nmid 4b + 1$,

$$(4b + 1)^i = \left((4b + 1)^{\frac{p-1}{2}}\right)^r \equiv \varepsilon_b^r \pmod{p},$$

where

$$\varepsilon_b = \begin{cases} 
1, & 4b + 1 \text{ quadratic residue } \pmod{p}; \\
-1, & 4b + 1 \text{ quadratic nonresidue } \pmod{p}.
\end{cases}$$
• Since \( p \nmid 4b + 1 \),

\[
(4b + 1)^i = \left( (4b + 1)^{\frac{p-1}{2}} \right)^r \equiv \varepsilon_b^r \pmod{p},
\]

where

\[
\varepsilon_b = \begin{cases} 
1, & 4b + 1 \text{ quadratic residue } \pmod{p}; \\
-1, & 4b + 1 \text{ quadratic nonresidue } \pmod{p}.
\end{cases}
\]

So (2) becomes

\[
pB_{2m}(x_b) \equiv -\varepsilon_b^q \sum_{r=1}^{q} \left( \frac{q(p - 1)}{r(p - 1)} \right) \varepsilon_b^r \pmod{p}.
\]

When \( \varepsilon_b = 1 \), sum is well-known to be \( \equiv 1 \pmod{p} \) (Hermite, 1876).
• Since \( p \nmid 4b + 1 \),

\[
(4b + 1)^j = \left( (4b + 1)^{\frac{p-1}{2}} \right)^r \equiv \varepsilon_b^r \quad (\text{mod } p),
\]

where

\[
\varepsilon_b = \begin{cases} 
1, & 4b + 1 \text{ quadratic residue } \quad (\text{mod } p); \\
-1, & 4b + 1 \text{ quadratic nonresidue } \quad (\text{mod } p).
\end{cases}
\]

So (2) becomes

\[
pB_{2m}(x_b) \equiv -\varepsilon_b^q \sum_{r=1}^{q} \left( \frac{q(p-1)}{r(p-1)} \right) \varepsilon_b^r \quad (\text{mod } p).
\]

When \( \varepsilon_b = 1 \), sum is well-known to be \( \equiv 1 \) (mod \( p \)) (Hermite, 1876). So

\[
pB_{2m}(x_b) \equiv -1 \quad (\text{mod } p),
\]

and there can be no multiple zero.
Remaining case, $\varepsilon_b = -1$: Set

$$S_p(q) := \sum_{r=1}^{q} \binom{q(p-1)}{r(p-1)} (-1)^r.$$
Remaining case, $\varepsilon_b = -1$: Set

$$S_p(q) := \sum_{r=1}^{q} \binom{q(p-1)}{r(p-1)} (-1)^r.$$ 

**Lemma**

$$S_p(q) \equiv \begin{cases} 
-1 \pmod{p}, & q \text{ odd;} \\
0 \pmod{p}, & q = k(p+1); \\
1 \pmod{p}, & q \text{ even, } q \neq k(p+1). 
\end{cases}$$
Remaining case, $\varepsilon_b = -1$: Set

$$S_p(q) := \sum_{r=1}^{q} \binom{q(p - 1)}{r(p - 1)} (-1)^r.$$ 

**Lemma**

$$S_p(q) \equiv \begin{cases} 
-1 \pmod{p}, & q \text{ odd}; \\
0 \pmod{p}, & q = k(p + 1); \\
1 \pmod{p}, & q \text{ even}, q \neq k(p + 1). 
\end{cases}$$

**Proof**: Case $q$ odd is obvious, by symmetry.
Remaining case, $\varepsilon_b = -1$: Set

$$S_p(q) := \sum_{r=1}^{q} \binom{q(p-1)}{r(p-1)} (-1)^r.$$

**Lemma**

$$S_p(q) \equiv \begin{cases} 
-1 \pmod{p}, & q \text{ odd}; \\
0 \pmod{p}, & q = k(p+1); \\
1 \pmod{p}, & q \text{ even, } q \neq k(p+1).
\end{cases}$$

**Proof**: Case $q$ odd is obvious, by symmetry. The other cases are more difficult; $(2p-2)$th roots of units are used; $S_p(q)$ is considered a linear recurrence sequence.
Lemma means:

The only case that remains open is the case $p + 1 \mid q$ and $\varepsilon_b = -1$. 
Lemma means:

The only case that remains open is the case $p + 1 \mid q$ and $\varepsilon_b = -1$.

To deal with this case, we use the fact that if $x_b$ is a multiple zero of $B_{2m}(x)$, it must be a zero of $B_{2m-1}(x)$.
Lemma means:

The only case that remains open is the case $p + 1 \mid q$ and $\varepsilon_b = -1$.

To deal with this case, we use the fact that if $x_b$ is a multiple zero of $B_{2m}(x)$, it must be a zero of $B_{2m-1}(x)$.

This is easy to exclude, using again the Lemma.
Proof of the Lemma (sketch)

With Hermite’s congruence

\[ \sum_{j=0}^{q} \binom{q(p-1)}{j(p-1)} \equiv 2 \pmod{p} \]

it is easy to see (by just adding congruences) that the Lemma is equivalent to

\[ \sum_{j=0}^{\lfloor q/2 \rfloor} \binom{q(p-1)}{2j(p-1)} \equiv \begin{cases} 1 \pmod{p} & \text{for } q \text{ odd,} \\ 2 \pmod{p} & \text{for } q \text{ even, } p+1 \nmid q, \\ 3^2 \pmod{p} & \text{for } p+1 \mid q. \end{cases} \]
The key step is the following

**Lemma**

Let $p$ be an odd prime and $\zeta$ a primitive $(2p - 2)$th root of unity. Define, for $q = 1, 2, \ldots$,

$$T_p(q) := \sum_{k=1}^{2p-2} \left(1 + \zeta^k\right)^{(p-1)q}.$$
The key step is the following

Lemma

Let $p$ be an odd prime and $\zeta$ a primitive $(2p - 2)$th root of unity. Define, for $q = 1, 2, \ldots$,

$$T_p(q) := \sum_{k=1}^{2p-2} \left( 1 + \zeta^k \right)^{(p-1)q}.$$ 

Then

$$T_p(q) = (2p - 2) \sum_{j=0}^{\lfloor q/2 \rfloor} \binom{q(p-1)}{2j(p-1)}.$$
The key step is the following

**Lemma**

Let $p$ be an odd prime and $\zeta$ a primitive $(2p - 2)$th root of unity. Define, for $q = 1, 2, \ldots$,

$$T_p(q) := \sum_{k=1}^{2p-2} \left(1 + \zeta^k\right)^{(p-1)q}.$$  

Then

$$T_p(q) = (2p - 2) \sum_{j=0}^{\lfloor q/2 \rfloor} \binom{q(p-1)}{2j(p-1)}.$$  

The proof is easy: Use a binomial expansion and change the order of summation.
By the theory of linear recurrence relations with constant coefficients:

• \{T_p(q)\}, q = 1, 2, \ldots,
• order is at most \(p - 2\);
• characteristic polynomial has \((1 + \zeta_k)^p - 1\), \(k = 1, 2, \ldots, 2p - 2\), as its roots.

This motivates the following lemma.
By the theory of linear recurrence relations with constant coefficients:

- \( \{ T_p(q) \}, \ q = 1, 2, \ldots, \) is such a sequence;
By the theory of linear recurrence relations with constant coefficients:

- \( \{ T_p(q) \} \), \( q = 1, 2, \ldots \), is such a sequence;
- order is at most \( 2p - 2 \);
By the theory of linear recurrence relations with constant coefficients:

• \( \{ T_p(q) \}, \ q = 1, 2, \ldots, \) is such a sequence;

• order is at most \( 2p - 2; \)

• characteristic polynomial has

\[
(1 + \zeta^k)^{p-1}, \quad k = 1, 2, \ldots, 2p - 2,
\]

as its roots.
By the theory of linear recurrence relations with constant coefficients:

- \( \{ T_p(q) \} \), \( q = 1, 2, \ldots \), is such a sequence;
- order is at most \( 2p - 2 \);
- characteristic polynomial has
  \[
  (1 + \zeta^k)^{p-1}, \quad k = 1, 2, \ldots, 2p - 2,
  \]
as its roots.

This motivates the following lemma.
Lemma

Let $p$ be an odd prime and $f_p(x)$ the unique monic polynomial that has $(1 + \zeta^k)^{p-1}$, $k = 1, 2, \ldots, 2p - 2$, as its roots.
Lemma

Let $p$ be an odd prime and $f_p(x)$ the unique monic polynomial that has $(1 + \zeta^k)^{p-1}$, $k = 1, 2, \ldots, 2p - 2$, as its roots. Then

$$f_p(x) \equiv x \sum_{n=0}^{2p-3} a_n x^{2p-3-n} \pmod{p},$$

Proof uses various congruences and identities for binomial coefficients and finite sums.

Karl Dilcher
On Multiple Zeros of Bernoulli Polynomials
Lemma

Let $p$ be an odd prime and $f_p(x)$ the unique monic polynomial that has $(1 + \zeta^k)^{p-1}$, $k = 1, 2, \ldots, 2p - 2$, as its roots. Then

$$f_p(x) \equiv x \sum_{n=0}^{2p-3} a_n x^{2p-3-n} \pmod{p},$$

where for $0 \leq n \leq p - 2$ we have

$$a_n \equiv \begin{cases} (m + 1)^2 \pmod{p} & \text{for } n = 2m, \\ (m + 1)(m + 2) \pmod{p} & \text{for } n = 2m + 1, \end{cases}$$

and for $p - 1 \leq n \leq 2p - 3$,

$$a_n \equiv -a_{2p-3-n} \pmod{p}.$$
Lemma

Let $p$ be an odd prime and $f_p(x)$ the unique monic polynomial that has $(1 + \zeta^k)^{p-1}$, $k = 1, 2, \ldots, 2p - 2$, as its roots. Then

$$f_p(x) \equiv x^{2p-3} \sum_{n=0}^{2p-3} a_n x^{2p-3-n} \quad (\text{mod } p),$$

where for $0 \leq n \leq p - 2$ we have

$$a_n \equiv \begin{cases} (m+1)^2 \quad (\text{mod } p) & \text{for } n = 2m, \\ (m+1)(m+2) \quad (\text{mod } p) & \text{for } n = 2m + 1, \end{cases}$$

and for $p - 1 \leq n \leq 2p - 3$,

$$a_n \equiv -a_{2p-3-n} \quad (\text{mod } p).$$

Proof uses various congruences and identities for binomial coefficients and finite sums.
The conjecture that

\[ T_p(q) \equiv \begin{cases} 
-2 \pmod{p} & \text{for } q \text{ odd}, \\
-4 \pmod{p} & \text{for } q \text{ even, } p + 1 \nmid q, \\
-3 \pmod{p} & \text{for } p + 1 | q,
\end{cases} \]

would complete the proof. We can prove this as follows:
The conjecture that

\[ T_p(q) \equiv \begin{cases} 
-2 \pmod{p} & \text{for } q \text{ odd,} \\
-4 \pmod{p} & \text{for } q \text{ even, } p + 1 \nmid q, \\
-3 \pmod{p} & \text{for } p + 1 \mid q,
\end{cases} \]

would complete the proof. We can prove this as follows:

- Verify it for all \( q \leq 2p. \)
The conjecture that

\[ T_p(q) \equiv \begin{cases} 
-2 \pmod{p} & \text{for } q \text{ odd}, \\
-4 \pmod{p} & \text{for } q \text{ even, } p + 1 \nmid q, \\
-3 \pmod{p} & \text{for } p + 1 \mid q,
\end{cases} \]

would complete the proof. We can prove this as follows:

- Verify it for all \( q \leq 2p \).
  This can be done by elementary (but tricky) manipulations of congruences for binomial coefficients.
The conjecture that

\[ T_p(q) \equiv \begin{cases} 
-2 \pmod{p} & \text{for } q \text{ odd}, \\
-4 \pmod{p} & \text{for } q \text{ even, } p + 1 \nmid q, \\
-3 \pmod{p} & \text{for } p + 1 \mid q,
\end{cases} \]

would complete the proof. We can prove this as follows:

- Verify it for all \( q \leq 2p \).

This can be done by elementary (but tricky) manipulations of congruences for binomial coefficients.

- Then show that the numbers given above satisfy the recurrence relation

\[ a_0 T_p(n) + a_1 T_p(n - 1) + \ldots + a_{2p - 3} T_p(n - 2p + 3) \equiv 0 \pmod{p} \]

for all \( n \geq 2p - 2 \), with the \( a_j \) as given in the previous Lemma.
The conjecture that

\[ T_p(q) \equiv \begin{cases} 
-2 \pmod{p} & \text{for } q \text{ odd,} \\
-4 \pmod{p} & \text{for } q \text{ even, } p + 1 \nmid q, \\
-3 \pmod{p} & \text{for } p + 1 \mid q,
\end{cases} \]

would complete the proof. We can prove this as follows:

- Verify it for all \( q \leq 2p \).
  This can be done by elementary (but tricky) manipulations of congruences for binomial coefficients.

- Then show that the numbers given above satisfy the recurrence relation

\[ a_0 T_p(n) + a_1 T_p(n - 1) + \ldots + a_{2p-3} T_p(n - 2p + 3) \equiv 0 \pmod{p} \]

for all \( n \geq 2p - 2 \), with the \( a_j \) as given in the previous Lemma. This is again elementary but tricky.
The conjecture that

\[ T_p(q) \equiv \begin{cases} 
-2 \pmod{p} & \text{for } q \text{ odd}, \\
-4 \pmod{p} & \text{for } q \text{ even, } p + 1 \nmid q, \\
-3 \pmod{p} & \text{for } p + 1 \mid q,
\end{cases} \]

would complete the proof. We can prove this as follows:

- Verify it for all \( q \leq 2p \).
  This can be done by elementary (but tricky) manipulations of congruences for binomial coefficients.

- Then show that the numbers given above satisfy the recurrence relation

\[ a_0 T_p(n) + a_1 T_p(n-1) + \ldots + a_{2p-3} T_p(n - 2p + 3) \equiv 0 \pmod{p} \]

for all \( n \geq 2p - 2 \), with the \( a_j \) as given in the previous Lemma. This is again elementary but tricky.

The proof is complete.
Thank you