VALUES OF BERNOULLI POLYNOMIALS

ANDREW GRANVILLE\textsuperscript{1} AND ZHI-WEI SUN\textsuperscript{2}

\textit{Dedicated to Emma Lehmer}

Let $B_n(t)$ be the $n$th Bernoulli polynomial. We show that $B_{p-1}(a/q) - B_{p-1} \equiv q(U_p - 1)/2p \pmod{p}$, where $U_n$ is a certain linear recurrence of order $\lfloor q/2 \rfloor$ which depends only on $a, q$ and the least positive residue of $p \pmod{q}$. This can be re-written as a sum of linear recurrence sequences of order $\leq \phi(q)/2$, and so we can recover the classical results where $\phi(q) < 2$ (for instance, $B_{p-1}(1/6) - B_{p-1} \equiv (3p - 3)/2p + (2p - 2)/p \pmod{p}$). Our results provide the first advance on the question of evaluating these polynomials when $\phi(q) > 2$, a problem posed by Emma Lehmer in 1938.

\textbf{Introduction.}

It has long been known that the $n$th Bernoulli polynomial $B_n(t)$, where

$$B_n(t) = \sum_{j=0}^{n} \binom{n}{j} B_{n-j} t^j$$

and $B_k$, the $k$th Bernoulli number, defined by the power series

$$\frac{x}{e^x - 1} = \sum_{k \geq 0} B_k \frac{x^k}{k!},$$

take 'special' values at certain rational numbers with small denominators:

\begin{align*}
(1) & \quad & B_n(1) &= B_n(0) = B_n, \quad \text{for } n \neq 1 \\
& & B_n\left(\frac{1}{2}\right) &= (2^{1-n} - 1)B_n;
\end{align*}

\textsuperscript{1}The first author is an Alfred P. Sloan Research Fellow and a Presidential Faculty Fellow. Also supported, in part, by the National Science Foundation.

\textsuperscript{2}The second author was supported by the National Natural Science Foundation of the People's Republic of China.
and for all even \( n \geq 2 \),

\[
B_n \left( \frac{1}{3} \right) = B_n \left( \frac{2}{3} \right) = \frac{1}{2} (3^{1-n} - 1)B_n,
\]

\[
B_n \left( \frac{1}{4} \right) = B_n \left( \frac{3}{4} \right) = \frac{1}{2} (4^{1-n} - 2^{1-n})B_n,
\]

\[
B_n \left( \frac{1}{6} \right) = B_n \left( \frac{5}{6} \right) = \frac{1}{2} (6^{1-n} - 3^{1-n} - 2^{1-n} + 1)B_n.
\]

It is not known if \( B_n(a/q) \) has as simple a ‘closed form’ for any other rational \( a/q \) with \( 1 \leq a \leq q - 1 \) and \( (a,q) = 1 \), though this has long been considered an interesting question.

Following work of Friedmann and Tamarkin [FT], Emma Lehmer [Lh, 1938] considered Bernoulli numbers and polynomials modulo primes and prime powers, and showed amongst other things that (1) and (2) imply

\[
(3)
\]

\[
B_{p-1} \left( \frac{1}{2} \right) - B_{p-1} = \frac{2^p - 2}{p} \quad (\text{mod } p)
\]

\[
B_{p-1} \left( \frac{1}{3} \right) - B_{p-1} = B_{p-1} \left( \frac{2}{3} \right) - B_{p-1} = \frac{1}{2} \frac{(3^p - 3)}{p} \quad (\text{mod } p)
\]

\[
B_{p-1} \left( \frac{1}{4} \right) - B_{p-1} = B_{p-1} \left( \frac{3}{4} \right) - B_{p-1} = \frac{3}{2} \frac{(2^p - 2)}{p} \quad (\text{mod } p)
\]

\[
B_{p-1} \left( \frac{1}{6} \right) - B_{p-1} = B_{p-1} \left( \frac{5}{6} \right) - B_{p-1} = \frac{1}{2} \frac{(3^p - 3)}{p} + \frac{2^p - 2}{p} \quad (\text{mod } p).
\]

The “Fermat quotients”, \((2^p - 2)/p\) and \((3^p - 3)/p\) play a central rôle in the study of the first case of Fermat’s Last Theorem (see Ribenboim’s elegant account [Ri]), and this connection with Bernoulli polynomials has recently been explored in much greater depth by Skula [Sk] (see also [Gr]).

However, until now, no progress has been made in extending the table of intriguing congruences given in (3). This is the intention here. (It should be mentioned that recent papers of H. C. Williams [W1, W2], of G. Andrews [An] as well as of the second author and his twin brother Zhi-Hong Sun [SS], each come close to doing this.)

Before stating our main result, which is of a somewhat technical nature, let’s discuss the next class of examples after (3). The two important things to note about (3) are that,

(i): We’ve evaluated \( B_{p-1}(\frac{a}{q}) - B_{p-1} \) (mod \( p \)) where \( \phi(q) = 1 \) or \( 2 \) (\( \phi \) is Euler’s totient function);

(ii): Each of the terms of the right hand side, like \( 2^p, 3^p \), are numbers taken from a first-order linear recurrence sequence \( u_{n+1} = 2u_n \) and \( u_{n+1} = 3u_n \) respectively).
This is the viewpoint we need to generalize. We shall show, for \( q > 2 \), that \( B_{p-1}(\frac{a}{q}) - B_{p-1} \pmod{p} \) is congruent to a sum of multiples of terms, each of which are numbers taken from a \( k \)-th order linear recurrence sequence with \( k \leq \phi(q)/2 \).

Thus the next class of examples are those \( q \) for which \( \phi(q) = 4 \), namely \( q = 5, 8, 10, 12 \). We shall show that, for \( 1 \leq a < q-1 \) with \((a, q) = 1\) (there being four such integers \( a \)), we have, when prime \( p \) does not divide \( q \),

\[
B_{p-1}\left(\frac{a}{5}\right) - B_{p-1} \equiv \frac{5}{4} \left\{ \left(\frac{ap}{5}\right) \frac{1}{p} F_{p-\left(\frac{a}{p}\right)} + \frac{5^{p-1} - 1}{p} \right\} \pmod{p}
\]

\[
B_{p-1}\left(\frac{a}{8}\right) - B_{p-1} \equiv \left\{ 2 \left(\frac{8}{ap}\right) \frac{1}{p} G_{p-\left(\frac{a}{p}\right)} + 4 \frac{(2^{p-1} - 1)}{p} \right\} \pmod{p}
\]

\[
B_{p-1}\left(\frac{a}{10}\right) - B_{p-1} \equiv \frac{15}{4} \left\{ \left(\frac{ap}{10}\right) \frac{1}{p} F_{p-\left(\frac{a}{p}\right)} + \frac{5}{4} \frac{5^{p-1} - 1}{p} + \frac{2(2^{p-1} - 1)}{p} \right\} \pmod{p}
\]

\[
B_{p-1}\left(\frac{a}{12}\right) - B_{p-1} \equiv 3 \left\{ \left(\frac{12}{a}\right) \frac{1}{p} H_{p-\left(\frac{a}{p}\right)} + \frac{3(2^{p-1} - 1)}{2} + \frac{3(3^{p-1} - 1)}{2} \right\} \pmod{p}
\]

where \((-\text{)}\) is the Jacobi symbol, and we define the following second-order linear recurrence sequences:

\[
\begin{align*}
F_0 &= 0, \quad F_1 = 1, \quad \text{and} \quad F_{n+2} = F_{n+1} + F_n \quad \text{for all} \quad n \geq 0 \\
G_0 &= 0, \quad G_1 = 1, \quad \text{and} \quad G_{n+2} = 2G_{n+1} + G_n \quad \text{for all} \quad n \geq 0 \\
H_0 &= 0, \quad H_1 = 1, \quad \text{and} \quad H_{n+2} = 4H_{n+1} - H_n \quad \text{for all} \quad n \geq 0.
\end{align*}
\]

\(\{F_n\}\) is, of course, the Fibonacci sequence.

In general we fix residue classes \( a \) and \( b \) \((\text{mod} \ q)\), with \((ab, q) = 1\). Then, for each divisor \( d \) of \( q \), there exists a recurrence sequence \( u_n = u_n(d, a, b) \) of order \( D = \phi(d)/2 \), with characteristic polynomial

\[
\prod_{\substack{1 \leq j \leq d/2 \\ (j, d) = 1}} \left( X - 2 + e^{2i\pi j/d} + e^{-2i\pi j/d} \right) = X^D - \sum_{i=0}^{D-1} f_i X^{D-1-i} ,
\]

so that

\[
u_{n+D} = f_0 u_{n+D-1} + f_1 u_{n+D-2} + \cdots + f_{D-1} u_n
\]

for all \( n \geq 0 \). The values of \( u_0, \cdots, u_{D-1} \) depend on \( a \) and \( b \) \((\text{mod} \ d)\) and are somewhat complicated to describe – see Section 2 for precise details.

Our main result is that, for any \((a, q) = 1, 1 \leq a \leq q\),

\[
B_{p-1}\left(\frac{a}{q}\right) - B_{p-1} \equiv \sum_{d|q} \frac{1}{2p} \left\{ u_p(d; a, b) - (\phi(d) - \mu(d)) \right\} \pmod{p}
\]
where \( b \) is the least positive residue of \( p \) (mod \( q \)) (and \( \mu \) is the Möbius function), provided prime \( p \) does not divide \( q \). Each term in the sum is a \( p \)-unit.

Our formula involves such an awkward sum of recurrence sequences though each appears "naturally" in

\[
(6) \quad \sum_{d|q} \mu \left( \frac{q}{d} \right) \left( B_{p-1} \left( \frac{a_d}{d} \right) - B_{p-1} \right) \equiv \frac{1}{2p} \left\{ u_p(q; a, b) - (\phi(q) - \mu(q)) \right\} \pmod{p}
\]

where \( a_d \) is the least positive residue of \( a \) mod \( d \). Indeed this is the formula we shall prove and then (5) is deduced by summing (6) over divisors of \( q \).

We are unable to answer the question as to whether it is possible to give such a congruence for \( B_{p-1}(\frac{a}{q}) - B_{p-1} \) involving only lower order recurrence sequences. Indeed this seems difficult, unless one can give a complete characterization of all linear recurrence sequences \( (X_n)_{n>0} \) for which \( X_p \equiv 0 \pmod{p^2} \) for all but finitely many primes \( p \). However we do not even know how to decide this for \( X_n = 2^n - 2 \).

However, it is easily shown that any sum of recurrence sequences can be written as one recurrence sequence, though of higher order. Thus (5) can be rewritten

\[
(7) \quad B_{p-1} \left( \frac{a}{q} \right) - B_{p-1} \equiv \frac{q}{2p} \left\{ U_p(q; a, b) - 1 \right\} \pmod{p}
\]

where, now, \( U_n \) has characteristic polynomial

\[
\prod_{1 \leq j \leq q/2} \left( X - 2 + e^{2i\pi j/q} + e^{-2i\pi j/q} \right).
\]

Again it is complicated to compute the values of \( U_n \) for small \( n \).

It is tempting to provide one "concrete" example for arbitrarily large \( q \). We will now completely describe \( U_p(q; a, b) \) in the case that \( a \equiv \pm b \pmod{q} \) (that is \( a \equiv \pm p \pmod{q} \)) and \( q \) is odd:

**Theorem.** If \( q \) is an odd integer \( \geq 3 \) and \( 1 < a < q \) with \( (a, q) = 1 \), then

\[
(8) \quad B_{p-1} \left( \frac{a}{q} \right) - B_{p-1} \equiv \frac{q}{2p} \left\{ x_p - 1 \right\} \pmod{p}
\]

whenever \( p \equiv \pm a \pmod{q} \) where \( \{x_n\}_{n \geq 0} \) is the \( \frac{q-1}{2} \)th order recurrence sequence given by

\[
x_n = \frac{1}{2} \binom{2n}{n}, \quad 0 \leq n \leq \frac{q-1}{2};
\]
and for $D = \frac{a-1}{2}$ we have

$$x_{n+D} = \frac{f_{D-1}}{(D-1)!} x_{n+D-1} - \frac{f_{D-2}}{(D-2)!} x_{n+D-2} + \cdots \pm \frac{f_0}{0!} x_n$$

where

$$f_k = \sum_{0 \leq j \leq \lfloor \frac{1}{2} (D-k) \rfloor} \frac{(D-j)!}{j!(D-2j-k)!} (-1)^j 2^{D-2j-k}.$$

Since this is the simplest general case, we hope the reader understands why we suppress so many details in this introduction!

Finally we give the first example with $\phi(q) = 6$, namely $q = 7$: Here we have that, for $1 \leq a \leq 6$, and any odd prime $p \neq 7$,

$$B_{p-1} \left( \frac{a}{7} \right) - B_{p-1} \equiv \frac{7}{2p} \left\{ U_p(7; a, b) - 1 \right\} \pmod{p}$$

where $b = 1, 2$ or $3$ with $b \equiv \pm p \pmod{7}$, and $U_n$ satisfies the recurrence relation

$$U_{n+3} = 7U_{n+2} - 14U_{n+1} + 7U_n.$$

The values of $U_1, U_2, U_3$ are given in the table below:

<table>
<thead>
<tr>
<th>±a</th>
<th>±b</th>
<th>U_1</th>
<th>U_2</th>
<th>U_3</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>2</td>
<td>7</td>
<td>26</td>
</tr>
<tr>
<td>1</td>
<td>3</td>
<td>2</td>
<td>6</td>
<td>19</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>11</td>
<td>41</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>2</td>
<td>5</td>
<td>13</td>
</tr>
<tr>
<td>a</td>
<td>a</td>
<td>1</td>
<td>3</td>
<td>10</td>
</tr>
</tbody>
</table>

Analogous results can be given for generalized Bernoulli numbers (for Dirichlet characters) since they may be expressed in terms of values of Bernoulli polynomials. It is perhaps more obvious that there should be simple expressions for these since they can be described in terms of $p$-adic $L$-functions which, in turn, can be written in a number of elegant ways. The case of quadratic characters has been examined in [KS] and [W2], and here we give a somewhat different proof of a result proved there:

Suppose that $q$ is a prime $\equiv 1 \pmod{4}$. Let $h_q$ and $\varepsilon_q$ be the class number and fundamental unit, respectively, of the real quadratic field $\mathbb{Q}(\sqrt{q})$. It is well-known that $\varepsilon_q^{(p-\frac{a}{q})} = U + p\sqrt{q}V$ for some integers $U$ and $V$, where
\( \left( \frac{a}{q} \right) \) is the Legendre symbol. Thus the generalized Bernoulli polynomial

\[
(9) \quad B_{p-1,(\frac{a}{q})} := \sum_{a=1}^{q-1} \left( \frac{a}{q} \right) \left\{ B_{p-1} \left( \frac{a}{q} \right) - B_{p-1} \right\} \equiv -2 \left( \frac{p}{q} \right) qh_q V \pmod{p}.
\]

The organization of the paper is as follows: In the next section we shall develop basic identities and results about Bernoulli polynomials that we shall require in our proofs. In Section 2 we shall see how the values of Bernoulli polynomials can be expressed in terms of certain functions of roots of unity. This leads to the proof of a number of the cases mentioned in the introduction; though, because of the computations needed, we give the complete proof of the Theorem in Section 4, and the complete proof of (4) in Section 5. In Section 3 we develop the analogous formulae for those generalized Bernoulli numbers with quadratic characters, which leads to (9) above.

We thank Emma Lehmer, Hugh Williams and the anonymous referee for many useful comments.

1. The (regular) theory of Bernoulli polynomials.

The \( n \)th Bernoulli number \( B_n \) is defined by the power series

\[
(1.1) \quad \frac{x}{e^x - 1} = \sum_{n \geq 0} B_n \frac{x^n}{n!}.
\]

The \( n \)th Bernoulli polynomial \( B_n(t) \) is defined by the power series

\[
(1.2) \quad \frac{xe^{tx}}{e^x - 1} = \sum_{n \geq 0} B_n(t) \frac{x^n}{n!}
\]

so that \( B_n(0) = B_n \) and

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

Perhaps the most important property of Bernoulli polynomials is that

\[
(1.4) \quad B_n(t + 1) - B_n(t) = nt^{n-1} \quad \text{for all } n \geq 1
\]

as is easily deduced from (1.2). From (1.4) we notice that \( B_n(1) = B_n(0) = B_n \) for all \( n \neq 1 \), and that it is “easy” to deduce the value of \( B_n(t) \) for any real number \( t \), once we understand the value of \( B_n(t) \) for \( t \) in the interval \([0, 1)\).
It is thus of interest to determine $B_n(t)$ for ‘special’ values of $t$ in $[0, 1)$, for instance those rational $t$ with small denominator. We already have

$$B_n(0) = B_n(1) = B_n$$ for $n \neq 1,$

and from the identity

$$\frac{2xe^x}{e^{2x} - 1} = 2 \frac{x}{e^x - 1} - \frac{2x}{e^{2x} - 1}$$

we easily deduce that

$$B_n\left(\frac{1}{2}\right) = (2^{1-n} - 1) B_n,$$

and thus we have proved (1). We next observe that

(1.5) $$B_n(1 - t) = (-1)^n B_n(t)$$

from the identity

$$\frac{xe^{(1-t)x}}{e^x - 1} = \frac{(-x)e^{(-x)}}{e^{(-x)} - 1},$$

so we study only $t \in (0, \frac{1}{2})$.

The next important observation is due to Lerch [Lr]: By taking the identity

$$\frac{qxe^{ax}}{e^{qx} - 1} + \frac{qxe^{(a+1)x}}{e^{qx} - 1} + \frac{qxe^{(a+2)x}}{e^{qx} - 1} + \cdots + \frac{qxe^{(a+q-1)x}}{e^{qx} - 1} = \frac{qxe^{ax}}{e^x - 1}$$

we obtain

(1.6) $$B_n\left(\frac{a}{q}\right) + B_n\left(\frac{a+1}{q}\right) + B_n\left(\frac{a+2}{q}\right) + \cdots + B_n\left(\frac{a+q-1}{q}\right) = q^{1-n} B_n(a)$$

and, in particular if $a = 0$,

(1.7) $$B_n + B_n\left(\frac{1}{q}\right) + B_n\left(\frac{2}{q}\right) + \cdots + B_n\left(\frac{q-1}{q}\right) = q^{1-n} B_n.$$  

In order to remove those $B_n(j/q)$ in which $j/q$ is not in lowest terms we may use the standard Möbius inversion formula, as follows: Take $\sum_{d|q} \mu(d)(1.7)_{q/d}$ for $q \geq 3$, so that

(1.8) $$\sum_{\substack{j=0 \\ (j,q)=1}}^{q-1} B_n\left(\frac{j}{q}\right) = \left(\sum_{d|q} \mu(d) \left(\frac{q}{d}\right)^{1-n}\right) B_n.$$
Using (1.5) we have, for all \( q \geq 3 \) and \( n \) even,

\[
\sum_{1 \leq j < q/2 \atop (j,q)=1} B_n \left( \frac{j}{q} \right) = \frac{1}{2} q^{1-n} \prod_{p|q} (1 - p^{n-1}) B_n.
\]

Taking \( q = 3, 4 \) and \( 6 \) we deduce (2).

The seven values \( \frac{1}{2}, \frac{1}{3}, \frac{2}{3}, \frac{1}{4}, \frac{3}{4}, \frac{1}{6}, \frac{5}{6} \) are the only rationals with small denominators for which such “straightforward” values of \( B_n(t) \) are known, with \( 0 < t < 1 \). It has, however, been recently observed [AM] that \( B_n(t) - B_n \) shares one surprising property with polynomials which have integer coefficients: namely that \( q^n(B_n(a/q) - B_n) \) is an integer whenever \( a \) and \( q \) are non-zero integers.

One of the most important, and elegant, applications of these valuations is to the study of Bernoulli polynomials modulo \( p \) for \( p \) prime. The Von Staudt-Clausen theorem asserts that

\[ pB_{2k} \equiv -1 \pmod{p} \]

whenever \( 2k \) is divisible by \( p - 1 \). In 1850 Eisenstein observed the following (easily proved) congruences:

\[
\frac{(ab)^{p-1} - 1}{p} \equiv \frac{a^{p-1} - 1}{p} + \frac{b^{p-1} - 1}{p} \pmod{p}
\]

and

\[
\frac{a^{1-(p-1)} - a}{p} \equiv - \frac{(a^p - a)}{p} \pmod{p}.
\]

Thus we deduce (3) from (2) with \( n = p - 1 \). Such congruences fit elegantly into the general overview of the first case of Fermat’s Last Theorem (see Chapter 8 of [Ri]).

Actually, by the same method, we can transform (1.9) to read, for any even \( n \geq 2 \),

\[
\sum_{1 \leq j < q/2 \atop (j,q)=1} \left( B_n \left( \frac{j}{q} \right) - B_n \right) = qB_n \frac{2}{2} \sum_{d|q} \mu(d) \left( \left( \frac{q}{d} \right)^{-n} - 1 \right).
\]

Taking \( n = p - 1 \) we thus obtain

\[
\sum_{1 \leq j < q/2 \atop (j,q)=1} \left( B_{p-1} \left( \frac{j}{q} \right) - B_{p-1} \right) \equiv \frac{1}{2} \sum_{d|q} \mu(d) \left\{ \frac{(q/d)^p - (q/d)}{p} \right\} \equiv \frac{\phi(q)}{2} \left( \frac{q^{p-1} - 1}{p} + \sum_{l|q \atop l \text{ prime}} \frac{p^l - 1}{l^p - 1} \right) \pmod{p}
\]
However such a formula allows us to evaluate $B_n(a/q)$ only for particular values of $a$ coprime to $q$, provided $\phi(q) \leq 2$. It is the main purpose of this paper to determine the value of

$$B_{p-1}\left(\frac{a}{q}\right) - B_{p-1} \quad (\text{mod } p).$$

2. Working with roots of unity.

**Key Proposition.** If $1 \leq a \leq q$ and odd prime $p$ does not divide $q$ then

(2.1)

$$B_{p-1}\left(\frac{a}{q}\right) - B_{p-1} \equiv \sum_{\gamma^a = 1 \atop \gamma \neq 1} \frac{(\gamma^a - 2 + \gamma^{-a})}{\gamma^p - 2 + \gamma^{-p}} \left(\frac{(1 - \gamma)^p - 1 + \gamma^p}{p}\right) \quad (\text{mod } p).$$

**Proof.** If $\gamma^a = 1$ then

$$\frac{(1 - \gamma)^p - 1 + \gamma^p}{p} = \sum_{j=1}^{p-1} \frac{1}{p} \binom{p}{j} (-1)^j \gamma^j \equiv - \sum_{j=1}^{p-1} \frac{\gamma^j}{j} \quad (\text{mod } p),$$

since

$$\frac{1}{p} \binom{p}{j} (-1)^j = \frac{(-p)(1-p)(2-p)\cdots(j-1-p)}{p \cdot 2 \cdots (j-1) \cdot j} \equiv - \frac{1}{j} \quad (\text{mod } p).$$

We also have

$$\frac{\gamma^a - 2 + \gamma^{-a}}{\gamma^p - 2 + \gamma^{-p}} = m + \sum_{i=1}^{m} (m - i) (\gamma^{ip} + \gamma^{-ip})$$

by substituting $x = \gamma^p$ and $m \equiv a/p \text{ mod } q$ into the identity

(2.2)

$$\frac{x^m - 2 + x^{-m}}{x - 2 + x^{-1}} = m + \sum_{i=1}^{m} (m - i) (x^i + x^{-i}).$$

Therefore the righthand side of (2.1) is

$$\equiv - \sum_{\gamma^a = 1} \left\{ m + \sum_{i=1}^{m} (m - i) (\gamma^{ip} + \gamma^{-ip}) \right\} \sum_{j=1}^{p-1} \frac{\gamma^j}{j} \quad (\text{mod } p)$$

$$\equiv -q \left\{ m \sum_{0 < j < p \atop q \mid j} \frac{1}{j} + \sum_{i=1}^{m} (m - i) \left( \sum_{0 < j < p \atop q \mid ip + j} \frac{1}{ip + j} - \sum_{0 < j < p \atop q \mid ip - j} \frac{1}{ip - j} \right) \right\} \quad (\text{mod } p),$$
using the fact, for $\gamma = 1$, that $\sum_{j=1}^{p-1} 1/j \equiv 0 \pmod{p}$. Now, since $ip < ip + j < (i + 1)p$ and $(i - 1)p < ip - j < ip$, we replace $q/(ip \pm j)$ by $1/k$ so that the above is

$$
\equiv - \left\{ m \sum_{0 < k < \frac{m}{q}} \frac{1}{k} + \sum_{i=1}^{m} (m - i) \left( \sum_{\frac{ip}{q} < k < (i+1)p} \frac{1}{k} - \sum_{\frac{(i-1)p}{q} < k < \frac{ip}{q}} \frac{1}{k} \right) \right\} \pmod{p}
$$

$$
\equiv - \sum_{0 < k < \frac{mp}{q}} \frac{1}{k} \pmod{p}
$$

$$
\equiv (p - 1) \sum_{0 < k \leq \frac{mp-a}{q}} k^{p-2} \pmod{p}.
$$

But this equals the coefficient of $x^{p-1}/(p - 1)!$ in

$$
x^{(mp-a)/q} = x \frac{e^{x(mp-a+q)/q} - 1}{e^x - 1}
$$

which is $B_{p-1} \left( \frac{mp-a+q}{q} \right) - B_{p-1}$ by (1.2). However the Von Staudt-Clausen Theorem tells us that $p$ divides the denominator of $B_n$ if and only if $p - 1$ divides $n$; and so, by (1.3), the denominators of the coefficients of $B_{p-1}(t) - B_{p-1}$ are not divisible by $p$. Therefore

$$
B_{p-1} \left( \frac{mp-a+q}{q} \right) - B_{p-1} \equiv B_{p-1} \left( \frac{-a+q}{q} \right) - B_{p-1} \pmod{p}
$$

$$
\equiv B_{p-1} \left( \frac{a}{q} \right) - B_{p-1} \pmod{p},
$$

by (1.5), and the Proposition follows. \hfill \Box

**Corollary 1.** If $1 \leq a \leq q - 1$ and odd prime $p$ does not divide $q$ then

$$
(2.3) \quad B_{p-1} \left( \frac{a}{q} \right) - B_{p-1} \equiv \frac{1}{2} \sum_{\gamma \neq 1} \left( 1 - \frac{\gamma^a + \gamma^{-a}}{2} \right) \frac{1}{p} \left( \frac{(2 - \gamma - \gamma^{-1})^p}{2 - \gamma^p - \gamma^{-p}} - 1 \right) \pmod{p}.
$$

**Proof.** It is evident that

$$
(1 - \gamma)^p \equiv 1 - \gamma^p \equiv 2^{p-1}(1 - \gamma^p) \pmod{p}.
$$
Therefore

\[ 0 \equiv \{(1 - \gamma)^p - 2^{p-1}(1 - \gamma^p)\}^2 / (2\gamma)^p \pmod{p^2} \]

\[ = - \left(1 - \frac{\gamma + \gamma^{-1}}{2}\right)^p + (1 - \gamma)^p + (1 - \gamma^{-1})^p - 2^{p-1} \left(1 - \frac{\gamma^p + \gamma^{-p}}{2}\right) . \]

Thus

\[ (1 - \gamma)^p + (1 - \gamma^{-1})^p - 2 + \gamma^p + \gamma^{-p} \]

\[ \equiv \left(1 - \frac{\gamma + \gamma^{-1}}{2}\right)^p - \left(1 - \frac{\gamma^p + \gamma^{-p}}{2}\right) + \frac{2^{p-1} - 1}{p} \left(1 - \frac{\gamma^p + \gamma^{-p}}{2}\right) \pmod{p} . \]

Now, adding each term to its conjugate in (2.1) we get the following congruence modulo \( p \):

\[ B_{p-1} \left(\frac{a}{q}\right) - B_{p-1} \]

\[ \equiv \frac{1}{2} \sum_{\gamma^{-1} \neq 1} \left(1 - \frac{\gamma^a + \gamma^{-a}}{2}\right) \left\{ \frac{1}{p} \left(\frac{\left(1 - \frac{\gamma + \gamma^{-1}}{2}\right)^p}{\left(1 - \frac{\gamma^p + \gamma^{-p}}{2}\right)} - 1\right) + \frac{2^{p-1} - 1}{p} \right\} . \]

Since the two terms in the final brackets are both units mod \( p \) we may multiply the first by \( 2^{p-1} \equiv 1 \pmod{p} \) to get

\[ \frac{1}{p} \left(\frac{(2 - \gamma - \gamma^{-1})^p}{2 - \gamma^p - \gamma^{-p}} - 2^{p-1}\right) + \left(\frac{2^{p-1} - 1}{p}\right) \]

\[ \equiv \frac{1}{p} \left(\frac{(2 - \gamma - \gamma^{-1})^p}{2 - \gamma^p - \gamma^{-p}} - 1\right) \pmod{p} . \]

The result follows.

The next result follows immediately by applying Möbius inversion to (2.3) and associating the \( \gamma \) and \( \gamma^{-1} \) terms.

**Corollary 2.** If \( q \geq 3, 1 \leq a \leq q \) and odd prime \( p \) does not divide \( q \) then

\[ \sum_{d|q} \mu \left(\frac{q}{d}\right) B_{p-1} \left(\frac{a_d}{d}\right) \]

\[ \equiv \frac{1}{2} \sum_{\substack{j=1 \\ (j, q) = 1}}^{q/2} \left(2 - (w^j + w^{-j})\right) \frac{1}{p} \left(\frac{(2 - w^j - w^{-j})^p}{2 - w^jp - w^{-jp}} - 1\right) \pmod{p} . \]
where \( w = e^{2i\pi/q} \) and \( a_d \) is the least positive residue of \( a \) (mod \( d \)).

Next note that if \( (a, q) = 1 \) then
\[
\sum_{j=1}^{q/2} (2 - w^{ja} - w^{-ja}) = \phi(q) - \sum_{i=1}^{q} w^i = \phi(q) - \mu(q).
\]

Thus if we define
\[
u_n(q; a, b) := \sum_{\substack{j=1 \\ (j, q) = 1}}^{q/2} \left( \frac{2 - w^{ja} - w^{-ja}}{2 - w^b - w^{-b}} \right) (2 - w^j - w^{-j})^n,
\]
where \( a, b \) are taken (mod \( q \)), then by Corollary 2,
\[
\sum_{d \mid q} \mu\left(\frac{q}{d}\right) B_{p-1} \left( \frac{a_d}{d} \right) \equiv \frac{1}{2p} \{ u_p(q; a, p \mod q) - (\phi(q) - \mu(q)) \} \pmod{p}.
\]

Now \( \nu_n \) so defined is a recurrence sequence with characteristic polynomial
\[
F_q(X) := \prod_{j=1}^{q/2} \left( X - 2 + w^j + w^{-j} \right).
\]

Note that
\[
F_q((1 - X^{-1})(1 - X)) = \prod_{j=1}^{q/2} \left( 1 - \frac{1}{X} \right) (X - w^j)(X - w^{-j})
= (-X^{-1})^{\phi(q)/2} \phi_q(X)
\]
where \( \phi_q(X) \) is the \( q \)th cyclotomic polynomial.

If \( F(X) = X^D - \sum_{i=0}^{D-1} f_i X^i \) where \( D = \phi(q)/2 \), then
\[
u_{n+D} = f_{D-1} u_{n+D-1} + f_{D-2} u_{n+D-2} + \cdots + f_0 u_n \quad \text{for all} \ n \geq 0.
\]

We get the same recurrence relation for all \( \nu_n \) with a given \( q \), but the starting values, \( \nu_0, \nu_1, \ldots, \nu_{D-1} \), are different.

Let's define
\[
V_n(q; k) = \sum_{\substack{j=1 \\ (j, q) = 1}}^{q} w^{j\cdot k}(2 - w^j - w^{-j})^n.
\]
This satisfies the same recurrence relation. Moreover since for \( m \equiv a/b \pmod{q} \) we have

\[
\frac{w^{ja} - 2 + w^{-ja}}{w^{jb} - 2 + w^{-jb}} = \sum_{k=-m}^{m} (m - |k|)w^{jbk},
\]

thus

\[
u_n(q; bm \mod q, b) = \frac{1}{2} \sum_{k=-m}^{m} (m - |k|)V_n(q; bk \mod q);
\]

so we may find the starting values, \( u_0, \ldots, u_{D-1} \) given those of \( V_0, \ldots, V_{D-1} \).

Now, for \( 0 \leq n < \phi(q)/2 = D \), we have

\[
V_n(q; k) = \sum_{j=1, (j,q)=1}^{q} w^{jkb} (2 - w^{j} - w^{-j})^n = \sum_{j=1, (j,q)=1}^{q} (-1)^n w^{j(bk-n)} (1 - w^{j})^{2n}
\]

\[
= \sum_{m=0}^{2n} \binom{2n}{m} (-1)^{n+m} \sum_{j=1, (j,q)=1}^{q} w^{j(bk+m-n)}
\]

\[
= \sum_{m=0}^{2n} \binom{2n}{m} (-1)^{n+m} \sum_{d|q, d|m+bk-n} \mu \left( \frac{q}{d} \right) d
\]

\[
= \sum_{d|q} \mu \left( \frac{q}{d} \right) d \sum_{m=n-bk \mod d}^{2n} \binom{2n}{m} (-1)^{n+m},
\]

since

\[
\sum_{j=1}^{q} w^{jt} = \sum_{d|q} \frac{\mu(d)}{d} = \sum_{r | (t,q)} \mu \left( \frac{q}{r} \right) r,
\]

taking \( r = q/d \). This is computable (though not too beautiful!).

### 3. Generalized Bernoulli numbers.

For any even character \( \chi \pmod{q} \) define

\[
B_{p-1, \chi} = \sum_{a=0}^{q-1} \chi(a) \left( B_{p-1} \left( \frac{a}{q} \right) - B_{p-1} \right).
\]

Assume that \( q \) is prime, so that from Corollary 2 we have for \( w = e^{2\pi i/q} \),

\[
4pB_{p-1, \chi} \equiv \sum_{j=1}^{q-1} \left( \sum_{a=0}^{q-1} \chi(a)(2 - w^{ja} - w^{-ja}) \right) \left( \frac{2 - w^{j} - w^{-j}}{2 - w^{pj} - w^{-pj}} - 1 \right) \pmod{p^2}.
\]
However

\[
\sum_{a=0}^{q-1} \chi(a)(2 - w^{ja} - w^{-ja}) = \begin{cases} 
-2\overline{\chi}(j) \sum_{b=0}^{q-1} \chi(b)w^b & \text{for } \chi \text{ non-principal} \\
2q & \text{for } \chi \text{ principal.}
\end{cases}
\]

If \(\chi\) is principal we thus obtain from (1.7)\(_q\),

\[
2q \sum_{j=1}^{q-1} \left( \frac{(2 - w^j - w^{-j})^p}{2 - wp^j - w^{-pj}} - 1 \right) \equiv 4pB_{p-1,\chi} = 4pB_{p-1}(q^{1-(p-1)} - q) \equiv 4(q^p - q) \pmod{p^2},
\]

using the Von Staudt-Clausen theorem. On the other hand if \(\chi\) is even and non-principal then, for \(g(\chi) = \sum_{1 \leq b \leq q} \chi(b)w^b\), we have

\[
4pB_{p-1,\chi} \equiv -2g(\chi) \sum_{j=0}^{q-1} \overline{\chi}(j) \left( \frac{(2 - w^j - w^{-j})^p}{2 - wp^j - w^{-pj}} - 1 \right) \pmod{p^2}.
\]

As an example we’ll consider \(\chi\), the real non-principal character \(\pmod{q}\); that is \(\chi(a) = \left( \frac{a}{q} \right)\), the Legendre symbol. We will need \(q\) to be 1 \(\pmod{4}\) to ensure that \(\chi\) is an even character. Then

\[
\sum_{a=1}^{q-1} \left( \frac{a}{q} \right) \left\{ B_{p-1} \left( \frac{a}{q} \right) - B_{p-1} \right\} = B_{p-1,\left( \frac{a}{q} \right)} = \frac{-1}{2p} g \left( \left\{ \frac{j}{q} \right\} \right) \Sigma_q,
\]

where

\[
\Sigma_q \equiv \sum_{j=0}^{q-1} \left( \frac{j}{q} \right) \left( \frac{(2 - w^j - w^{-j})^p}{2 - wp^j - w^{-pj}} - 1 \right) \pmod{p^2}.
\]

We will examine \(\Sigma_q\) using \(p\)-adic logarithms (see Chapter 5 of [Wa] for definitions): Since

\[
\frac{(2 - w^j - w^{-j})^p}{2 - wp^j - w^{-pj}} - 1 \equiv \log_p \left( \frac{(2 - w^j - w^{-j})^p}{2 - wp^j - w^{-pj}} \right) \pmod{p^2},
\]
we deduce that

\[ \Sigma_q = \sum_{j=0}^{q-1} \left( \frac{j}{q} \right) \log_p \left( \frac{(2 - w^j - w^{-j})^p}{2 - w^{pj} - w^{-pj}} \right) \pmod{p^2} \]

\[ = \log_p \left( \prod_{j=1}^{q-1} (2 - w^j - w^{-j})^p \right) \pmod{p^2} \]

\[ = \log_p \left( \prod_{i=1}^{q-1} (2 - w^i - w^{-i})^{\left( \frac{i}{q} \right) \left( p - \left( \frac{p}{q} \right) \right)} \pmod{p^2} \right) \]

\[ = \log_p \left( \prod_{i=1}^{q-1} (1 - w^i)^{\left( \frac{i}{q} \right) \left( p - \left( \frac{p}{q} \right) \right)} \pmod{p^2} \right) , \]

since \( q \equiv 1 \pmod{4} \). Now, as Dirichlet discovered (see Ex. 4.6. of [Wa]),

\[ \prod_{i=1}^{q-1} (1 - w^i)^{\left( \frac{i}{q} \right) \left( p - \left( \frac{p}{q} \right) \right)} = \varepsilon_q^{2h(\sqrt{q})} \]

where \( \varepsilon_q, h(\sqrt{q}) \) are the fundamental unit and class number of \( \mathbb{Q}(\sqrt{q}) \), respectively. Thus

\[ \sum_{a=1}^{q-1} \left( \frac{a}{q} \right) \left\{ B_{p-1} \left( \frac{a}{q} \right) - B_{p-1} \right\} \]

\[ \equiv -\frac{1}{p} \left( \frac{1}{q} \right) g \left( \left( \frac{1}{q} \right) \right) h(\sqrt{q}) \log p \left( \varepsilon_q^{2 \left( p - \left( \frac{p}{q} \right) \right)} \right) \pmod{p} . \]

So, as \( \varepsilon_q = u + v\sqrt{q} \) where \( u^2 - v^2 q = -1 \), then

\[ \varepsilon_q^p \equiv u^p + v^p \sqrt{q}^p \equiv u + v \left( \frac{q}{p} \right) \sqrt{q} \pmod{p} \]

so that \( \varepsilon_q^{p - \left( \frac{p}{q} \right)} \equiv \left( \frac{p}{q} \right) \pmod{p} \) and thus \( \varepsilon_q^{2 \left( p - \left( \frac{p}{q} \right) \right)} \equiv 1 \pmod{p} \). Suppose that

\[ \varepsilon_q^{2 \left( p - \left( \frac{p}{q} \right) \right)} = 1 + pu + pv\sqrt{q} \pmod{p^2} . \]

Then

\[ 1 = \varepsilon_q^{2 \left( p - \left( \frac{p}{q} \right) \right)} \varepsilon_q^{2 \left( p - \left( \frac{p}{q} \right) \right)} \equiv (1 + pu)^2 - (pv\sqrt{q}^2) \equiv 1 + 2pu \pmod{p^2} , \]

so that \( p \) divides \( u' \). So if

\[ x_n = \frac{\varepsilon_q^n - \varepsilon_q^n}{2v\sqrt{q}} \quad \text{then} \quad \varepsilon_q^{2 \left( p - \left( \frac{p}{q} \right) \right)} \equiv 1 + vx_{2 \left( p - \left( \frac{p}{q} \right) \right)} \sqrt{q} \pmod{p^2} . \]
Therefore \( \log_p\left(2^{p-(\xi)}\right) \equiv vx_{2(p-(\xi))}\sqrt{q} \pmod{p^2} \), and since \( g\left(\frac{1}{q}\right) = \sqrt{q} \) (which was proved first by Gauss), we have

\[
(3.1) \sum_{a=1}^{q-1} \left\{ \frac{a}{q} \right\} \left\{ B_{p-1}\left(\frac{a}{q}\right) - B_{p-1} \right\} \equiv \frac{-q}{p} h(\sqrt{q})vx_{2(p-(\xi))} \pmod{p};
\]

this is equivalent to (9).

## 4. Proof of the Theorem.

Take \( p \equiv \pm a \pmod{q} \) in Corollary 1 to get

\[
B_{p-1}\left(\frac{a}{q}\right) - B_{p-1} = \frac{1}{4p} \sum_{\gamma^q=1} \{(2 - \gamma - \gamma^{-1})^p - (2 - \gamma^p - \gamma^{-p})\} \pmod{p}.
\]

Now \( \frac{1}{2} \sum_{\gamma^q=1} (2 - \gamma^p - \gamma^{-p}) = q \). Thus, for \( x_n = \frac{1}{2q} \sum_{\gamma^q=1} (2 - \gamma - \gamma^{-1})^n \), we obtain (8). Now if \( 0 \leq n \leq \frac{p-1}{2} \) then

\[
x_n = \frac{1}{2q} \sum_{\gamma^q=1} (-\gamma^{-1})^n (1 - \gamma)^{2n} = \frac{1}{2} \sum_{m=0}^{n} \binom{2n}{m} (-1)^{n+m} \frac{1}{q} \sum_{\gamma^q=1} \gamma^{m-n} = \frac{1}{2} \binom{2n}{n};
\]

If \( w = e^{2i\pi/q} \) then the characteristic polynomial for \( x_n \) is

\[
\prod_{j=1}^{(q-1)/2} (X - 2 + w^j + w^{-j}).
\]

The anonymous referee noted that this polynomial seems to be closely related to the Chebyshev polynomial of the first kind; and we should be able to determine its coefficients directly from known results. Although we agree with this opinion we have been unable to do so. To compute the coefficients we thus proceed as follows: First note that

\[
\sum_{j \geq 0} (-1)^j \binom{m-j}{j} (X + X^{-1})^{m-2j} = \sum_{j \geq 0} (-1)^j \binom{m-j}{j} \sum_{i \geq 0} \binom{m-2j}{i} X^{m-2j-2i} = \sum_{k \geq 0} X^{m-2k} \left( \sum_{j=0}^{k} \binom{m-j}{j} \left( \frac{m-2j}{k-j} \right) (-1)^j \right)
\]
taking $i + j = k$. The inner sum

$$= \sum_{j=0}^{k} \binom{k}{j} \binom{m-j}{k} (-1)^j$$

$$= \sum_{j=0}^{k} \text{coeff of } T^j \text{ in } (1 - T)^k \ast \text{coeff of } T^{m-k-j} \text{ in } (1 - T)^{-k-1}$$

$$= \text{coeff of } T^{m-k} \text{ in } (1 - T)^{-1} = \begin{cases} 1 & \text{if } k \leq m \\ 0 & \text{otherwise.} \end{cases}$$

Thus

$$\sum_{j \geq 0} (-1)^j \binom{m-j}{j} (X + X^{-1})^{m-2j} = \sum_{i=m \pmod{2}}^{m} X^i .$$

So define

(4.1) \quad F_q(y) := \sum_{j \geq 0} (-1)^j \binom{q-j}{j} (2 - y)^{q-1-2j}$$

$$+ \sum_{i \geq 0} (-1)^i \binom{q-3}{i} (2 - y)^{q-3-2i} .$$

Then $F_q(y)$ is a polynomial in $y$ of degree $\frac{q-1}{2}$. For any $k$, $1 \leq k \leq \frac{q-2}{2}$,

$$F_q(2 - w^k - w^{-k}) = \sum_{j \geq 0} (-1)^j \binom{q-j}{j} (w^k + w^{-k})^{q-1-2j}$$

$$+ \sum_{i \geq 0} (-1)^i \binom{q-3}{i} (w^k + w^{-k})^{q-3-2i}$$

$$= \sum_{l=-\left(\frac{q-1}{2}\right)}^{\frac{q-1}{2}} w^{kl} = 0$$

by (4.1). Thus $F_q(y)$ is our characteristic polynomial, and

$$F_q(y) = \sum_{k=0}^{\frac{q-1}{2}} \frac{F_k}{k!} (-y)^k \quad \text{where}$$

$$f_k = \frac{\frac{1}{2} \binom{q-1}{2} \binom{q-j}{j}}{j! \binom{q-1}{2} - 2j - k} \binom{q-1}{2} (-1)^j 2^{\frac{q-1}{2} - 2j - k} .$$

Actually $F_q(X) = R_{\frac{q-1}{2}}(X)$ where $R_n(X)$ satisfies the recurrence

$$R_m(X) = (2 - X)R_{m-1}(X) + R_{m-2}(X) .$$
5. Proof of (4).

A Lucas sequence \( \{x_n\}_{n \geq 0} \) is defined by \( x_0 = 0, \ x_1 = 1 \) and \( x_n = bx_{n-1} - cx_{n-2} \) for all \( n \geq 2 \), for some integers \( b \) and \( c \). As is well-known, if we let \( D = b^2 - 4c \) then the roots of the characteristic polynomial \( t^2 - bt + c \) of \( \{x_n\} \) are \( \alpha, \beta = (b \pm \sqrt{D})/2; \) and \( x_n = (\alpha^n - \beta^n) / (\alpha - \beta) \). Let \( y_n = (\alpha^n + \beta^n) \) be the 'companion sequence', which satisfies the same recurrence relation; and we have \( \alpha^n, \beta^n = (y_n \pm x_n\sqrt{D})/2 \).

We shall be considering these recurrence sequences modulo powers of any prime \( p \) that does not divide \( 2cD \): Now, since \( p \) divides \( \binom{p}{j} \) except when \( j = 0 \) or \( p \), we have

\[
\left( \frac{b \pm \sqrt{D}}{2} \right)^p \equiv \frac{b^p \pm D^{(p-1)/2}\sqrt{D}}{2^p} \equiv \frac{b \pm \left( \frac{D}{2} \right) \sqrt{D}}{2} \pmod{p}.
\]

Thus

\[
\left( \frac{b \pm \sqrt{D}}{2} \right)^{p-\left( \frac{D}{p} \right)} \equiv \left( \frac{b \pm \left( \frac{D}{2} \right) \sqrt{D}}{2} \right)^{-(\frac{D}{p})} \equiv c^{\frac{1}{2}(1-\left( \frac{D}{p} \right))} \pmod{p}.
\]

Therefore \( x_{p^{-\left( \frac{D}{p} \right)}} \equiv 0 \pmod{p} \) and

\[
c^{p-\left( \frac{D}{p} \right)} = \alpha^{p-\left( \frac{D}{p} \right)} \beta^{p-\left( \frac{D}{p} \right)} = \frac{y_{p^{-\left( \frac{D}{p} \right)}}^2 - D^2 x_{p^{-\left( \frac{D}{p} \right)}}^2}{4} \equiv \frac{y_{p^{-\left( \frac{D}{p} \right)}}^2}{4} \pmod{p^2}.
\]

Therefore \( y_{p^{-\left( \frac{D}{p} \right)}} \equiv 2c^{\frac{1}{2}(1-\left( \frac{D}{p} \right))} \left( \frac{c^{p-1} + 1}{2} \right) \pmod{p^2} \). In fact \( c = \pm 1 \) in every case below so that

\[
\alpha^{p-\left( \frac{D}{p} \right)}, \beta^{p-\left( \frac{D}{p} \right)} \equiv \begin{cases} 1 \pm p\sqrt{D} \left( \frac{1}{2p} x_{p-\left( \frac{D}{p} \right)} \right) \pmod{p^2} & \text{if } c = 1; \\ \left( \frac{D}{p} \right) \pm p\sqrt{D} \left( \frac{1}{2p} x_{p-\left( \frac{D}{p} \right)} \right) \pmod{p^2} & \text{if } c = -1. \end{cases}
\]

When \( \phi(q) = 4 \), we let \( t \) be the unique integer in the range \( 1 < t < q/2 \) that is coprime to \( q \). Fix a primitive \( q \)-th root \( w \) of \( 1 \), and let \( \alpha_j = 2 - w^j - w^{-j} \).

By Corollary 2

\[
\sum_{d|q} \mu \left( \frac{q}{d} \right) B_{p-1} \left( \frac{a_d}{d} \right) \equiv \frac{1}{2p} \left\{ \frac{\alpha_d^p}{\alpha_1} \frac{\alpha_1^p}{\alpha_2} \alpha_2^p - (\alpha_1 + \alpha_2) \right\} \pmod{p}
\]

(5.2)

\[
\equiv \frac{1}{2p} \left\{ \frac{1}{C'} \left( \alpha_1 \alpha_1^{p-\left( \frac{D}{p} \right)} + \alpha_2 \alpha_2^{p-\left( \frac{D}{p} \right)} \right) - B \right\} \pmod{p}
\]

where \( B = \alpha_1 + \alpha_2, \ C = \alpha_1 \alpha_2 \) and \( C' = C \) if \( \left( \frac{q}{p} \right) = -1 \), with \( C' = 1 \) otherwise.
The cases \( q = 5 \) and \( q = 10 \): When \( q = 5 \) we have \( t = 2 \), \((x - \alpha_1)(x - \alpha_2) = x^2 - 5x + 5\), so that \( B = C = 5 \) and we may take \( \alpha_j = \frac{1}{5}\sqrt{5} \left(\sqrt{5} + \left(\frac{j}{5}\right)\right) \) for \( 1 \leq j \leq 4 \). Let \( \alpha = (1 + \sqrt{5})/2 \) and \( \beta = (1 - \sqrt{5})/2 \). By substituting into (5.2) and then using (5.1) (with \( b = 1 \), \( c = -1 \) so that \( x_n = F_n \)) we get

\[
B_{p-1} \left(\frac{a}{5}\right) - B_{p-1} \\
\equiv \frac{5}{2p} \left\{ \frac{5^{(p-1)/2}}{2\sqrt{5}} \left( \left(\sqrt{5} + \left(\frac{a}{5}\right)\right) \alpha^{p-\left(\frac{a}{5}\right)} + \left(\sqrt{5} - \left(\frac{a}{5}\right)\right) \beta^{p-\left(\frac{a}{5}\right)} \right) - 1 \right\}
\]

\[
\equiv \frac{5}{2p} \left\{ \frac{5^{(p-1)/2}}{2\sqrt{5}} \left( \left(\frac{p}{5}\right) + p \frac{1}{2p} F_{p-\left(\frac{a}{5}\right)} \left(\frac{a}{5}\right) \right) - 1 \right\}
\]

\[
\equiv \frac{5}{4} \left\{ \left(\frac{5^{p-1} - 1}{p}\right) + \frac{1}{p} F_{p-\left(\frac{a}{5}\right)} \left(\frac{a}{5}\right) \right\} \pmod{p}
\]

giving the first congruence in (4), since

\[
5^\frac{p+1}{2} \equiv \left(\frac{5}{p}\right) \left(1 + \frac{1}{2} (5^{p-1} - 1) \right) \pmod{p^2}.
\]

It would be possible to obtain the congruence for \( q = 10 \) in a similar way. However, by taking \( q = 2 \) and \( a = 1/5 \) and \( a = 3/5 \) in (1.6) we get the identities

\[
B_{p-1} \left(\frac{1}{10}\right) = 2^{2-p} B_{p-1} \left(\frac{1}{5}\right) - B_{p-1} \left(\frac{3}{5}\right)
\]

\[
B_{p-1} \left(\frac{3}{10}\right) = 2^{2-p} B_{p-1} \left(\frac{3}{5}\right) - B_{p-1} \left(\frac{4}{5}\right).
\]

By substituting in the first congruence in (4), and by using the Von Staudt-Clausen theorem, we get the third congruence in (4).

The case \( q = 8 \): Now \( t = 3 \), \((x - \alpha_1)(x - \alpha_3) = x^2 - 4x + 2\), so that \( B = 4 \), \( C = 2 \) and we may take \( \alpha_j = \sqrt{2} \left(\sqrt{2} + \left(\frac{j}{8}\right)\right) \) for any odd \( j \). Let \( \alpha = (1 + \sqrt{2}) \) and \( \beta = (1 - \sqrt{2}) \). By substituting into (5.2) and then using (5.1) (with \( b = 2 \), \( c = -1 \) so that \( x_n = G_n \)), we see that the right side of (5.2) is

\[
\equiv \frac{2}{p} \left\{ \frac{2^{(p-1)/2}}{2\sqrt{2}} \left( \left(\sqrt{2} + \left(\frac{8}{a}\right)\right) \alpha^{p-\left(\frac{8}{a}\right)} + \left(\sqrt{2} - \left(\frac{8}{a}\right)\right) \beta^{p-\left(\frac{8}{a}\right)} \right) - 1 \right\}
\]

\[
\equiv \frac{2}{p} \left\{ \frac{2^{(p-1)/2}}{2\sqrt{2}} \left( \left(\frac{8}{p}\right) + p \frac{1}{p} G_{p-\left(\frac{8}{a}\right)} \left(\frac{8}{a}\right) \right) - 1 \right\}
\]

\[
\equiv \left(\frac{2^{p-1} - 1}{p}\right) + 2 \left(\frac{8}{ap}\right) \frac{1}{p} G_{p-\left(\frac{8}{a}\right)} \pmod{p}
\]
since $2^{\frac{p-1}{2}} \equiv \left( \frac{8}{p} \right) (1 + \frac{1}{2}(2^{p-1} - 1)) \pmod{p^2}$. Adding this to the third congruence in (3) gives the second congruence in (4).

The case $q = 12$: Now $t = 5$, $(x - \alpha_1)(x - \alpha_3) = x^2 - 4x + 1$, so that $b = B = 4$, $c = C = 1$ and we may take $\alpha_j = 2 + \left( \frac{12}{j} \right) \sqrt{3}$ for $j = 1, 5, 7, 11$; and let $\alpha = \alpha_1$, $\beta = \alpha_2$. Therefore, by using (5.1), the right side of (5.2) is

$$\equiv \frac{1}{2p} \left\{ \left( 2 + \left( \frac{12}{a} \right) \sqrt{3} \right) \alpha^{p-\left( \frac{12}{p} \right)} + \left( 2 - \left( \frac{12}{a} \right) \sqrt{3} \right) \beta^{p-\left( \frac{12}{p} \right)} - 4 \right\}$$

$$\equiv 3 \left( \frac{12}{a} \right)^{-1} H_{p-\left( \frac{12}{p} \right)} \pmod{p}.$$  

The final congruence of (4) follows by adding the last two congruences of (3) and subtracting the first.

References


Received July 21, 1993.

University of Georgia
Athens, Ga 30602
E-mail address: andrew@math.uga.edu

AND

Nanjing University
Nanjing 210008, P. R. CHINA