Values of Bernoulli polynomials

Andrew Granville * and Zhi-Wei Sun †

Let $B_n(t)$ be the nth 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 $[q/2]$ 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 $\le \phi(q)/2$, and so we can recover the classical results where $\phi(q) \le 2$ (for instance, $B_{p-1}(1/6) - B_{p-1} \equiv (3^p - 3)/2p + (2^p - 2)/p \pmod p$). 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.

Dedicated to Emma Lehmer.

Introduction.

It has long been known that the nth 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 kth Bernoulli number, defined by the power series

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

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

$$\begin{aligned} B_n(1) &= B_n(0) = B_n, \quad \text{for } n \ne 1 \\ B_n\left(\frac{1}{2}\right) &= (2^{1-n} - 1) B_n; \end{aligned} \tag{1}$$

and for all even $n \ge 2$,

$$\begin{aligned} B_n\left(\frac{1}{3}\right) = B_n\left(\frac{2}{3}\right) &= \frac{1}{2}\,(3^{1-n} - 1) B_n, \\ B_n\left(\frac{1}{4}\right) = B_n\left(\frac{3}{4}\right) &= \frac{1}{2}\,(4^{1-n} - 2^{1-n}) B_n, \\ B_n\left(\frac{1}{6}\right) = B_n\left(\frac{5}{6}\right) &= \frac{1}{2}\,(6^{1-n} - 3^{1-n} - 2^{1-n} + 1) B_n. \end{aligned} \tag{2}$$

* An Alfred P. Sloan Research Fellow. Also supported, in part, by the National Science Foundation.

† Supported by the National Natural Science Foundation of the People's Republic of China.

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

Following work of Friedman and Tamarkine [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

$$
\begin{aligned}
&B_{p-1}\left(\frac{1}{2}\right) - B_{p-1} \equiv \frac{2^p-2}{p} \pmod p \\
&B_{p-1}\left(\frac{1}{3}\right) - B_{p-1} \equiv B_{p-1}\left(\frac{2}{3}\right) - B_{p-1} \equiv \frac{1}{2}\frac{(3^p-3)}{p} \pmod p \\
&B_{p-1}\left(\frac{1}{4}\right) - B_{p-1} \equiv B_{p-1}\left(\frac{3}{4}\right) - B_{p-1} \equiv \frac{3}{2}\frac{(2^p-2)}{p} \pmod p \\
&B_{p-1}\left(\frac{1}{6}\right) - B_{p-1} \equiv B_{p-1}\left(\frac{5}{6}\right) - B_{p-1} \equiv \frac{1}{2}\frac{(3^p-3)}{p} + \frac{2^p-2}{p} \pmod p
\end{aligned} \tag{3}
$$

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 $B_{p-1}(\frac{a}{q}) - B_{p-1} \pmod p$ where $\phi(q) = 1$ or 2 (ϕ 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 <u>first-order</u> 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 kth-order linear recurrence sequence with

$$k \le \phi(q)/2.$$

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 $1 \le a \le q-1$ with $(a,q) = 1$ (there being four such integers a), we have

$$
\begin{aligned}
B_{p-1}\left(\frac{a}{5}\right) - B_{p-1} &\equiv \frac{5}{4}\left\{\left(\frac{ap}{5}\right)\frac{1}{p}\,F_{p-(\frac{p}{5})} + \frac{5^{p-1}-1}{p}\right\} \pmod p \\
B_{p-1}\left(\frac{a}{8}\right) - B_{p-1} &\equiv \left\{2\left(\frac{ap}{8}\right)\frac{1}{p}\,G_{p-(\frac{p}{8})} + 4\,\frac{(2^{p-1}-1)}{p}\right\} \pmod p \\
B_{p-1}\left(\frac{a}{10}\right) - B_{p-1} &\equiv \frac{15}{4}\left(\frac{ap}{5}\right)\frac{1}{p}\,F_{p-(\frac{p}{5})} + \frac{5}{4}\cdot\frac{5^{p-1}-1}{p} + \frac{2(2^{p-1}-1)}{p} \pmod p \\
B_{p-1}\left(\frac{a}{12}\right) - B_{p-1} &\equiv 3\left(\frac{a}{12}\right)\frac{1}{p}\,H_{p-(\frac{p}{12})} + \frac{3(2^{p-1}-1)}{p} + \frac{3}{2}\frac{(3^{p-1}-1)}{p} \pmod p
\end{aligned}
\tag{4}
$$

where $(-)$ is the Jacobi symbol, and we define the following second-order linear recurrence sequences:

$$
\begin{aligned}
F_0 = 0,\ F_1 = 1, \text{ and } F_{n+2} &= F_{n+1} + F_n \ \text{ for all } n \ge 0 \\
G_0 = 0,\ G_1 = 1, \text{ and } G_{n+2} &= 2G_{n+1} + G_n \ \text{ for all } n \ge 0 \\
H_0 = 0,\ H_1 = 1, \text{ and } H_{n+2} &= 4H_{n+1} - H_n \ \text{ for all } n \ge 0.
\end{aligned}
$$

In general we fix residue classes a and $b \pmod q$, 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

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

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 $n \ge 0$. The values of $u_0, \cdots, u_{D-1}$ depend on a and $b \pmod d$ and are somewhat complicated to describe – see section 2 for precise details.

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

$$
B_{p-1}\left(\frac{a}{q}\right) - B_{p-1} \equiv \sum_{d|q} \frac{1}{2p}\left\{u_p(d;a,b) - (\phi(d) - \mu(d))\right\} \pmod p \tag{5}
$$

where b is the least positive residue of $p \pmod q$ (and μ is the Möbius function). Each term in the sum is a p-unit.

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

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

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 $(X_n)_{n\ge0}$ for which $X_p\equiv 0 \bmod p^2$ 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 well known that any sum of recurrence sequences can be written as one recurrence sequence, though of higher order. Thus (5) can be rewritten

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

where, now, U_n has characteristic polynomial

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

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 ≥ 3 and $1\le a\le q$ with $(a,q)=1$, then*

$$(8)\qquad B_{p-1}\left(\frac{a}{q}\right)-B_{p-1}\equiv\frac{q}{2p}\left\{x_p-1\right\}\pmod p$$

whenever $p\equiv\pm a \pmod q$ where $\{x_n\}_{n\ge0}$ is the $\frac{q-1}{2}$th order recurrence sequence given by

$$x_n=\frac{1}{2}\binom{2n}{n},\qquad 0\le n\le\frac{q-1}{2};$$

and for $D=\frac{q-1}{2}$ 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

$$f_k = \sum_{0 \le j \le [\frac{1}{2}(D-k)]} \frac{(D-j)!}{j!(D-2j-k)!} \quad (-1)^j 2^{D-2j-k}$$

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 $1 \le a \le 6$, and any odd prime $p \ne 7$,

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

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_0, U_1, U_2 are given in the table below:

$\pm a$	$\pm b$	U_0	U_1	U_2
2	1	5/7	1	2
3	2	5/7	2	7
1	3	5/7	2	6
3	1	6/7	1	2
1	2	6/7	3	11
2	3	6/7	2	5
a	a	3/7	1	3

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

$$(9)\qquad B_{p-1,(\frac{\cdot}{q})} := \sum_{a=1}^{q-1}\left(\frac{a}{q}\right)\left\{B_{p-1}\left(\frac{a}{q}\right)-B_{p-1}\right\} \equiv -2\left(\frac{p}{q}\right)qh_qV \pmod p.$$

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 both Hugh Williams and the anonymous referee for many useful comments.

1. The (regular) theory of Bernoulli polynomials.

The nth Bernoulli number B_n is defined by the power series

$$(1.1)\qquad \frac{x}{e^x-1}=\sum_{n\ge 0}B_n\,\frac{x^n}{n!}$$

The nth Bernoulli polynomial $B_n(t)$ is defined by the power series

$$(1.2)\qquad \frac{xe^{tx}}{e^x-1}=\sum_{n\ge 0}B_n(t)\,\frac{x^n}{n!}$$

so that $B_n(0)=B_n$ and

$$(1.3)\qquad B_n(t)=\sum_{j=0}^{n}\binom{n}{j}B_jt^{n-j}.$$

Perhaps the most important property of Bernoulli polynomials is that

$$(1.4)\qquad B_n(t+1)-B_n(t)=nt^{n-1}\quad\text{for all } n\ge 1$$

as is easily deduced from (1.2). From (1.4) we notice that $B_n(1)=B_n(0)=B_n$ for all $n\ne 1$, 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

$$B_n(0) = B_n(1) = B_n \quad \text{for } n \neq 1,$$

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

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

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

$$B_n(1-t) = (-1)^n B_n(t) \tag{1.5}$$

from the identity

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

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

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

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

and, in particular if $a = 0$,

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

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

$$\sum_{\substack{j=0 \\ (j,q)=1}}^{q-1} B_n\left(\frac{j}{q}\right) = \left(\sum_{d|q} \mu(d)\left(\frac{q}{d}\right)^{1-n}\right) B_n. \tag{1.8}$$

Using (1.5) we have, for all $q \geq 3$ and n even,

$$\sum_{\substack{1\le j<q/2\\(j,q)=1}} B_n\left(\frac{j}{q}\right) = \frac{1}{2}\, q^{1-n} \prod_{p\mid q}\left(1-p^{n-1}\right) B_n. \tag{1.9}$$

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 $n \geq 2$,

$$\sum_{\substack{1\le j<q/2\\(j,q)=1}} \left(B_n\left(\frac{j}{q}\right) - B_n\right) = \frac{qB_n}{2} \sum_{d\mid q} \frac{\mu(d)}{d}\left(\left(\frac{q}{d}\right)^{-n} - 1\right).$$

Taking $n = p-1$ we thus obtain

$$\begin{aligned}\sum_{\substack{1\le j<q/2\\(j,q)=1}} \left(B_{p-1}\left(\frac{j}{q}\right) - B_{p-1}\right) &\equiv \frac{1}{2}\sum_{d\mid q}\mu(d)\,\frac{\{(q/d)^p-(q/d)\}}{p}\\ &\equiv \frac{\phi(q)}{2}\left(\frac{q^{p-1}-1}{p} + \sum_{\substack{l\mid q\\ l \text{ prime}}} \frac{l^{p-1}-1}{p(l-1)}\right) \pmod{p}\end{aligned}$$

However such a formula only allows us to evaluate $B_n(a/q)$, for particular values of a coprime to q, provided $\phi(q) \le 2$. It is the main purpose of this paper to determine the value of

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

2. Working with roots of unity.

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

$$B_{p-1}\left(\frac{a}{q}\right) - B_{p-1} \equiv \sum_{\substack{\gamma^q=1\\ \gamma\ne 1}} \left(\frac{\gamma^a - 2 + \gamma^{-a}}{\gamma^p - 2 + \gamma^{-p}}\right)\left(\frac{(1-\gamma)^p - 1 + \gamma^p}{p}\right) \pmod p. \tag{2.1}$$

Proof: If $\gamma^q = 1$ then

$$\frac{(1-\gamma)^p - 1 + \gamma^p}{p} = \sum_{j=1}^{p-1} \frac{1}{p}\binom{p}{j}(-1)^j\gamma^j \equiv -\sum_{j=1}^{p-1}\frac{\gamma^j}{j} \pmod p$$

since

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

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 $m \equiv a/p \bmod q$ into the identity

$$\frac{x^m - 2 + x^{-m}}{x - 2 + x^{-1}} = m + \sum_{i=1}^{m}(m-i)(x^i + x^{-i}). \tag{2.2}$$

Therefore the righthand side of (2.1) is

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

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

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

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

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

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

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

$$x \sum_{k=0}^{(mp-a)/q} e^{kx} = x\, \frac{e^{(mp-a+q)/q\, x} - 1}{e^x - 1}$$

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 $p-1$ 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.

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

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

Proof: It is evident that

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

Therefore

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

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

Thus

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

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

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

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 γ and γ^{-1} terms.

Corollary 2. *If $q\geq 3$, $1\leq a\leq q$ and odd prime p does not divide q then*
(2.4)
$$\sum_{d|q}\mu\left(\frac{q}{d}\right)B_{p-1}\left(\frac{a_d}{d}\right)\equiv\frac{1}{2}\sum_{\substack{j=1\\(j,q)=1}}^{q/2}\left(2-(w^{ja}+w^{-ja})\right)\frac{1}{p}\left(\frac{(2-w^j-w^{-j})^p}{2-w^{jp}-w^{-jp}}-1\right) \pmod p$$

where $w=e^{2i\pi/q}$ and a_d is the least positive residue of $a \pmod d$.

Next note that if $(a,q)=1$ then

$$\sum_{\substack{j=1\\(j,q)=1}}^{q/2}(2-w^{ja}-w^{-ja})=\phi(q)-\sum_{\substack{i=1\\(i,q)=1}}^{q}w^i=\phi(q)-\mu(q).$$

Thus if we define

$$u_n(q;a,b):=\sum_{\substack{j=1\\(j,q)=1}}^{q/2}\left(\frac{2-w^{ja}-w^{-ja}}{2-w^{jb}-w^{-jb}}\right)(2-w^j-w^{-j})^n,$$

where a, b are taken $\pmod q$, then by Corollary 2,

$$\sum_{d|q} \mu\left(\frac{q}{d}\right) B_{p-1}\left(\frac{a_d}{d}\right) \equiv \frac{1}{2p}\left\{u_p(q; a, p \bmod q) - (\phi(q) - \mu(q))\right\} \pmod p.$$

Now u_n so defined is a recurrence sequence with characteristic polynomial

$$F_q(X) := \prod_{\substack{j=1 \\ (j,q)=1}}^{q/2} (X - 2 + w^j + w^{-j}) .$$

Note that

$$\begin{aligned} F_q((1-X^{-1})(1-X)) &= \prod_{\substack{j=1 \\ (j,q)}}^{q/2} \left(-\frac{1}{X}\right)(X - w^j)(X - w^{-j}) \\ &= (-X^{-1})^{\phi(q)/2}\phi_q(X) \end{aligned}$$

where $\phi_q(X)$ is the qth cyclotomic polynomial.

If $F(X) = X^D - \sum_{i=0}^{D-1} f_i X^i$ where $D = \phi(q)/2$, then

$$u_{n+D} = f_{D-1}u_{n+D-1} + f_{D-2}u_{n+D-2} + \cdots + f_0 u_n \quad \text{for all } n \ge 0.$$

We get the same recurrence relation for all u_n with a given q, but the starting values, $u_0, u_1, \cdots, u_{D-1}$, are different.

Let's define

$$V_n(q; k) = \sum_{\substack{j=1 \\ (j,q)=1}}^{q} w^{jk}(2 - w^j - w^{-j})^n$$

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

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

so we may find the starting values, $u_0, \cdots, u_{D-1}$ given those of $V_0, \cdots, V_{D-1}$. Now, for $0 \le n < \phi(q)/2 = D$, we have

$$\begin{aligned} V_n(q;k) &= \sum_{\substack{j=1 \\ (j,q)=1}}^{q} w^{jkb}(2 - w^j - w^{-j})^n = \sum_{\substack{j=1 \\ (j,q)=1}}^{q} (-1)^n w^{j(bk-n)}(1-w^j)^{2n} \\ &= \sum_{m=0}^{2n} \binom{2n}{m} (-1)^{n+m} \sum_{\substack{j=1 \\ (j,q)=1}}^{q} w^{j(bk+m-n)} \\ &= \sum_{m=0}^{2n} \binom{2n}{m} (-1)^{n+m} \sum_{d|q, d|m+bk-n} \mu\left(\frac{q}{d}\right) d. \\ &= \sum_{d|q} \mu\left(\frac{q}{d}\right) d \sum_{\substack{m=0 \\ m \equiv n - bk \bmod d}}^{2n} \binom{2n}{m} (-1)^{n+m}, \end{aligned}$$

since

$$\sum_{\substack{j=1 \\ (j,q)=1}}^{q} w^{jl} = \sum_{\substack{d|q \\ q|dl}} q \, \frac{\mu(d)}{d} = \sum_{r|(l,q)} \mu\left(\frac{q}{r}\right) r,$$

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 $w = e^{2i\pi/q}$,

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

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 χ is principal we thus obtain from $(1.7)_q$,

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

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

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

As an example we'll consider χ, 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 χ is an even character. Then

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

$$\text{where}\qquad \Sigma_q\equiv\sum_{j=0}^{q-1}\left(\frac{j}{q}\right)\left(\frac{(2-w^j-w^{-j})^p}{2-w^{pj}-w^{-pj}}-1\right)\pmod{p^2}.$$

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

$$\frac{(2-w^j-w^{-j})^p}{2-w^{pj}-w^{-pj}}-1\equiv \log_p\left(\frac{(2-w^j-w^{-j})^p}{2-w^{pj}-w^{-pj}}\right)\pmod{p^2},$$

we deduce that

$$\begin{aligned}\Sigma_q&\equiv\sum_{j=0}^{q-1}\left(\frac{j}{q}\right)\log_p\left(\frac{(2-w^j-w^{-j})^p}{2-w^{pj}-w^{-pj}}\right)\pmod{p^2}\\&\equiv\log_p\left(\frac{\prod_{j=1}^{q-1}(2-w^j-w^{-j})^{p(\frac{j}{q})}}{\prod_{i=1}^{q-1}(2-w^i-w^{-i})^{(\frac{pi}{q})}}\right)\pmod{p^2}\\&\equiv\log_p\left(\prod_{i=1}^{q-1}(2-w^i-w^{-i})^{(\frac{i}{q})(p-(\frac{p}{q}))}\right)\pmod{p^2}\\&\equiv 2\log_p\left(\prod_{i=1}^{q-1}(1-w^i)^{(\frac{i}{q})(p-(\frac{p}{q}))}\right)\pmod{p^2},\end{aligned}$$

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

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

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

$$\sum_{a=1}^{q-1} \left(\frac{a}{q}\right) \left\{ B_{p-1}\left(\frac{a}{q}\right) - B_{p-1} \right\} \equiv \frac{-1}{p}\, g\left(\left(\frac{\cdot}{q}\right)\right) h\left(\sqrt{q}\right) \log_p\left(\varepsilon_q^{2\left(p-\left(\frac{p}{q}\right)\right)}\right) \pmod p.$$

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

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

Then

$$1 = \varepsilon_q^{2(p-\left(\frac{p}{q}\right))} \overline{\varepsilon}_q^{2(p-\left(\frac{p}{q}\right))} \equiv (1+pu')^2 - (pv'\sqrt{q})^2 \equiv 1 + 2pu' \pmod{p^2},$$

so that p divides u'. So if

$$x_n = \frac{\varepsilon_q^n - \overline{\varepsilon}_q^n}{2v\sqrt{q}} \quad \text{then} \quad \varepsilon_q^{2(p-\left(\frac{p}{q}\right))} \equiv 1 + v x_{2(p-\left(\frac{p}{q}\right))}\sqrt{q} \pmod{p^2}.$$

Therefore $\log_p(\varepsilon_q^{2(p-\left(\frac{p}{q}\right))}) \equiv v x_{2(p-\left(\frac{p}{q}\right))}\sqrt{q} \pmod{p^2}$, and since $g\left(\left(\frac{\cdot}{q}\right)\right) = \sqrt{q}$ (which was proved first by Gauss), we have

$$\sum_{a=1}^{q-1} \left(\frac{a}{q}\right) \left\{ B_{p-1}\left(\frac{a}{q}\right) - B_{p-1} \right\} \equiv \frac{-q}{p}\, h(\sqrt{q}) v x_{2\left(p-\left(\frac{p}{q}\right)\right)} \pmod p; \tag{3.1}$$

this is equivalent to (9).

4. Proof of the Theorem.

Take $p \equiv \pm a \pmod q$ in Corollary 1 to get

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

Now $\frac12\sum_{\gamma^q=1}(2-\gamma^p-\gamma^{-p})=q$. Thus, for $x_n=\frac{1}{2q}\sum_{\gamma^q=1}(2-\gamma-\gamma^{-1})^n$, we obtain (8). Now if $0\le n\le\frac{q-1}{2}$ then

$$\begin{aligned}x_n=&\frac{1}{2q}\sum_{\gamma^q=1}(-\gamma^{-1})^n(1-\gamma)^{2n}\\ =&\frac12\sum_{m=0}^{2n}\binom{2n}{m}(-1)^{n+m}\,\frac1q\sum_{\gamma^q=1}\gamma^{m-n}\\ =&\frac12\binom{2n}{n}.\end{aligned}$$

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

$$\begin{aligned}\sum_{j\ge0}(-1)^j\binom{m-j}{j}(X+X^{-1})^{m-2j}&=\sum_{j\ge0}(-1)^j\binom{m-j}{j}\sum_{i\ge0}\binom{m-2j}{i}X^{m-2j-2i}\\ &=\sum_{k\ge0}X^{m-2k}\left(\sum_{j=0}^{k}\binom{m-j}{j}\binom{m-2j}{k-j}(-1)^j\right)\end{aligned}$$

taking $i+j=k$. The inner sum

$$\begin{aligned}&=\sum_{j=0}^{k}\binom{k}{j}\binom{m-j}{k}(-1)^j\\ &=\sum_{j=0}^{k}\text{ coeff of }T^j\text{ in }(1-T)^k*\text{ coeff of }T^{m-k-j}\text{ in }(1-T)^{-k-1}\\ &=\text{ coeff of }T^{m-k}\text{ in }(1-T)^{-1}=\begin{cases}1&\text{if }k\le m\\0&\text{otherwise.}\end{cases}\end{aligned}$$

Thus

$$\sum_{j\ge0}(-1)^j\binom{m-j}{j}(X+X^{-1})^{m-2j}=\sum_{\substack{i=-m\\ i=m\pmod 2}}^{m}X^i\ .$$

So define

$$F_q(y):=\sum_{j\ge0}(-1)^j\binom{\frac{q-1}{2}-j}{j}(2-y)^{\frac{q-1}{2}-2j}+\sum_{i\ge0}(-1)^i\binom{\frac{q-3}{2}-i}{i}(2-y)^{\frac{q-3}{2}-2i}.\tag{4.1}$$

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

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

$$+\sum_{i\ge 0}(-1)^i\binom{\frac{q-3}{2}-i}{i}(w^k+w^{-k})^{\frac{q-3}{2}-2i} = \sum_{l=-(\frac{q-1}{2})}^{\frac{q-1}{2}} w^{kl} = 0$$

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

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

$$f_k = \sum_{j=0}^{\frac{1}{2}(\frac{q-1}{2}-k)} \frac{(\frac{q-1}{2}-j)!}{j!(\frac{q-1}{2}-2j-k)!}(-1)^j 2^{\frac{q-1}{2}-2j-k}.$$

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* $\{x_n\}_{n\ge 0}$ is defined by $x_0 = 0$, $x_1 = 1$ and $x_n = bx_{n-1} - cx_{n-2}$ for all $n \ge 2$, 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

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

Thus

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

Therefore $x_{p-(\frac{D}{p})} \equiv 0 \pmod p$ and

$$c^{p-(\frac{D}{p})} = \alpha^{p-(\frac{D}{p})}\beta^{p-(\frac{D}{p})} = \frac{y^2_{p-(\frac{D}{p})} - Dx^2_{p-(\frac{D}{p})}}{4} \equiv \frac{y^2_{p-(\frac{D}{p})}}{4} \pmod{p^2}.$$

Therefore $y_{p-(\frac{D}{p})} \equiv 2c^{\frac12(1-(\frac{D}{p}))}\left(\frac{c^{p-1}+1}{2}\right) \pmod{p^2}$. In fact $c = \pm 1$ in every case below so that

$$\alpha^{p-(\frac{D}{p})}, \beta^{p-(\frac{D}{p})} \equiv \begin{cases} 1 \pm p\sqrt{D}\ \left(\frac{1}{2p}x_{p-(\frac{D}{p})}\right) \pmod{p^2} & \text{if } c = 1; \\ (\frac{D}{p}) \pm p\sqrt{D}\ \left(\frac{1}{2p}x_{p-(\frac{D}{p})}\right) \pmod{p^2} & \text{if } c = -1; \end{cases} \tag{5.1}$$

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 qth root w of 1, and let $\alpha_j = 2 - w^j - w^{-j}$. By Corollary 2

$$\begin{aligned} \sum_{d|q} \mu\left(\frac{q}{d}\right) B_{p-1}\left(\frac{a_d}{d}\right) \equiv & \frac{1}{2p}\left\{\frac{\alpha_a}{\alpha_p}\,\alpha_1^p + \frac{\alpha_{at}}{\alpha_{pt}}\,\alpha_t^p - (\alpha_a + \alpha_{at})\right\} \pmod p \\ \equiv & \frac{1}{2p}\left\{\frac{1}{C'}\left(\alpha_a\alpha_1^{p-(\frac{p}{q})} + \alpha_{at}\alpha_t^{p-(\frac{p}{q})}\right) - B\right\} \pmod p \end{aligned} \tag{5.2}$$

where $B = \alpha_1 + \alpha_t$, $C = \alpha_1\alpha_t$ and $C' = C$ if $\left(\frac{p}{q}\right) = -1$, 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 $\alpha_j = \frac12\sqrt5\left(\sqrt5 + \left(\frac{j}{5}\right)\right)$ for $1 \le j \le 4$. Let $\alpha = (1+\sqrt5)/2$ and $\beta = (1-\sqrt5)/2$. By substituting into (5.2) and then using (5.1) (with $b = 1$, $c = -1$ so that $x_n = F_n$) we get

$$\begin{aligned} B_{p-1}\left(\frac{a}{5}\right) - B_{p-1} \equiv & \frac{5}{2p}\left\{\frac{5^{(p-1)/2}}{2\sqrt5}\left(\left(\sqrt5 + \left(\frac{a}{5}\right)\right)\alpha^{p-(\frac{p}{5})} + \left(\sqrt5 - \left(\frac{a}{5}\right)\right)\beta^{p-(\frac{p}{5})}\right) - 1\right\} \\ \equiv & \frac{5}{2p}\left\{5^{(p-1)/2}\left(\left(\frac{p}{5}\right) + p\frac{1}{2p}F_{p-(\frac{p}{5})}\left(\frac{a}{5}\right)\right) - 1\right\} \\ \equiv & \frac54\left\{\left(\frac{5^{p-1}-1}{p}\right) + \left(\frac{ap}{5}\right)\,\frac1p F_{p-(\frac{p}{5})}\right\} \pmod p \end{aligned}$$

giving the first congruence in (4), since $5^{\frac{p-1}{2}} \equiv \left(\frac{5}{p}\right)\left(1 + \frac12\left(5^{p-1}-1\right)\right) \pmod{p^2}$.

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

$$\begin{aligned} B_{p-1}\left(\frac{1}{10}\right) &= 2^{2-p}B_{p-1}\left(\frac15\right) - B_{p-1}\left(\frac35\right) \\ B_{p-1}\left(\frac{3}{10}\right) &= 2^{2-p}B_{p-1}\left(\frac35\right) - B_{p-1}\left(\frac45\right). \end{aligned}$$

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

$$\begin{aligned}
&\equiv \frac{2}{p}\left\{\frac{2^{(p-1)/2}}{2\sqrt{2}}\left(\left(\sqrt{2}+\left(\frac{a}{8}\right)\right)\alpha^{p-\left(\frac{p}{8}\right)} + \left(\sqrt{2}-\left(\frac{a}{8}\right)\right)\beta^{p-\left(\frac{p}{8}\right)}\right) - 1\right\} \\
&\equiv \frac{2}{p}\left\{2^{(p-1)/2}\left(\left(\frac{p}{8}\right) + p\frac{1}{p}G_{p-\left(\frac{p}{8}\right)}\left(\frac{a}{8}\right)\right) - 1\right\} \\
&\equiv \left(\frac{2^{p-1}-1}{p}\right) + 2\left(\frac{ap}{8}\right)\ \frac{1}{p}G_{p-\left(\frac{p}{8}\right)} \pmod{p}
\end{aligned}$$

since $2^{\frac{p-1}{2}} \equiv \left(\frac{p}{8}\right)\left(1+\frac{1}{2}\left(2^{p-1}-1\right)\right) \pmod{p^2}$. 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 $\alpha_j = 2 + \left(\frac{j}{12}\right)\sqrt{3}$ 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

$$\begin{aligned}
&\equiv \frac{1}{2p}\left\{\left(\left(2+\left(\frac{a}{12}\right)\sqrt{3}\right)\alpha^{p-\left(\frac{p}{12}\right)} + \left(2-\left(\frac{a}{12}\right)\sqrt{3}\right)\beta^{p-\left(\frac{p}{12}\right)}\right) - 4\right\} \\
&\equiv 3\left(\frac{a}{12}\right)\frac{1}{p}H_{p-\left(\frac{p}{12}\right)} \pmod{p}.
\end{aligned}$$

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

References

[AM] Almkvist, G. and Meurman, A., , Values of Bernoulli polynomials and Hurwitz's zeta function at rational points , *C.R. Math. Rep. Acad. Sci. Canada* **13** (1991) 104–108.

[An] Andrews, G. H. , Some formulae for the Fibonacci sequence with generalizations , *Fib. Quart.* **7** (1969) 113–130.

[FT] Friedmann A. and Tamarkine J. , Quelques formules concernent la théorie de la fonction [x] et des nombres de Bernoulli , *J. Reine Angew. Math* **137** (1909) 146–156.

[Gr] Granville, A. , On the Kummer-Wieferich-Skula criteria for the first case of Fermat's Last Theorem , in '*Advances in Number Theory*', ed. F.Q. Gouvêa and N. Yui (Oxford, Midsomer Norton, 1993) 479–498.

[KS] Kiselev, A.A. and Slavutskiĭ, I.Š. , On the number of classes of ideals of a quadratic field and its rings (Russian) , *Dokl. Akad. Nauk SSSR* **126** (1959) 1191–1194.

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

[Lr] Lerch, M. , Zur Theorie des Fermatschen Quotienten $(a^{p-1}-1)/p = q(a)$, *Math. Ann.* **60** (1905) 471–490.

[Ri] Ribenboim, P. , *13 Lectures on Fermat's Last Theorem* , (Springer, New York, 1979).

[Sk] Skula, L. , Fermat's Last Theorem (1^{st} Case) and the Fermat quotients, *Comm. Math. Univ. Sancti. Pauli* **41** (1992) 35–54.

[SS] Sun, Z-H and Sun, Z-W , Fibonacci numbers and Fermat's Last Theorem , *Acta Arith.* **60** (1992) 371-388.

[Wa] Washington, L.C. , Introduction to Cyclotomic Fields , (Springer, New York, 1982).

[W1] Williams, H. C. , A note on the Fibonacci quotient $F_{p-\epsilon/p}$, *Can. Math. Bull* **25** (1982) 366-370.

[W2] Williams, H. C. , Some formulas concerning the fundamental unit of a real quadratic field , *Disc. Math.* **92** (1991) 431-440.

(Granville) Department of Mathematics, University of Georgia, Athens, Ga 30602, USA

(Granville) Isaac Newton Institute for the Mathematical Sciences, 20 Clarkson Road, Cambridge CB2 OEH, England.

(Sun) Department of Mathematics, Nanjing University, Nanjing 210008, P. R. CHINA