On the Vanishing of the Iwasawa Invariant $\mu_p$
for $p < 8000$

By Wells Johnson

Abstract. The irregular primes less than 8000 are computed, and it is shown that the
Iwasawa invariant $\mu_p = 0$ for all primes $p < 8000$.

1. Introduction. Let $p = 2m + 1$ be an odd prime number, and let $F_n (n \geq 0)$
be the cyclotomic field of $p^{n+1}$th roots of unity over the rational field $\mathbb{Q}$. Let $p^{e(n)}$
be the exact power of $p$ which divides the class number $h_n$ of $F_n$. Iwasawa [4] has shown
that there exist integers $\mu_p \geq 0$, $\lambda_p \geq 0$ and $\nu_p$ such that
\[ e(n) = \mu_p p^n + \lambda_p n + \nu_p \]
for all $n$ sufficiently large. Iwasawa and Sims [7] have computed the cyclotomic invariants
$\mu_p$, $\lambda_p$, and $\nu_p$ for all primes $p \leq 4001$. In particular, they showed that $\mu_p = 0$
for every $p \leq 4001$.

In this paper, we derive some conditions on $p$ which are necessary if $\mu_p > 0$.
Computations have been performed which show that these conditions are not satisfied
for any prime $p$, $p < 8000$, so that $\mu_p = 0$ for all such primes. In particular, the
computations of $\mu_p$ in [7] have been verified, although these appear to have been
incomplete, since they were based upon the incomplete tables in the first paper of [8].

The author wishes to acknowledge the assistance of his colleagues, R. B. S. Brooks
and M. W. Curtis, in the preparation of the computer programs.

2. Notation. Let $\mathbb{Z}_p$ denote the ring of $p$-adic integers. Let $U$ be the group of
units of $\mathbb{Z}_p$ and let $V$ denote the cyclic subgroup of $U$ consisting of the $(p - 1)$st roots
of unity.

Any $x$ in $\mathbb{Z}_p$ has the $p$-adic representation
\[ x = \sum_{k=0}^{\infty} x_k p^k, \]
where the $x_k$ are rational integers satisfying $0 \leq x_k < p$ for $k \geq 0$. In the following,
the subscript notation $x_k$ will always denote the coefficient of $p^k$ in the $p$-adic expansion
of the $p$-adic integer $x$. If $x$ is given as above, we define the truncated sum $s_n(x)$ by
\[ s_n(x) = \sum_{k=0}^{n} x_k p^k. \]
Thus, \( x \equiv s_n(x) \pmod{p^{n+1}} \) and \( 0 \leq s_n(x) < p^{n+1} \) for all \( n \geq 0 \).

For any rational integer \( a, 1 \leq a \leq p - 1 \), we let \( \sigma(a) \) denote the unique member of \( V \) satisfying \( \sigma(a) \equiv a \pmod{p} \). In particular, we always have \( \sigma(a)_0 = a \).

We use the so-called “even-index” notation for the sequence of Bernoulli numbers, \( B_n \). This notation and the basic results on Bernoulli numbers used here are given in [1].

### 3. Results of Iwasawa

Iwasawa ([3], [5], and [6]) has proved the following fundamental theorem on the cyclotomic invariant \( \mu_p \):

**Theorem 1.** \( \mu_p > 0 \) if and only if there exists an odd index \( i, 1 \leq i \leq p - 4 \), such that

\[
\sum_{u \in V} s_n(u^i) \equiv 0 \pmod{p^{n+2}}
\]

for all units \( u \in U \) and for all \( n \geq 0 \).

In [3], Iwasawa proves the equivalence of (1) with another set of congruences modulo \( p \), using the relation \( (u^i)_n^p = s_n(u^i) = s_{n-1}(u^i) \) for \( n \geq 1 \):

**Theorem 2.** \( \mu_p > 0 \) if and only if there exists an odd index \( i, 1 \leq i \leq p - 4 \), such that

\[
\sum_{u \in V} (u^i)_n \equiv 0 \pmod{p}
\]

for all \( u \in U \) and for all \( n \geq 1 \).

By choosing \( u = 1 \) in Theorems 1 and 2, we obtain

**Theorem 3.** If \( \mu_p > 0 \), then there exists an odd index \( i, 1 \leq i \leq p - 4 \), such that

(1) \[
\sum_{u \in V} s_n(u^i) \equiv 0 \pmod{p^{n+2}}
\]

and

(2) \[
\sum_{u \in V} v_n^i \equiv 0 \pmod{p}
\]

for all \( n \geq 1 \).

It is known from the general theory of \( \Gamma \)-extensions that \( \mu_p = 0 \) for all regular primes \( p \) (see [11] for a nice proof). We show next how this follows at once from Theorem 3.

**Corollary.** If \( \mu_p > 0 \), then there exists an odd index \( i, 1 \leq i \leq p - 4 \), such that

\( B_{i+1} \equiv 0 \pmod{p} \). Hence \( p \) is an irregular prime.

**Proof.** Part (1) of Theorem 3 implies that

\[
\sum_{u \in V} s_n(v_0 + v_1p)^i \equiv \sum_{u \in V} v_0^{i+1} + p \sum_{u \in V} v_1v_0^i \equiv 0 \pmod{p^2}.
\]

But the second term is \( 0 \pmod{p^2} \) by part (2) of Theorem 3. Hence

\[
B_{i+1} \equiv \sum_{a=1}^{p-1} a^{i+1} \equiv \sum_{u \in V} v_0^{i+1} \equiv 0 \pmod{p^2},
\]

as desired.

### 4. Additional Conditions for Positive \( \mu_p \)

In this section, we investigate the implications of Theorem 2 for different choices of the units \( u \in U \), obtaining additional necessary conditions that \( \mu_p \) be positive.

**Theorem 4.** If \( \mu_p > 0 \), then there exists an odd index \( i, 1 \leq i \leq p - 4 \), such that
(1) \[ B_{i+1} \equiv 0 \pmod{p}, \]

(2) \[ \sum_{a=1; a+i(a) \leq p}^{p-1} a^i \equiv \sum_{a=1; a+i(a) \leq 2p}^{p-1} a^i \equiv 0 \pmod{p} \quad \text{for all } n \geq 1. \]

Proof. We have already seen that (1) is true. If \( n \geq 1 \) and \( v \in V \), we can write

\[ v \equiv v_0 + v_1 p + \cdots + v_{n+1} p^{n+1} \pmod{p^{n+2}}. \]

For \( u = 1 + p^n \), we have

\[ uv = v_0 + \cdots + v_{n-1} p^{n-1} + (v_0 + v_n) p^n + (v_1 + v_{n+1}) p^{n+1} \pmod{p^{n+2}}. \]

Thus, if \( v_0 + v_n < p \), we have that \((uv)_n = v_0 + v_n \) and \((uv)_{n+1} = v_1 + v_{n+1} \pmod{p}\).

However, if \( v_0 + v_n \geq p \), then \((uv)_n = v_0 + v_n - p \) and \((uv)_{n+1} = v_1 + v_{n+1} + 1 \pmod{p} \).

By Theorem 2, \( \sum_{s \in V} (uv)_{n+1} v^i \equiv 0 \pmod{p} \), or

\[ \sum_{s \in V} (v_1 + v_{n+1}) v^i + \sum_{s \in V; s \neq a+i(a) \leq 2p} v_0^i \equiv 0 \pmod{p}. \]

But by Theorem 3, the first sum is \( 0 \pmod{p} \), and therefore, so is the second. Since \( \sum_{s \in V} v_0^i \equiv 0 \pmod{p} \), we have

\[ \sum_{s \in V; s \neq a+i(a) \leq 2p} v_0^i \equiv \sum_{s \in V; s \neq a+i(a) \leq 2p} v_i^0 \equiv 0 \pmod{p}, \]

which is the same as (2).

We remark that for several other choices of the unit \( u \) in Theorem 2 (e.g., \( u = p - 1 \) and \( u = 1 + 2p^n \)) we have derived additional congruences which are also necessary conditions for \( \mu_p > 0 \). These are omitted here since they are not required for any of our computations. We have selected the congruences of Theorem 4 since they lead (in the next section) to a sum with relatively few terms, thus providing for the greatest computational efficiency.

5. Main Theorem. For the actual computation of \( \mu_p \) for \( p < 8000 \), it was necessary to use Theorem 4 only in the case that \( n = 1 \). In this section, we derive some simplifications of Theorem 4 when \( n = 1 \).

By expanding the congruence

\[ 1 = v(a)^{p-1} \equiv (a + v(a), p)^{p-1} \pmod{p^2}, \]

we see that \( v(a) \) is completely determined by the conditions

(2) \[ v(a) \equiv (a^p - a) / p \pmod{p} \quad \text{and} \quad 0 \leq v(a) < p. \]

It is easy to see by (2) that

(3) \[ v(a) + v(p - a) = p - 1, \quad 1 \leq a \leq p - 1. \]

It follows immediately that \( a + v(a), < p \) if and only if \( (p - a) + v(p - a) \geq p \), so that, letting \( b = p - a \) and recalling that \( i \) is odd, we obtain

\[ \sum_{a=1; a+i(a) \leq p}^{p-1} a^i \equiv - \sum_{b=m+1; b+i(b) \leq 2p}^{p-1} b^i \pmod{p}. \]
By the Mirimanoff congruence [9]

\[ 2^i(i + 1) \sum_{a=1}^{m} a^i \equiv (1 - 2^{i+1}) B_{i+1} \pmod{p}, \]

we see that \( B_{i+1} \equiv 0 \pmod{p} \) implies that

\[ \sum_{a=1}^{m} a^i \equiv \sum_{a=m+1}^{p-1} a^i \equiv 0 \pmod{p}. \]

Combining the above congruences with the results of Theorem 4, we arrive at our main result:

**Theorem 5.** If \( \mu_p > 0 \), then there exists an odd index \( i, 1 \leq i \leq p - 4 \), such that

1. \( B_{i+1} \equiv 0 \pmod{p} \), and
2. \( \sum_{a=1}^{m} a^i \equiv 0 \pmod{p} \).

The computations of Theorem 5 were carried out on the PDP-10 computer at Bowdoin College for all primes \( p < 8000 \), and the results are included in the Table accompanying this paper. About 60 hours of computing time were required for all the computations, the bulk of it in the search for the irregular primes and for the Bernoulli numbers satisfying (1). For no prime \( p < 8000 \) is the conclusion of Theorem 5 satisfied, so that we have

**Theorem 6.** The Iwasawa invariant \( \mu_p = 0 \) for all primes \( p < 8000 \).

A more detailed explanation of how the computations of Theorem 5 were carried out is given in the following sections.

6. The Irregular Primes. The first condition of Theorem 5, that involving the Bernoulli numbers, has been of interest since Kummer's fundamental work on Fermat's Last Theorem in the nineteenth century. In a series of papers, Vandiver and others [8] claimed to have found all ordered pairs \((p, i + 1)\) satisfying \( B_{i+1} \equiv 0 \pmod{p} \), for \( p \leq 4001 \). They then verified that Fermat's Last Theorem is true for all exponents in this range. These pairs were used by Iwasawa and Sims [7] for their computation of the cyclotomic invariants \( \mu_p, \lambda_p, \) and \( \nu_p \) for primes \( p \leq 4001 \).

Our approach to finding these pairs was somewhat different from that used in [8]. The Bernoulli numbers satisfy the recursion relation

\[ \sum_{j=0}^{k} \binom{k+1}{j} B_j = 0, \]

with \( B_0 = 1 \). Computing the binomial coefficients \( \pmod{p} \), we can use the above to compute \( B_k \pmod{p} \) recursively. This requires, of course, that we store the \( B_j \)'s as we go along. Since \( B_j = 0 \) for \( j \) odd, \( j \geq 3 \), there are really only approximately \( k/2 \) terms in the sum defining \( B_k \).

Carlitz posed the following identity for the Bernoulli numbers as a problem in [2]:

\[ (-1)^m \sum_{r=0}^{m} \binom{m}{r} B_{n+r} = (-1)^n \sum_{s=0}^{n} \binom{n}{s} B_{m+s}, \quad m, n \geq 0. \]

If we let \( f(m, n) \) be the left-hand side of this equation, the problem is to show that \( f(m, n) = f(n, m) \) for all \( m, n \geq 0 \). This is easily done by induction on \( m \), using the
identity \( f(m + 1, n) = -f(m, n) - f(m, n + 1) \).

If we now consider the special case \( m = n + 1 \) in (5), we obtain

\[
\sum_{r=0}^{n} C(n, r)B_{n+r} = 0, \quad n \geq 1, \tag{6}
\]

where \( C(n, 0) = 1 \) and

\[
C(n, r) = \binom{n+1}{r} + \binom{n}{r-1} \quad \text{for} \quad 1 \leq r \leq n + 1.
\]

Equation (6) defines \( B_{2n} \) recursively in terms of \( B_n, B_{n+1}, \ldots, B_{2n-2} \), a considerable saving in computation time over the recursive relation (4). The coefficients \( C(n, r) \) are easily computed modulo \( p \), since they form a Pascal triangle whose first row is 1 2.

Using Eq. (6) modulo \( p \), we found all pairs \((p, i + 1)\) with \( B_{i+1} \equiv 0 \) (mod \( p \)) for all primes \( p < 8000 \), at which time the program was terminated, since each additional prime took an excessively long time to run. Four additions were found to the tables in the first paper of [8], and these are marked with an asterisk in the accompanying Table. These omissions also occur in the table on p. 430-431 of [1], and, presumably, in the table (not completely published) of [7].

In [8], a prime \( p \) was first tested for irregularity by means of the congruence

\[
2(i + 1) \sum_{p/5 < a < p/4} a^i \equiv (4^{p-i-1} + 3^{p-i-1} - 6^{p-i-1} - 1)B_{i+1} \pmod{p}
\]

which holds for \( p > 7 \). As a check on our computations, we ran another program for the four pairs \((p, i + 1)\) omitted from [8] as well as for those pairs for which \( 4002 < p < 8000 \). For each of these pairs, it was found that the sum on the left-hand side of the congruence above is 0 modulo \( p \), while the coefficient of \( B_{i+1} \) is not, so that indeed, \( B_{i+1} \equiv 0 \) (mod \( p \)).

Selfridge and Pollack [10] have found all pairs \((p, i + 1)\) with \( B_{i+1} \equiv 0 \) (mod \( p \)) for primes \( p < 25,000 \), and they have verified that Fermat's Last Theorem is true for all exponents less than or equal to 25,000 using the methods of [8]. A complete table of their calculations has not yet been published, but when it appears, we intend to use it to make further computations of the Iwasawa invariant \( \mu_p \). The validity of Fermat's Last Theorem for exponents less than or equal to 8000 was also verified by us in still another machine computation, using the criteria developed in [8].

7. Computation of the Sum in Theorem 5. In this section, we make some remarks on the algorithm that we devised for computing the sum in Theorem 5. The real problem lies in computing \( v(a)_i \) for \( a = 1, 2, \ldots, m \). This can be done, of course, by Eq. (2), but those computations really have to be done modulo \( p^2 \). Below, we indicate how certain of the \( v(a)_i \)'s can be found from others by means of a linear congruence modulo \( p \).

Clearly, \( v(1)_i = 0 \), so that the index \( a = 1 \) is never included in the sum. We first computed \( v(2)_i \), using Eq. (2). The following identities can be derived from (2) and (3):

\[
v(a)_i - 2v(a/2)_i - ((a/2)_i v(2)_i \equiv 0 \pmod{p} \quad (a \text{ even}),
\]

\[
v(a)_i + 2v((p - a)/2)_i + ((p - a)/2)v(2)_i + 1 \equiv 0 \pmod{p} \quad (a \text{ odd}).
\]

Hence, given \( v(a)_i \) for some \( a, 1 \leq a \leq m \), these identities may be used to compute either \( v(a/2)_i \), if \( a \) is even or \( v((p - a)/2)_i \), if \( a \) is odd, without resorting to Eq. (2).
<table>
<thead>
<tr>
<th>Term</th>
<th>Coefficients</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10, 9, 7, 8, 6, 5, 4, 3, 2, 1, 0</td>
</tr>
<tr>
<td>2</td>
<td>10, 9, 7, 8, 6, 5, 4, 3, 2, 1, 0</td>
</tr>
<tr>
<td>3</td>
<td>10, 9, 7, 8, 6, 5, 4, 3, 2, 1, 0</td>
</tr>
<tr>
<td>4</td>
<td>10, 9, 7, 8, 6, 5, 4, 3, 2, 1, 0</td>
</tr>
<tr>
<td>5</td>
<td>10, 9, 7, 8, 6, 5, 4, 3, 2, 1, 0</td>
</tr>
<tr>
<td>6</td>
<td>10, 9, 7, 8, 6, 5, 4, 3, 2, 1, 0</td>
</tr>
<tr>
<td>7</td>
<td>10, 9, 7, 8, 6, 5, 4, 3, 2, 1, 0</td>
</tr>
<tr>
<td>8</td>
<td>10, 9, 7, 8, 6, 5, 4, 3, 2, 1, 0</td>
</tr>
<tr>
<td>9</td>
<td>10, 9, 7, 8, 6, 5, 4, 3, 2, 1, 0</td>
</tr>
<tr>
<td>10</td>
<td>10, 9, 7, 8, 6, 5, 4, 3, 2, 1, 0</td>
</tr>
</tbody>
</table>

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
<table>
<thead>
<tr>
<th>(p)</th>
<th>(i+1)</th>
<th>(\text{terms})</th>
<th>(\text{sum})</th>
<th>(p)</th>
<th>(i+1)</th>
<th>(\text{terms})</th>
<th>(\text{sum})</th>
</tr>
</thead>
<tbody>
<tr>
<td>6287</td>
<td>4452</td>
<td>803</td>
<td>1358</td>
<td>7039</td>
<td>1454</td>
<td>604</td>
<td>4693</td>
</tr>
<tr>
<td>6287</td>
<td>5034</td>
<td>603</td>
<td>603</td>
<td>7057</td>
<td>4154</td>
<td>903</td>
<td>669</td>
</tr>
<tr>
<td>6317</td>
<td>2554</td>
<td>793</td>
<td>1653</td>
<td>7057</td>
<td>4972</td>
<td>903</td>
<td>3496</td>
</tr>
<tr>
<td>6329</td>
<td>5102</td>
<td>816</td>
<td>2169</td>
<td>7059</td>
<td>1470</td>
<td>850</td>
<td>3103</td>
</tr>
<tr>
<td>6337</td>
<td>3956</td>
<td>732</td>
<td>633</td>
<td>7069</td>
<td>2570</td>
<td>850</td>
<td>3586</td>
</tr>
<tr>
<td>6343</td>
<td>750</td>
<td>773</td>
<td>555</td>
<td>7109</td>
<td>570</td>
<td>887</td>
<td>3838</td>
</tr>
<tr>
<td>6343</td>
<td>5820</td>
<td>773</td>
<td>555</td>
<td>7121</td>
<td>1502</td>
<td>865</td>
<td>2851</td>
</tr>
<tr>
<td>6367</td>
<td>1110</td>
<td>750</td>
<td>2520</td>
<td>7127</td>
<td>6758</td>
<td>849</td>
<td>4876</td>
</tr>
<tr>
<td>6373</td>
<td>2838</td>
<td>803</td>
<td>4876</td>
<td>7177</td>
<td>962</td>
<td>884</td>
<td>1391</td>
</tr>
<tr>
<td>6373</td>
<td>4226</td>
<td>803</td>
<td>3447</td>
<td>7187</td>
<td>3906</td>
<td>945</td>
<td>6847</td>
</tr>
<tr>
<td>6379</td>
<td>218</td>
<td>779</td>
<td>342</td>
<td>7207</td>
<td>1670</td>
<td>972</td>
<td>1891</td>
</tr>
<tr>
<td>6421</td>
<td>438</td>
<td>793</td>
<td>1151</td>
<td>7207</td>
<td>5774</td>
<td>972</td>
<td>1800</td>
</tr>
<tr>
<td>6449</td>
<td>4894</td>
<td>775</td>
<td>3003</td>
<td>7211</td>
<td>898</td>
<td>906</td>
<td>3893</td>
</tr>
<tr>
<td>6449</td>
<td>5830</td>
<td>775</td>
<td>3431</td>
<td>7213</td>
<td>1436</td>
<td>893</td>
<td>2097</td>
</tr>
<tr>
<td>6451</td>
<td>3266</td>
<td>817</td>
<td>4290</td>
<td>7213</td>
<td>6330</td>
<td>893</td>
<td>2163</td>
</tr>
<tr>
<td>6491</td>
<td>346</td>
<td>807</td>
<td>2178</td>
<td>7229</td>
<td>6236</td>
<td>926</td>
<td>739</td>
</tr>
<tr>
<td>6521</td>
<td>236</td>
<td>816</td>
<td>3348</td>
<td>7309</td>
<td>324</td>
<td>890</td>
<td>1510</td>
</tr>
<tr>
<td>6529</td>
<td>1564</td>
<td>810</td>
<td>3664</td>
<td>7321</td>
<td>348</td>
<td>892</td>
<td>2405</td>
</tr>
<tr>
<td>6547</td>
<td>734</td>
<td>671</td>
<td>613</td>
<td>7351</td>
<td>1466</td>
<td>928</td>
<td>2133</td>
</tr>
<tr>
<td>6569</td>
<td>1692</td>
<td>833</td>
<td>2814</td>
<td>7411</td>
<td>4712</td>
<td>898</td>
<td>4054</td>
</tr>
<tr>
<td>6569</td>
<td>1776</td>
<td>813</td>
<td>3851</td>
<td>7449</td>
<td>5286</td>
<td>947</td>
<td>6940</td>
</tr>
<tr>
<td>6571</td>
<td>1744</td>
<td>774</td>
<td>3308</td>
<td>7487</td>
<td>2500</td>
<td>924</td>
<td>2778</td>
</tr>
<tr>
<td>6577</td>
<td>1312</td>
<td>814</td>
<td>5070</td>
<td>7499</td>
<td>4250</td>
<td>915</td>
<td>1314</td>
</tr>
<tr>
<td>6619</td>
<td>1552</td>
<td>829</td>
<td>6068</td>
<td>7499</td>
<td>5642</td>
<td>930</td>
<td>327</td>
</tr>
<tr>
<td>6619</td>
<td>3170</td>
<td>829</td>
<td>2729</td>
<td>7507</td>
<td>6324</td>
<td>921</td>
<td>5061</td>
</tr>
<tr>
<td>6559</td>
<td>2950</td>
<td>800</td>
<td>1532</td>
<td>7537</td>
<td>2264</td>
<td>945</td>
<td>7122</td>
</tr>
<tr>
<td>6559</td>
<td>4014</td>
<td>800</td>
<td>2968</td>
<td>7547</td>
<td>5644</td>
<td>914</td>
<td>3305</td>
</tr>
<tr>
<td>6669</td>
<td>5252</td>
<td>850</td>
<td>3333</td>
<td>7559</td>
<td>116</td>
<td>906</td>
<td>3207</td>
</tr>
<tr>
<td>6701</td>
<td>5848</td>
<td>833</td>
<td>2400</td>
<td>7591</td>
<td>2620</td>
<td>965</td>
<td>460</td>
</tr>
<tr>
<td>6733</td>
<td>1690</td>
<td>878</td>
<td>4596</td>
<td>7607</td>
<td>3594</td>
<td>934</td>
<td>1945</td>
</tr>
<tr>
<td>6763</td>
<td>4144</td>
<td>835</td>
<td>6633</td>
<td>7643</td>
<td>5026</td>
<td>960</td>
<td>6969</td>
</tr>
<tr>
<td>6763</td>
<td>6210</td>
<td>835</td>
<td>4046</td>
<td>7661</td>
<td>368</td>
<td>926</td>
<td>5662</td>
</tr>
<tr>
<td>6763</td>
<td>6300</td>
<td>835</td>
<td>2419</td>
<td>7687</td>
<td>1246</td>
<td>969</td>
<td>60</td>
</tr>
<tr>
<td>6779</td>
<td>3904</td>
<td>832</td>
<td>2092</td>
<td>7687</td>
<td>3216</td>
<td>969</td>
<td>192</td>
</tr>
<tr>
<td>6783</td>
<td>2686</td>
<td>852</td>
<td>2303</td>
<td>7687</td>
<td>6116</td>
<td>969</td>
<td>6570</td>
</tr>
<tr>
<td>6823</td>
<td>4052</td>
<td>865</td>
<td>6253</td>
<td>7691</td>
<td>2218</td>
<td>835</td>
<td>4092</td>
</tr>
<tr>
<td>6827</td>
<td>4108</td>
<td>854</td>
<td>6063</td>
<td>7727</td>
<td>950</td>
<td>829</td>
<td>4841</td>
</tr>
<tr>
<td>6833</td>
<td>2254</td>
<td>873</td>
<td>1146</td>
<td>7727</td>
<td>3756</td>
<td>929</td>
<td>1487</td>
</tr>
<tr>
<td>6833</td>
<td>5144</td>
<td>873</td>
<td>369</td>
<td>7817</td>
<td>7346</td>
<td>941</td>
<td>6876</td>
</tr>
<tr>
<td>6857</td>
<td>6676</td>
<td>820</td>
<td>2447</td>
<td>7823</td>
<td>3298</td>
<td>987</td>
<td>2519</td>
</tr>
<tr>
<td>6863</td>
<td>6406</td>
<td>859</td>
<td>6442</td>
<td>7829</td>
<td>1392</td>
<td>988</td>
<td>5036</td>
</tr>
<tr>
<td>699</td>
<td>2432</td>
<td>864</td>
<td>2726</td>
<td>7853</td>
<td>3494</td>
<td>1014</td>
<td>807</td>
</tr>
<tr>
<td>6971</td>
<td>2010</td>
<td>804</td>
<td>5889</td>
<td>7901</td>
<td>2472</td>
<td>921</td>
<td>1056</td>
</tr>
<tr>
<td>6972</td>
<td>1746</td>
<td>873</td>
<td>240</td>
<td>7901</td>
<td>4266</td>
<td>921</td>
<td>4182</td>
</tr>
<tr>
<td>7001</td>
<td>4042</td>
<td>862</td>
<td>2394</td>
<td>7907</td>
<td>584</td>
<td>963</td>
<td>7541</td>
</tr>
</tbody>
</table>
Starting with $a = 1$, for example, we next computed $v(m) = v((p - 1)/2)\_i$, then $v(m/2)\_i$ or $v((p - m)/2) = v((p + 1)/4)$ (depending upon whether $m$ was even or odd), and so forth, until a full cycle was completed. We then searched for the first $a$, $1 \leq a \leq m$, for which $v(a)$ had not yet been computed, found the value of $v(a)$, by using Eq. (2) again, and then began another cycle using the identities above. This procedure was continued until $v(a)$ had been computed for all $a = 1, 2, \cdots, m$. It can be shown that the cycles arising in this way all have the same length and that, in the particular case that $m$ is also a prime number, there is but one cycle, indicating the efficiency of the algorithm thus devised.

If we assume that, for fixed $a$, it is equally likely that $v(a)$, assumes any one of the values $0, 1, 2, \cdots, p - 1$, then the probability that the term $a^i$ appears in the sum of Theorem 5 (i.e., the probability that $a + v(a) \geq p$) is just $a/p$. Thus, the expected number of terms in the sum is $\sum_{a=1}^{m} a/p = p/8 - (8p)^{-1}$, or approximately $p/8$ for large primes $p$. It is interesting to compare the value $p/8$ with the entries in the third column of the accompanying Table.

8. The Table. In the first two columns of the accompanying Table, we have listed all pairs $(p, i + 1)$, where $p$ is a prime, $p < 8000$, and where the Bernoulli number $B_{i+1} \equiv 0 \pmod{p}$. The four additions to the tables of [8] are marked with an asterisk. The third column contains, for each of these pairs, the number of integers $a$, $1 \leq a \leq m$, satisfying the condition $a + v(a) \geq p$. This is the same as the number of terms in the sum $\sum_{a=1}^{m} a_{a+1}(a) \equiv a^i$ of Theorem 5. The value of this sum modulo $p$ is given in the final column of the Table. Since a zero never appears in this final column, we can conclude by Theorem 5 that Theorem 6 must be true.

Department of Mathematics
Bowdoin College
Brunswick, Maine 04011