MATHEMATICS OF COMPUTATION, VOLUME 27, NUMBER 122, APRIL, 1973

On the Vanishing of the Iwasawa Invariant μ_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 $(n \geqq 0)$ be the cyclotomic field of p^{n+1}th roots of unity over the rational field $\mathbf{Q}$. 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 $\mu_p \geqq 0$, $\lambda_p \geqq 0$ and ν_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 μ_p, λ_p, and ν_p for all primes $p \leqq 4001$. In particular, they showed that $\mu_p = 0$ for every $p \leqq 4001$.

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

Any x in $\mathbf{Z}_p$ has the p-adic representation

$$x = \sum_{k=0}^{\infty} x_k p^k,$$

where the x_k are rational integers satisfying $0 \leqq x_k < p$ for $k \geqq 0$. 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

$$s_n(x) = \sum_{k=0}^{n} x_k p^k.$$

Received June 15, 1972.

AMS (MOS) subject classifications (1970). Primary 12A35, 12A50; Secondary 10A40.

Key words and phrases. Cyclotomic fields, class numbers, irregular primes, Γ-extensions, cyclotomic invariants, Fermat's Last Theorem.

Thus, $x \equiv s_n(x) \pmod{p^{n+1}}$ and $0 \leqq s_n(x) < p^{n+1}$ for all $n \geqq 0$.

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

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 μ_p:

THEOREM 1. *$\mu_p > 0$ if and only if there exists an odd index i, $1 \leqq i \leqq p-4$, such that*

$$\sum_{v \in V} s_n(uv)v^i \equiv 0 \pmod{p^{n+2}} \tag{1}$$

for all units $u \in U$ and for all $n \geqq 0$.

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

THEOREM 2. *$\mu_p > 0$ if and only if there exists an odd index i, $1 \leqq i \leqq p-4$, such that*

$$\sum_{v \in V} (uv)_n v^i \equiv 0 \pmod{p}$$

for all $u \in U$ and for all $n \geqq 1$.

By choosing $u = 1$ in Theorems 1 and 2, we obtain

THEOREM 3. *If $\mu_p > 0$, then there exists an odd index i, $1 \leqq i \leqq p-4$, such that*

$$\sum_{v \in V} v_0 v^i \equiv 0 \pmod{p^2}, \quad \textit{and} \tag{1}$$

$$\sum_{v \in V} v_n v_0^i \equiv 0 \pmod{p} \quad \textit{for all } n \geqq 1. \tag{2}$$

It is known from the general theory of Γ-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, $1 \leqq i \leqq p-4$, such that $B_{i+1} \equiv 0 \pmod{p}$. Hence p is an irregular prime.*

Proof. Part (1) of Theorem 3 implies that

$$\sum_{v \in V} v_0(v_0 + v_1 p)^i \equiv \sum_{v \in V} v_0^{i+1} + pi \sum_{v \in V} v_1 v_0^i \equiv 0 \pmod{p^2}.$$

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

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

as desired.

4. Additional Conditions for Positive μ_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 μ_p be positive.

THEOREM 4. *If $\mu_p > 0$, then there exists an odd index i, $1 \leqq i \leqq p-4$, such that*

(1) $$B_{i+1} \equiv 0 \pmod{p},$$

(2) $$\sum_{a=1;\, a+v(a)_n<p}^{p-1} a^i \equiv \sum_{a=1;\, a+v(a)_n\geqq p}^{p-1} a^i \equiv 0 \pmod{p} \quad \textit{for all } n \geqq 1.$$

Proof. We have already seen that (1) is true. If $n \geqq 1$ 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

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

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

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

$$\sum_{v\in V} (v_1 + v_{n+1})v_0^i + \sum_{v\in V;\, v_0+v_n\geqq p} v_0^i \equiv 0 \pmod{p}.$$

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

$$\sum_{v\in V;\, v_0+v_n<p} v_0^i \equiv \sum_{v\in V;\, v_0+v_n\geqq p} v_0^i \equiv 0 \pmod{p},$$

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 μ_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

$$1 = v(a)^{p-1} \equiv (a + v(a)_1 p)^{p-1} \pmod{p^2},$$

we see that $v(a)_1$ is completely determined by the conditions

(2) $$v(a)_1 \equiv (a^p - a)/p \pmod{p} \quad \text{and} \quad 0 \leqq v(a)_1 < p.$$

It is easy to see by (2) that

(3) $$v(a)_1 + v(p - a)_1 = p - 1, \qquad 1 \leqq a \leqq p - 1.$$

It follows immediately that $a + v(a)_1 < p$ if and only if $(p - a) + v(p - a)_1 \geqq p$, so that, letting $b = p - a$ and recalling that i is odd, we obtain

$$\sum_{a=1;\, a+v(a)_1<p}^{m} a^i \equiv -\sum_{b=m+1;\, b+v(b)_1\geqq p}^{p-1} b^i \pmod{p}.$$

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, $1 \leqq i \leqq p-4$, such that*

$$B_{i+1} \equiv 0 \pmod{p}, \quad \textit{and} \tag{1}$$

$$\sum_{a=1;\, a+v(a)_i \geqq p}^{m} a^i \equiv 0 \pmod{p}. \tag{2}$$

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 $p \leqq 4001$. 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 μ_p, λ_p, and ν_p for primes $p \leqq 4001$.

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

$$\sum_{j=0}^{k} \binom{k+1}{j} B_j = 0, \tag{4}$$

with $B_0 = 1$. Computing the binomial coefficients (mod p), we can use the above to compute B_k (mod p) recursively. This requires, of course, that we store the B_j's as we go along. Since $B_j = 0$ for j odd, $j \geqq 3$, 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]:

$$(-1)^m \sum_{r=0}^{m} \binom{m}{r} B_{n+r} = (-1)^n \sum_{s=0}^{n} \binom{n}{s} B_{m+s}, \qquad m, n \geqq 0. \tag{5}$$

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 $m, n \geqq 0$. 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

$$\sum_{r=0}^{n} C(n, r)B_{n+r} = 0, \qquad n \geqq 1, \tag{6}$$

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

$$C(n, r) = \binom{n+1}{r} + \binom{n}{r-1} \quad \text{for } 1 \leqq r \leqq n+1.$$

Equation (6) defines B_{2n} recursively in terms of $B_n, B_{n+1}, \cdots, B_{2n-2}$, 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 $B_{i+1} \equiv 0 \pmod p$ 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

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

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, $B_{i+1} \equiv 0 \pmod p$.

Selfridge and Pollack [10] have found all pairs $(p, i+1)$ with $B_{i+1} \equiv 0 \pmod p$ 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 μ_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 $v(a)_1$ for $a = 1, 2, \cdots, m$. 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 $v(a)_1$'s can be found from others by means of a linear congruence modulo p.

Clearly, $v(1)_1 = 0$, so that the index $a = 1$ is never included in the sum. We first computed $v(2)_1$, using Eq. (2). The following identities can be derived from (2) and (3):

$$v(a)_1 - 2v(a/2)_1 - (a/2)v(2)_1 \equiv 0 \pmod p \qquad (a \text{ even}),$$

$$v(a)_1 + 2v((p-a)/2)_1 + ((p-a)/2)v(2)_1 + 1 \equiv 0 \pmod p \qquad (a \text{ odd}).$$

Hence, given $v(a)_1$ for some a, $1 \leqq a \leqq m$, these identities may be used to compute either $v(a/2)_1$ if a is even or $v((p-a)/2)_1$ if a is odd, without resorting to Eq. (2).

p	i+1	terms	sum
37	32	3	7
59	44	6	25
67	58	7	43
101	68	11	91
103	24	9	88
131	22	16	49
149	130	17	79
157	62	21	108
157	110	21	69
233	84	24	140
257	164	36	81
263	100	32	99
271	84	30	179
283	20	39	174
293	156	34	217
307	88	40	220
311	292	34	200
347	280	49	198
353	186	43	49
353	300	43	232
379	100	47	362
379	174	47	164
389	200	50	159
401	382	45	209
409	126	46	282
421	240	57	287
433	366	55	18
461	196	53	270
463	130	59	456
467	94	67	169
467	194	67	400
491	292	68	397
491	336	68	139
491	338	68	25
523	400	63	142
541	86	65	327
547	270	67	174
547	486	67	172
557	222	61	238
577	52	68	558
587	90	78	373
587	92	78	476
593	22	84	102
607	592	75	515
613	522	72	428

p	i+1	terms	sum
617	20	66	303
617	174	66	335
617	338	66	191
619	428	83	334
631	80	81	551
631	226	81	361
647	236	84	221
647	242	84	320
647	554	84	219
653	48	76	613
659	224	88	277
673	408	91	8
673	502	91	571
677	628	85	624
683	32	87	2
691	12	67	555
691	200	87	598
727	378	88	628
751	290	87	16
757	514	90	719
761	260	80	62
773	732	106	184
797	220	95	38
809	330	88	673
809	628	88	265
811	544	102	39
821	744	100	83
827	102	97	691
839	66	96	150
877	868	114	455
881	162	117	610
887	418	119	174
929	520	117	679
929	820	117	907
953	156	119	510
971	166	114	759
1061	474	123	488
1091	888	150	1042
1117	794	131	167
1129	348	143	68
1151	534	140	751
1151	784	140	74
1151	968	140	986
1153	802	156	1112
1193	262	149	344

p	i+1	terms	sum
1201	676	159	1048
1217	784	174	57
1217	866	174	19
1217	1118	174	118
1229	784	139	739
1237	874	148	1227
1279	518	146	861
1283	510	168	1233
1291	206	173	702
1291	824	173	1234
1297	202	151	1271
1297	220	151	250
1301	176	163	165
1307	382	184	48
1307	852	184	896
1319	304	165	1289
1327	466	163	332
1367	234	161	755
*1381	266	162	836
1409	358	171	1193
1429	996	178	94
1439	574	161	1230
1483	224	200	252
1499	94	191	1082
1523	1310	202	427
1559	862	186	1409
*1597	842	184	1579
1609	1356	191	1594
1613	172	207	221
1619	560	188	1199
1621	980	199	247
1637	718	205	434
1663	270	209	1599
*1663	1508	209	1155
1669	388	200	1231
1669	1086	200	728
1721	30	220	164
1733	810	218	1634
1733	942	218	1073
1753	712	233	1088
1759	1520	218	1626
1777	1192	240	1553
1787	1606	217	1591
1789	848	223	733
1789	1442	223	1468

p	*i+1*	*terms*	*sum*
1811	550	228	900
1811	698	228	1044
1811	1520	228	962
1831	1274	232	575
1847	954	224	866
1847	1016	224	1511
1847	1558	224	1528
1871	1794	233	370
*1877	1026	237	1539
1879	1260	241	1739
1889	242	251	1849
1901	1722	228	1365
1933	1058	237	1489
1933	1320	237	162
1951	1656	252	302
1979	148	257	1462
1987	510	248	286
1993	912	233	1117
1997	772	246	1959
1997	1888	246	1026
2003	60	255	1850
2003	600	255	1079
2017	1204	266	1429
2039	1300	256	764
2053	1932	252	1067
2087	376	263	1109
2087	1298	263	1324
2099	1230	277	492
2111	1038	243	657
2137	1624	270	1775
2143	1916	277	2036
2153	1832	266	1585
2213	154	295	461
2239	1826	258	1611
2267	2234	289	1182
2273	876	275	1210
2273	2166	275	1530
2293	2040	257	669
2309	1660	288	2018
2309	1772	288	1616
2357	2204	289	863
2371	242	298	1139
2371	2274	298	134
2377	1226	285	1496
2381	2060	271	1106

p	*i+1*	*terms*	*sum*
2383	842	327	1786
2383	2278	327	662
2389	776	299	2077
2411	2126	319	1033
2423	290	315	1243
2423	884	315	507
2441	366	307	2353
2441	1750	307	1923
2503	1044	311	90
2543	2374	318	1915
2557	1464	313	518
2579	1730	324	624
2591	854	314	1722
2591	2574	314	710
2621	1772	322	1473
2633	1416	316	2054
2647	1172	340	2060
2657	710	340	408
2663	1244	343	1260
2671	404	336	400
2671	2394	336	1344
2689	926	346	2263
2753	482	328	2611
2767	2528	328	13
2777	1600	362	2014
2789	1984	356	164
2789	2154	356	312
2791	2554	308	1507
2833	1832	326	1693
2857	98	331	1828
2861	352	349	1251
2909	400	396	930
2909	950	396	1239
2927	242	383	2702
2939	332	366	334
2939	1102	366	280
2939	2748	366	465
2957	138	361	31
2957	788	361	1776
2999	776	372	371
3011	1496	395	2526
3023	2020	347	2295
3049	700	397	2693
3061	2522	399	393
3083	1450	370	1734

p	*i+1*	*terms*	*sum*
3089	1706	402	2832
3119	1704	374	1185
3181	3142	382	2247
3203	2368	411	1303
3221	98	413	1129
3229	1634	392	3059
3257	922	436	629
3313	2222	399	1954
3323	3292	412	1176
3329	1378	428	2749
3391	2232	429	2415
3391	2534	429	673
3407	2076	444	2201
3407	2558	444	2335
3433	1300	436	2120
3469	1174	432	2415
3491	2544	411	2053
3511	1416	438	2441
3511	1724	438	1866
3517	1836	419	1157
3517	2586	419	943
3529	3490	451	2453
3533	2314	422	1462
3533	3136	422	478
3539	2082	422	1902
3539	2130	422	2676
3559	344	438	116
3559	1592	439	3289
3581	1466	417	275
3583	1922	454	611
3593	360	464	565
3593	642	464	3097
3607	1976	446	546
3613	2082	449	1491
3617	16	446	2869
3617	2856	446	1264
3631	1104	464	1447
3637	2526	473	1863
3637	3202	473	28
3671	1580	468	2742
3677	2238	436	2728
3697	1884	464	1137
3779	2362	456	2243
3797	1256	487	2179
3821	3296	477	2655

p	*i+1*	*terms*	*sum*
3833	1840	476	990
3833	1998	476	1089
3833	3206	476	2314
3851	216	471	736
3851	404	471	3380
3853	748	435	1422
3881	1686	462	3356
3881	2138	462	798
3917	1490	467	3067
3957	106	485	905
3989	1936	462	2037
4001	534	518	3299
4003	82	493	895
4003	142	493	1459
4003	2610	493	230
4021	3228	528	3783
4027	2332	497	329
4049	1854	486	1700
4051	3548	535	136
4073	3620	509	1621
4129	1784	535	581
4157	658	538	1029
4157	2322	538	3855
4219	4190	556	2220
4243	2712	543	381
4243	4146	543	2191
4259	3580	558	3855
4259	3726	558	1208
4261	2068	482	3725
4339	214	547	1243
4349	2052	511	428
4409	636	581	3991
4409	672	581	3237
4421	3768	560	2945
4451	2896	551	3965
4451	2978	551	3346
4457	444	552	209
4493	746	534	541
4519	848	553	2926
4523	456	551	3776
4561	436	587	1428
4591	2292	592	2652
4591	3596	592	776
4637	3618	567	1566
4639	3226	567	958

p	*i+1*	*terms*	*sum*
4657	1578	579	2183
4657	2416	579	3208
4657	4110	579	995
4663	216	603	3611
4663	4278	603	3314
4679	3592	576	4079
4691	3450	571	3948
4751	3768	601	4352
4783	252	604	3786
4793	2636	626	3762
4813	2620	565	1692
4861	4678	608	2789
4889	2924	640	4440
4903	3106	601	3481
4909	1462	630	2816
4943	492	624	315
4951	1914	609	586
4951	2468	609	4156
4951	3830	609	2946
4957	3812	619	4069
4969	1940	624	4109
4973	4208	645	3067
5009	1544	621	22
5009	4956	621	322
5039	594	651	4135
5077	3092	599	2770
5081	3016	630	3762
5099	1378	669	2497
5101	190	627	3455
5107	4872	639	1776
5119	4086	632	4701
5167	4112	626	2294
5179	4732	678	2277
5189	1102	677	2943
5209	644	640	3451
5209	2928	640	528
5227	308	633	5017
5231	3466	642	1224
5297	4810	670	4260
5303	4156	660	3140
5309	158	652	1623
5351	1948	687	872
5399	1482	674	3705
5413	1702	685	5133
5441	4726	683	2051

p	*i+1*	*terms*	*sum*
5443	1710	652	3387
5477	1150	631	630
5479	1826	650	5457
5479	4802	650	5245
5501	666	719	1935
5527	5206	706	4901
5531	3438	701	5344
5557	3196	714	2146
5569	938	710	2766
5573	2032	689	4879
5639	2672	744	5177
5641	4580	731	3806
5641	5258	731	3155
5669	2218	701	3879
5669	2680	701	1311
5689	348	711	1190
5701	2450	680	712
5783	2200	757	1074
5791	1258	737	4450
5813	4284	759	5487
5821	1150	717	2690
5839	2308	709	4879
5861	3554	744	580
5897	2996	729	2862
5903	3970	729	2071
5903	5000	729	5530
5923	4240	748	1466
5927	3642	739	4274
5939	342	735	5157
5939	5014	735	5527
5953	3274	763	4360
6007	912	714	118
6011	5870	722	624
6037	3396	752	4626
6043	1226	770	5010
6091	702	761	5812
6101	2008	741	2794
6173	5008	770	131
6173	5894	770	5093
6217	4186	777	3294
6247	1492	799	1767
6247	3474	799	4635
6257	4272	775	3473
6263	3286	793	6130
6263	4226	793	6010

p	$i+1$	terms	sum
6287	4452	803	1358
6287	5034	803	202
6317	2354	793	1683
6329	5102	816	2169
6337	1956	772	633
6343	750	773	555
6343	5820	773	3693
6367	1190	780	2528
6373	2838	803	4876
6373	4226	803	3447
6379	218	779	342
6421	438	793	1151
6449	4884	775	3003
6449	5830	775	3431
6451	3236	817	4290
6491	346	807	2178
6521	236	816	3448
6529	1564	810	3664
6547	734	871	6183
6569	1692	813	2814
6569	1776	813	3851
6571	1744	774	3308
6577	1312	848	5700
6619	1952	829	6068
6619	3170	829	1719
6659	2950	800	1532
6659	4014	800	2968
6689	5252	858	3333
6701	5484	833	2400
6733	1690	878	4696
6763	4144	835	6633
6763	6218	835	4046
6763	6230	835	2419
6779	3994	831	2091
6793	2686	852	2303
6823	4952	865	6253
6827	4108	854	6063
6833	2254	873	1146
6833	5144	873	369
6857	6676	820	2447
6863	6406	858	6442
6949	2432	864	2726
6971	2010	894	5888
6997	1746	873	240
7001	4642	862	2394

p	$i+1$	terms	sum
7039	1454	884	4693
7057	4154	903	669
7057	4972	903	3496
7069	1478	850	3103
7069	2570	850	3586
7109	290	887	3838
7121	1502	885	2851
7127	6798	849	4876
7177	962	884	1391
7187	3906	945	6847
7207	1670	972	1891
7207	5774	972	1800
7211	898	906	5989
7213	1436	893	2097
7213	6930	893	2163
7229	6236	926	738
7309	324	890	1510
7321	348	892	2405
7351	1466	928	2113
7411	4712	898	4054
7459	5286	947	6940
7487	2500	924	2778
7489	4250	951	1314
7499	3642	930	827
7507	6924	921	5601
7537	2264	945	7112
7547	5644	914	3305
7559	116	906	3207
7591	2620	965	460
7607	3594	934	1945
7643	5026	960	6969
7681	368	926	5662
7687	1246	969	60
7687	3216	969	192
7687	6516	969	6570
7691	2218	935	4092
7727	950	929	4841
7727	3756	929	1487
7817	7346	941	6876
7823	3298	987	2519
7829	1392	988	5036
7853	3494	1014	807
7901	2472	921	1056
7901	4286	921	4182
7907	584	963	7541

p	$i+1$	terms	sum
7919	3888	971	1498
7927	6448	980	621
7937	3980	935	6801
7949	2506	1009	1807
7949	3436	1009	926
7951	4328	961	2743
7963	4748	1033	74

Starting with $a = 1$, for example, we next computed $v(m)_1 = v((p-1)/2)_1$, then $v(m/2)_1$ or $v((p-m)/2)_1 = v((p+1)/4)_1$ (depending upon whether m was even or odd), and so forth, until a full cycle was completed. We then searched for the first a, $1 \leqq a \leqq m$, for which $v(a)_1$ had not yet been computed, found the value of $v(a)_1$ by using Eq. (2) again, and then began another cycle using the identities above. This procedure was continued until $v(a)_1$ 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 $v(a)_1$ 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 $a + v(a)_1 \geqq p$) 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, $1 \leqq a \leqq m$, satisfying the condition $a + v(a)_1 \geqq p$. This is the same as the number of terms in the sum $\sum_{a=1;a+v(a)_1 \geqq p}^{m} a^i$ 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

1. Z. I. Borevič & I. R. Šafarevič, *Number Theory*, "Nauka," Moscow, 1964; English transl., Pure and Appl. Math., vol. 20, Academic Press, New York, 1966. MR **30** #1080; MR **33** #4001.

2. L. Carlitz, "Problem 795," *Math. Mag.*, v. 44, 1971, p. 106.

3. K. Iwasawa, "On some invariants of cyclotomic fields," *Amer. J. Math.*, v. 80, 1958, pp. 773–783; erratum, ibid., v. 81, 1959, p. 280. MR **23** #A1631.

4. K. Iwasawa, "On Γ-extensions of algebraic number fields," *Bull. Amer. Math. Soc.*, v. 65, 1959, pp. 183–226. MR **23** #A1630.

5. K. Iwasawa, "A class number formula for cyclotomic fields," *Ann. of Math.*, (2), v. 76, 1962, pp. 171–179. MR **27** #4806.

6. K. Iwasawa, "On some modules in the theory of cyclotomic fields," *J. Math. Soc. Japan*, v. 16, 1964, pp. 42–82. MR **35** #6646.

7. K. Iwasawa & C. Sims, "Computation of invariants in the theory of cyclotomic fields," *J. Math. Soc. Japan*, v. 18, 1966, pp. 86–96. MR **34** #2560.

8a. D. H. Lehmer, E. Lehmer & H. S. Vandiver, "An application of high-speed computing to Fermat's last theorem," *Proc. Nat. Acad. Sci. U.S.A.*, v. 40, 1954, pp. 25–33. MR **15**, 778.

8b. H. S. Vandiver, "Examination of methods of attack on the second case of Fermat's last theorem," *Proc. Nat. Acad. Sci. U.S.A.*, v. 40, 1954, pp. 732–735. MR **16**, 13.

8c. J. L. Selfridge, C. A. Nicol & H. S. Vandiver, "Proof of Fermat's last theorem for all prime exponents less than 4002," *Proc. Nat. Acad. Sci. U.S.A.*, v. 41, 1955, pp. 970–973. MR **17**, 348.

9. D. Mirimanoff, "Sur la congruence $(r^{p-1} - 1)$: $p \equiv q_r \pmod{p}$," *J. Reine Angew. Math.*, v. 115, 1895, pp. 295–300.

10. J. L. Selfridge & B. W. Pollack, "Fermat's last theorem is true for any exponent up to 25,000," *Notices Amer. Math. Soc.*, v. 11, 1964, p. 97. Abstract #608-138.

11. J.-P. Serre, *Classes des corps cyclotomiques (d'après K. Iwasawa)*, Séminaire Bourbaki 1958/59, Exposé 174, fasc. 1, Secrétariat mathématique, Paris, 1959. MR **28** #1091.