MATHEMATICS OF COMPUTATION, VOLUME 28, NUMBER 126, APRIL 1974, PAGES 653–657

Irregular Prime Divisors of the Bernoulli Numbers

By Wells Johnson

Abstract. If p is an irregular prime, $p < 8000$, then the indices $2n$ for which the Bernoulli quotients $B_{2n}/2n$ are divisible by p^2 are completely characterized. In particular, it is always true that $2n > p$ and that $B_{2n}/2n \not\equiv (B_{2n+p-1}/2n + p - 1) \pmod{p^2}$ if $(p, 2n)$ is an irregular pair. As a result, we obtain another verification that the cyclotomic invariants μ_p of Iwasawa all vanish for primes $p < 8000$.

1. Introduction and Summary. Let B_n denote the sequence of Bernoulli numbers in the "even-index" notation of [1]. If $B_{2n} = P_{2n}/Q_{2n}$ with $(P_{2n}, Q_{2n}) = 1$, then the prime factorization of the denominator Q_{2n} is given precisely by the von Staudt-Clausen theorem. The prime divisors of P_{2n}, however, are more difficult to obtain. Their importance stems from the fact that, more than a century ago, Kummer proved that the Fermat equation $x^p + y^p = z^p$ has no integral solutions if p is a regular prime, that is, one for which p does not divide $P_2P_4P_6 \cdots P_{p-3}$.

A rather old result, now commonly known as J. C. Adams' theorem (cf. [10, p. 261]), states that if p is a prime not dividing Q_{2n} and p^e divides n for some $e \geqq 1$, then p^e also divides P_{2n}. Thus, given any prime power p^e for $p > 3$, $e \geqq 1$, there exist infinitely many Bernoulli numerators P_{2n} which are divisible by p^e. If we add the restriction that $(p, n) = 1$, however, then the problem of determining when p^e divides P_{2n} becomes more difficult. It turns out to be convenient to study the quotients $B_{2n}/2n = P_{2n}/2nQ_{2n}$, which, when reduced, are p-integers if $p - 1 \nmid 2n$ by the theorems of von Staudt-Clausen and J. C. Adams.

The general problem, then, is to determine, for a given prime-power p^e, those indices, $2n$, $p - 1 \nmid 2n$, for which p^e divides the p-integer $B_{2n}/2n$. It follows immediately from a congruence of Kummer that p must be irregular, and that p divides $B_{2n}/2n$ if and only if p divides $P_{2n'}$, where $2n'$ is the least positive residue of $2n \pmod{p - 1}$. This settles the case $e = 1$. Moreover, we see that any irregular prime p divides infinitely many Bernoulli numerators P_{2n} with $(p, n) = 1$.

This paper reports on some computations done recently on the PDP-10 computer at Bowdoin College to investigate the case $e = 2$. About fifty years ago, Pollaczek [9] noted that 37^2 divides $B_{284}/284$, showing that the case $e = 2$ is possible. Montgomery [8] raised the question whether or not p^2 divides P_{2n} for $0 < 2n < p - 1$. Our computations show that the answer to this is negative for all irregular primes $p < 8000$. Further, for the irregular primes $p < 8000$, we can characterize precisely those indices $2n$ for which p^2 divides $B_{2n}/2n$. Our results show that the *square* of any irregular prime $p < 8000$ divides infinitely many Bernoulli numerators P_{2n} with $(p, n) = 1$. Finally, we compare some of our computations to those done earlier

Received April 9, 1973.
AMS (MOS) subject classifications (1970). Primary 10A40; Secondary 12A35.
Key words and phrases. Bernoulli numbers, irregular primes, cyclotomic invariants.

by Pollaczek [9] and discuss the important relationship of these results to the determination of the cyclotomic invariants μ_p of Iwasawa.

If p is an irregular prime and p divides P_{2n} for $0 < 2n < p - 1$, then we shall refer to $(p, 2n)$ as an *irregular pair*. For a given irregular prime p, the number of such irregular pairs is called the *index of irregularity of p*.

2. The Congruences of Kummer. We state the fundamental congruences of Kummer (cf. [10, p. 266]), valid for $2 \leqq r + 1 \leqq 2n$ and primes p for which $p - 1 \nmid 2n$:

$$\sum_{s=0}^{r} (-1)^s \binom{r}{s} \frac{B_{2n+s(p-1)}}{2n + s(p-1)} \equiv 0 \pmod{p^r}.$$

For $r = 1, 2$ we obtain for $p - 1 \nmid 2n$:

$$\frac{B_{2n}}{2n} \equiv \frac{B_{2n+(p-1)}}{2n + (p-1)} \pmod{p}, \qquad n \geqq 1, \tag{1}$$

$$\frac{B_{2n}}{2n} - 2\frac{B_{2n+(p-1)}}{2n + (p-1)} + \frac{B_{2n+2(p-1)}}{2n + 2(p-1)} \equiv 0 \pmod{p^2}, \qquad n \geqq 2. \tag{2}$$

An analysis of (1) gives the results stated in the previous section for the case $e = 1$ of the general problem. We remark that the argument used here is essential for all known proofs of the existence of infinitely many irregular primes in certain arithmetic progressions (cf. [11], [2], [8], and [7]).

For the case $e = 2$, we use Eq. (2). If p^2 divides $B_{2n}/2n$, then as above, $(p, 2n')$ must be an irregular pair, where $2n'$ is the least positive residue of $2n \pmod{p-1}$. Also, given an irregular pair, $(p, 2n')$, we define $A_t = B_{2n'+t(p-1)}/2n' + t(p-1)$ for $t \geqq 0$. By (1), $A_t \equiv 0 \pmod{p}$, so that we may define a_t by the conditions $A_t \equiv a_t p \pmod{p^2}$, $0 \leqq a_t < p$. Hence p^2 divides A_t if and only if $a_t = 0$. Since $B_2 = \frac{1}{6}$, it follows that $n' > 1$. Equation (2) then implies that

$$a_{t+2} - a_{t+1} \equiv a_{t+1} - a_t \pmod{p}, \qquad t \geqq 0,$$

which gives

$$a_t - a_0 \equiv t(a_1 - a_0) \pmod{p}, \qquad t \geqq 1.$$

Thus p^2 divides $B_{2n}/2n$ if and only if $2n = 2n' + t(p-1)$, where $(p, 2n')$ is an irregular pair, and where $t \geqq 0$ and t satisfies the congruence

$$-a_0 \equiv t(a_1 - a_0) \pmod{p}. \tag{3}$$

Given an irregular pair $(p, 2n')$, if it happens that $a_1 = a_0$, then $a_t = a_0$ for all $t \geqq 1$. If $a_0 \neq 0$, then p^2 divides no $B_{2n}/2n$ with $2n \equiv 2n' \pmod{p-1}$, but if $a_0 = 0$, then p^2 divides every $B_{2n}/2n$ with $2n \equiv 2n' \pmod{p-1}$. If $a_1 \neq a_0$, however, then we can solve (3) for t uniquely $\pmod{p}$. In this case, then, every interval of length $p^2 - p$ contains exactly one index $2n$, $2n \equiv 2n' \pmod{p-1}$, for which p^2 divides $B_{2n}/2n$. The index $2n$ is divisible by p only when $t \equiv 2n' \pmod{p}$. Thus p^2 divides infinitely many Bernoulli numerators P_{2n} with $(p, n) = 1$ if and only if, for some irregular pair $(p, 2n')$, either (a) $a_0 = a_1 = 0$ or (b) $a_0 \neq a_1$ and the unique solution $t \pmod{p}$ to (3) is not $2n'$.

3. Computational Results. The values of a_0 and a_1 were computed for each of the 502 irregular pairs $(p, 2n)$, $p < 8000$, previously reported by the author [5]. For all 502 pairs, it was found that $a_0 \not\equiv 0$, and that $a_1 \not\equiv a_0$ so that it was possible to solve (3) for $t \pmod p$. For no pair $(p, 2n)$ did we ever obtain $t = 2n$. We thus have the following:

THEOREM. *If p is an irregular prime, $p < 8000$, then*
(A) *p^2 does not divide any of the Bernoulli numerators $P_2, P_4, P_6, \cdots, P_{p-3}$.*
(B) *$B_{2n}/2n \not\equiv (B_{2n+(p-1)}/2n + (p-1)) \pmod{p^2}$ for all irregular pairs $(p, 2n)$.*
(C) *Every interval of length $p^2 - p$ contains exactly i_p indices $2n$ with $B_{2n}/2n \equiv 0 \pmod{p^2}$, where i_p is the index of irregularity of p. Moreover, for all of these, $(p, n) = 1$, so that there exist infinitely many Bernoulli numerators P_{2n}, $(p, n) = 1$, divisible by p^2.*

For each irregular pair $(p, 2n)$, the values of a_0 and a_1 were computed from the following equations of E. Lehmer [6], valid for $p > 5$, $p - 1 \nmid 2s - 2$:

$$(4) \quad \sum_{r=1}^{[p/6]} (p - 6r)^{2s-1} \equiv (c_{2s}B_{2s}/4s) \pmod{p^2}, \qquad c_{2s} = 6^{2s-1} + 3^{2s-1} + 2^{2s-1} - 1,$$

$$(5) \quad \sum_{r=1}^{[p/4]} (p - 4r)^{2s-1} \equiv (d_{2s}B_{2s}/4s) \pmod{p^2}, \qquad d_{2s} = (2^{2s} - 1)(2^{2s-1} + 1).$$

For each irregular pair $(p, 2n)$, we first tested for the invertibility of $c_{2n} \pmod p$. For $c_{2n} \not\equiv 0 \pmod p$, we next computed the sum $\pmod{p^2}$ in (4) with $2s = 2n$, writing it in the form $e + fp$, $0 \leqq e, f < p$. It was first checked that $e = 0$, again verifying that indeed $(p, 2n)$ is an irregular pair. Then a_0 was computed from the congruence $a_0 \equiv 2c_{2n}^{-1}f \pmod p$. The value of a_1 was found similarly, using (4) with $2s = 2n + p - 1$. For only one irregular pair, (1201, 676), did c_{2n} fail to be invertible. For this pair, $d_{2n} \not\equiv 0 \pmod p$, so that we were able to compute the values of a_0 and a_1 from Eq. (5). After computing $t \pmod p$ from (3), we performed a final check by showing that the sum in (4) or (5) vanishes $\pmod{p^2}$ for $2s = 2n + t(p - 1)$. A partial table of our results is included at the end of this paper.

4. Pollaczek's Results and the Cyclotomic Invariants μ_p of Iwasawa. Pollaczek [9, p. 31] performed these computations some time ago for the three irregular primes $p < 100$. He computed $(-B_{2n}/n)$ rather than $(B_{2n}/2n) \pmod{p^2}$, so that our values of a_0 and a_1 must be multiplied by -2 in order to make valid comparisons. The results agree for $p = 37$ and also for $p = 59$ after a transposition of Pollaczek's indices to correct his obvious inconsistency. For $p = 67$, there seems to be an error in Pollaczek's value of B_{62}', corresponding to our value of a_1. A direct computation of Eq. (4) negates his claim that 67^2 divides P_{190}.

Iwasawa [3, p. 782] has shown that the cyclotomic invariant μ_p, important in the theory of class numbers of cyclotomic fields, vanishes if p is either a regular prime or an irregular prime for which $a_0 \not\equiv a_1$ for all irregular pairs $(p, 2n)$. Iwasawa invoked the computations of Pollaczek to conclude that $\mu_p = 0$ for all primes $p < 100$. More recently, using other tests, Iwasawa and Sims [4] and the author [5] have shown that $\mu_p = 0$ for all primes $p < 8000$. The computations reported here give another verification that this is true.

TABLE

p	$2n$	a_0	a_1	t	$2n + t(p-1)$
37	32	1	22	7	284
59	44	23	49	15	914
67	58	43	64	49	3292
101	68	30	72	57	5768
103	24	98	49	2	228
491	292	265	230	218	107112
491	336	225	328	260	127736
491	338	453	437	59	29248
523	400	413	387	36	19192
541	86	515	185	436	235526
953	156	827	851	720	685596
971	166	817	561	538	522026
1061	474	87	251	1054	1117714
1091	888	24	781	85	93538
1117	794	210	79	607	678206
1997	772	508	163	1136	2268228
1997	1888	591	348	1531	3057764
2003	60	1761	319	511	1023082
2003	600	1816	1656	1113	2228826
2017	1204	1621	1547	1412	2847796
3989	1936	933	1306	3794	15132408
4001	534	2447	2861	3019	12076534
4003	82	1757	3792	784	3137650
4003	142	430	85	3018	12078178
4003	2610	2010	3594	2258	9039126
5939	342	3660	124	3031	17998420
5939	5014	3488	4069	5749	34142576
5953	3274	1007	3675	2068	12312010
6007	912	4702	3459	4445	26697582
6011	5870	5292	399	4232	25440190
7937	3980	3192	5703	4503	35739788
7949	2506	3876	5215	2906	23099394
7949	3436	7398	2031	2263	17989760
7951	4328	5767	6327	799	6356378
7963	4748	5527	5570	3390	26995928

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, "Note on irregular primes," *Proc. Amer. Math. Soc.*, v. 5, 1954, pp. 329–331. MR **15**, 778.

K. IWASAWA, "On some invariants of cyclotomic fields," *Amer. J. Math.*, v. 80, 1958, pp. 773–7 erratum, *ibid.*, v. 81, 1959, p. 280. MR **23** #A1631.

4. 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.

5. W. JOHNSON, "On the vanishing of the Iwasawa invariant μ_p for $p < 8000$," *Math. Comp.*, v. 27, 1973, pp. 387–396.

E. LEHMER, "On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson," *Ann. of Math.*, (2), v. 39, 1938, pp. 350–360.

7. T. METSÄNKYLÄ, "Note on the distribution of irregular primes," *Ann. Acad. Sci. Fenn. Ser. A.I.*, v. 492, 1971, 7 pp. MR **43** #168.

8. H. L. MONTGOMERY, "Distribution of irregular primes," *Illinois J. Math.*, v. 9, 1965, pp. 553–558. MR **31** #5861.

9. F. POLLACZEK, "Über die irregulären Kreiskörper der l-ten und l^2-ten Einheitswurzeln," *Math. Z.*, No. 21, 1924, pp. 1–38.

10. J. USPENSKY & M. HEASLET, *Elementary Number Theory*, McGraw-Hill, New York, 1939. MR **1**, 38.

11. H. S. VANDIVER, "Is there an infinity of regular primes?," *Scripta Math.*, v. 21, 1955, pp. 306–309.