MATHEMATICS OF COMPUTATION, VOLUME 34, NUMBER 150
APRIL 1980, PAGES 647–649

p-Divisibility of Certain Sets of Bernoulli Numbers

By Samuel S. Wagstaff, Jr.

Abstract. Recently, Ullom has proved an upper bound on the number of Bernoulli numbers in certain sets which are divisible by a given prime. We report on a search for such Bernoulli numbers and primes up to 1000000.

Let $p \geqslant 5$ be prime. Let I be the set of even integers between 2 and $p - 3$. For each positive divisor d of $p - 1$ for which $(p - 1)/d$ is odd, let

$$I(d) = \{2k \in I\colon (2k - 1, p - 1) = (p - 1)/d\},$$

where (a, b) is the GCD of a and b. Then $I(d)$ is the set of $2k$ in I such that $2k - 1$ is of the form $a(p - 1)/d$ with $(a, d) = 1$. Hence, $I(p - 1)$ has cardinality $\phi(p - 1) - 1$, where ϕ is Euler's phi function, and otherwise $I(d)$ has cardinality $\phi(d)$. Also I is the disjoint union of the $I(d)$. Ullom has proved the following theorem concerning the divisibility of Bernoulli numbers B_{2k} by p.

THEOREM (ULLOM [3]). *With p and d as above, the number of* $2k \in I(d)$ *for which p divides* B_{2k} *is less than* $\phi(d)/2 + \phi(d)\log\log p/\log p$.

In this paper, we present numerical data concerning the sharpness of Ullom's inequality. It appears to be far weaker than the truth. See [2] for the relevance of this work to the theory of ideal class groups of cyclotomic fields.

If p divides B_{2k} with $2k$ in $I(d)$, then p divides the relative class number of the unique subfield of the pth cyclotomic field of degree d over the rationals. Thus, the search described below for $2k$ in $I(d)$ with p dividing B_{2k} is actually a search for subfields of the pth cyclotomic field whose relative class number is divisible by p.

We first investigated the triples $(p, 2k, d)$ with $2k \in I(d)$, p dividing B_{2k}, and $p < 125000$. This data was readily available from [4]. It is possible to have as many as five $2k$'s in the same division $I(d)$, as is shown by the example $p = 78233$, $d = p - 1$ in Table 1 of [4]. We have $d = p - 1$ for most of the triples with $p < 125000$. We found two examples of three $2k$'s in the same division $I(d)$ with $d < p - 1$, namely $p = 108877$, $2k = 52498$, 79558, and 81346, $d = 36292$; and $p = 109843$, $2k = 25396$, 27844, and 84202, $d = 36614$.

Obviously, the conclusion of Ullom's theorem is sharper when d is small. The extreme example is $p \equiv 3 \pmod 4$ and $d = 2$, when it gives the well-known corollary

Received July 27, 1979; revised August 22, 1979.
AMS (MOS) subject classifications (1970). Primary 10A40.
Key words and phrases. Bernoulli numbers, p-divisibility.

that p does not divide $B_{(p+1)/2}$. The greatest ratio $(p-1)/d$ which we found for at least two $2k$'s in the same $I(d)$ was 9 for $p = 70489$, $2k = 32932$ and 35272, $d = 7832$.

As reported in [3], we determined all such triples with $p < 125000$ and $d \leqslant 30$. They are (67, 58, 22), (631, 226, 14), (683, 32, 22), (757, 514, 28), (1201, 676, 16), and (12697, 10052, 24). Recently, we searched the following region for such triples:

$$\begin{array}{ll} 125000 < p < 140000, & d \leqslant 20, \\ 140000 < p < 160000, & d \leqslant 14, \\ 160000 < p < 500000, & d \leqslant 12, \\ 500000 < p < 600000, & d \leqslant 8, \\ 600000 < p < 1000000, & d \leqslant 6. \end{array}$$

We did not find a single new triple in all this computation. This evidence supports Ullom's conjecture that p does not divide B_{2k} for $2k \in I(4) \cup I(6)$.

We tested whether p divides B_{2k} by the methods of [4] with the following simplification. Given p and $2k$, let $c(x, y, z) = x^{p-2k} + y^{p-2k} - z^{p-2k} - 1$. If the coefficients of $B_{2k}/4k$ in the congruences

$$c(2, 5, 6)B_{2k}/4k \equiv (2^{2k-1} + 1) \sum_{p/6<s<p/5} s^{2k-1} - \sum_{3p/10<s<p/3} s^{2k-1} \pmod p,$$

$$c(3, 4, 6)B_{2k}/4k \equiv \sum_{p/6<s<p/4} s^{2k-1} \pmod p,$$

$$c(2, 3, 4)B_{2k}/4k \equiv \sum_{p/4<s<p/3} s^{2k-1} \pmod p,$$

all vanished modulo p, then we did not bother to try the congruence

$$c(4, 5, 8)B_{2k}/4k \equiv \sum_{p/8<s<p/5} s^{2k-1} + \sum_{3p/8<s<2p/5} s^{2k-1} \pmod p$$

because its coefficient must vanish, too. For suppose (with $t = p - 2k$)

(1) $$2^t + 5^t - 6^t - 1 \equiv 0 \pmod p,$$

(2) $$3^t + 4^t - 6^t - 1 \equiv 0 \pmod p,$$

and

(3) $$2^t + 3^t - 4^t - 1 \equiv 0 \pmod p.$$

Adding (2) and (3) gives $(2^t - 2)(3^t - 1) \equiv 0 \pmod p$. We consider the two possible cases $2^t \equiv 2 \pmod p$ and $3^t \equiv 1 \pmod p$, separately. If the first of these congruences holds, then (3) and (1) give $a^t \equiv a \pmod p$ for $a = 2, 3, 4, 5, 6$, and 8, so that

(4) $$4^t + 5^t - 8^t - 1 \equiv 0 \pmod p.$$

On the other hand, if $3^t \equiv 1 \pmod{p}$, then (2) and (1) give $a^t \equiv 1 \pmod{p}$ for $a =$ 2, 3, 4, 5, 6, and 8, so that (4) again holds. In the second case, the congruence

$$(5) \quad (2^{2k-1} + 3^{2k-1} + 6^{2k-1} - 1)B_{2k}/4k \equiv \sum_{0<s<p/6} (p - 6s)^{2k-1} \pmod{p^2}$$

of E. Lehmer [1] was used modulo p. This decides whether p divides B_{2k} because the coefficient of B_{2k} is $2^{-t} + 3^{-t} + 6^{-t} - 1 \equiv 2 \pmod{p}$. However, in the first case this coefficient is

$$2^{-t} + 3^{-t} + 6^{-t} - 1 \equiv \frac{1}{2} + \frac{1}{3} + \frac{1}{6} - 1 \equiv 0 \pmod{p}$$

and (5) modulo p does not work. In this case (5) modulo p^2 did work for every p and $2k$ we tried.

The author thanks S. Ullom for the use of [3] in preprint form. The computations were done on the IBM 360/75 computer at the University of Illinois.

Department of Mathematics
University of Illinois
Urbana, Illinois 61801

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

2. K. RIBET, "A modular construction of unramified p-extensions of $Q(\mu_p)$," *Invent. Math.*, v. 34, 1976, pp. 151–162.

3. S. V. ULLOM, "Upper bounds for p-divisibility of sets of Bernoulli numbers," *J. Number Theory*. (To appear.)

4. S. S. WAGSTAFF, JR., "The irregular primes to 125000," *Math. Comp.*, v. 32, 1978, pp. 583–591. MR 58 #10711.