MATHEMATICS OF COMPUTATION
VOLUME 48, NUMBER 177
JANUARY 1987, PAGES 341–350

New Congruences for the Bernoulli Numbers*

By Jonathan W. Tanner and Samuel S. Wagstaff, Jr.

To Daniel Shanks on his seventieth birthday

Abstract. We prove a new congruence for computing Bernoulli numbers modulo a prime. Since it is similar to Vandiver's congruences but has fewer terms, it may be used to test primes for regularity efficiently. We have programmed this test on a CYBER 205 computer. Fermat's "Last Theorem" has been proved for all exponents up to 150000.

1. Introduction. The first step in proving Fermat's "Last Theorem" (FLT) for a prime exponent p by computer is to determine the Bernoulli numbers B_{2k} with $2 \leqslant 2k \leqslant p - 3$ whose numerator is divisible by p. We use the even index notation for the Bernoulli numbers: $B_2 = 1/6$, $B_4 = -1/30$, etc. If p divides none of these Bernoulli numbers, then p is *regular* and FLT holds for exponent p by a theorem of Kummer. But if p divides some B_{2k} with $2 \leqslant 2k \leqslant p - 3$, then p is *irregular* and $(p, 2k)$ is called an *irregular pair*. Additional work is needed to prove FLT for an irregular prime exponent. We have performed this work, which is easy compared to the first step, and proved FLT for all primes p in the interval $125000 < p < 150000$. Since we have built on the work of others (see [6] and its references), FLT is now known to be true for all exponents up to 150000.

During the past 50 years several researchers have used congruences like (2) and (7) below to compute B_{2k} modulo p and find irregular pairs. (A minor problem arises when the coefficient of B_{2k} is a multiple of p. That rare case is discussed at the end of Section 3.) Similar congruences with fewer terms would provide swifter tests for regularity. Theorem 3 gives such a congruence. This theorem was used to compute the irregular pairs with $125000 < p < 150000$. The CYBER 205 program for this calculation is described in Section 3. In Section 4, we prove a lower bound for the number of terms in congruences like (2)–(5).

Many of the ideas in this paper were contained in the undergraduate thesis [4] of the first author, which was written at Harvard University under the supervision of Professor John T. Tate.

2. Some Congruences for the Bernoulli Numbers. We begin with Vandiver's well-known corollary to Voronoi's congruence. The notation $[x]$ means the greatest integer $\leqslant x$.

Received February 27, 1986; revised June 11, 1986 and June 30, 1986.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11B68, 11A07, 11D41.
Key words and phrases. Bernoulli numbers, Vandiver's congruence, Fermat's "Last Theorem."
*This research supported in part by an NSF grant.

0025-5718/87 $1.00 + $.25 per page

THEOREM 1 (VANDIVER [5]; see also [2]). *If p is an odd prime, $k \geqslant 1$, $p-1$ does not divide $2k$, $a \geqslant 2$ and $(a, p) = 1$, then*

$$(1 - a^{2k})\frac{B_{2k}}{2k} \equiv a^{2k-1} \sum_{j=1}^{a-1} \sum_{s=0}^{[jp/a]} s^{2k-1} \pmod{p}.$$

By Fermat's "Little Theorem," we can rewrite this as

$$\begin{aligned}(a^{p-2k} - a)\frac{B_{2k}}{2k} &\equiv \sum_{j=1}^{a-1} \sum_{s=0}^{[jp/a]} s^{2k-1} \\ &\equiv \sum_{j=1}^{a-1} (a-j) \sum_{(j-1)p/a < s < jp/a} s^{2k-1} \pmod{p}.\end{aligned}$$

The quantities jp/a, $j = 1, 2, \ldots, a-1$, cannot be integers because $(a, p) = 1$. When we combine the terms s^{2k-1} and $(p-s)^{2k-1} \equiv -s^{2k-1} \pmod{p}$, we find

$$\begin{aligned}(a^{p-2k} - a)\frac{B_{2k}}{2k} &\equiv \sum_{j=1}^{[a/2]} (a+1-2j) \sum_{(j-1)p/a < s < jp/a} s^{2k-1} \\ &\equiv \sum_{j=1}^{[a/2]} (a+1-2j) S\left(\frac{j-1}{a}, \frac{j}{a}\right) \pmod{p},\end{aligned} \tag{1}$$

where we have set $S(x, y) = \sum_{xp < s < yp} s^{2k-1}$. (A sum over the empty set is 0.)

We will keep p and $2k$ fixed in this section. Write $C(a, b, c) = a^{p-2k} + b^{p-2k} - c^{p-2k} - 1$. Let $\{z\}$ represent congruence (1) with a replaced by z. If $c = a + b - 1$, then the linear combination $\{a\} + \{b\} - \{c\}$ has $C(a, b, c)$ for the coefficient of $B_{2k}/2k$. The condition $c = a + b - 1$ guarantees a good deal of cancellation on the right side of $\{a\} + \{b\} - \{c\}$. For example, the combinations $\{2\} + \{3\} - \{4\}$, $\{3\} + \{4\} - \{6\}$, $\{4\} + \{5\} - \{8\}$, and $\{2\} + \{5\} - \{6\}$ are

$$C(2,3,4)\frac{B_{2k}}{2k} \equiv 2S\left(\frac{1}{4}, \frac{1}{3}\right) \pmod{p}, \tag{2}$$

$$C(3,4,6)\frac{B_{2k}}{2k} \equiv 2S\left(\frac{1}{6}, \frac{1}{4}\right) \pmod{p}, \tag{3}$$

$$C(4,5,8)\frac{B_{2k}}{2k} \equiv 2S\left(\frac{1}{8}, \frac{1}{5}\right) + 2S\left(\frac{3}{8}, \frac{2}{5}\right) \pmod{p}, \tag{4}$$

and

$$C(2,5,6)\frac{B_{2k}}{2k} \equiv 2S\left(\frac{1}{6}, \frac{1}{5}\right) + 2S\left(\frac{1}{3}, \frac{2}{5}\right) \pmod{p}, \tag{5}$$

respectively. The sums in congruences (2) and (3) have about $p/12$ terms s^{2k-1} each, while those in (4) and (5) have a total of about $p/10$ terms each. Obviously, B_{2k} may be computed modulo p more efficiently by congruences with fewer terms. Wagstaff [6] searched for congruences like

$$(\text{coefficient})\frac{B_{2k}}{2k} \equiv 2\sum_i S(x_i, y_i) \pmod{p}, \tag{6}$$

where x_i and y_i are exact multiples of $1/n$ with $n \leqslant 120$. He found nothing better than (2) and (3), and speculated that (6) could never have fewer than about $p/12$ terms in all its sums together. We prove in Section 4 that the right side of $\{a\} + \{b\} - \{a + b - 1\}$ never has fewer than about $p/12$ terms.

In spite of these negative results, some congruences for B_{2k} modulo p do have fewer than about $p/12$ terms. Vandiver [5] noted that the endpoints of the second sum in (5) are exactly twice those of the first sum. There is a one-to-one correspondence $s \leftrightarrow 2s$ between s in the first sum and even s in the second sum. When we separate the even and odd s in the second sum, (5) becomes

$$\begin{aligned} C(2,5,6)\frac{B_{2k}}{4k} &\equiv (1 + 2^{2k-1})S\left(\frac{1}{6}, \frac{1}{5}\right) + \sum_{\substack{p/3 < s < 2p/5 \\ s \text{ odd}}} s^{2k-1} \\ &\equiv (1 + 2^{2k-1})S\left(\frac{1}{6}, \frac{1}{5}\right) - 2^{2k-1}S\left(\frac{3}{10}, \frac{1}{3}\right) \pmod{p}. \end{aligned} \tag{7}$$

The total number of s's in the sums of (7) is about $p/15$. Theorem 3 below gives a similar congruence with about $p/18$ terms.

Vandiver's idea works best when the endpoints of one sum $S(x, y)$ in the congruence are exact multiples of the endpoints of some other sum. This coincidence appears in striking form in $\{2\} + \{b\} - \{b + 1\}$. Congruences (2) and (5) are the cases $b = 3$ and $b = 5$ of Theorem 2.

THEOREM 2. *Assume $b \geqslant 2$, p is prime, $p > b + 1$, $k \geqslant 1$ and $p - 1$ does not divide $2k$. Then*

$$C(2, b, b + 1)\frac{B_{2k}}{4k} \equiv \sum_{m=1}^{[b/2]} S\left(\frac{m}{b+1}, \frac{m}{b}\right) \pmod{p}.$$

When b is odd, the total number of terms s^{2k-1} in these sums is about $(b - 1)p/8b < p/8$. When b is even, the number of terms is about $(b + 2)p/8(b + 1) > p/8$.

Proof. By the corollary (1) to Vandiver's congruence we have

$$\begin{aligned} C(2, b, b + 1)\frac{B_{2k}}{2k} \equiv S\left(0, \frac{1}{2}\right) &+ \sum_{j=1}^{[b/2]} (b + 1 - 2j)S\left(\frac{j-1}{b}, \frac{j}{b}\right) \\ &- \sum_{j=1}^{[(b+1)/2]} (b + 2 - 2j)S\left(\frac{j-1}{b+1}, \frac{j}{b+1}\right) \pmod{p}. \end{aligned}$$

Let $l = \text{LCM}(2, b, b + 1) = b(b + 1)$. Express the sums above in terms of $S((i - 1)/l, i/l)$:

$$\begin{aligned} C(2, b, b + 1)\frac{B_{2k}}{2k} &\equiv \sum_{i=1}^{l/2} S\left(\frac{i-1}{l}, \frac{i}{l}\right) + \sum_{j=1}^{[b/2]} (b + 1 - 2j) \sum_{i=j(b+1)-b}^{j(b+1)} S\left(\frac{i-1}{l}, \frac{i}{l}\right) \\ &\quad - \sum_{j=1}^{[(b+1)/2]} (b + 2 - 2j) \sum_{i=jb-b+1}^{jb} S\left(\frac{i-1}{l}, \frac{i}{l}\right) \\ &\equiv 2\sum_{i=1}^{l/2} \left(\left[\frac{i-1}{b}\right] - \left[\frac{i-1}{b+1}\right]\right) S\left(\frac{i-1}{l}, \frac{i}{l}\right) \pmod{p}. \end{aligned}$$

Now the quantity $[(i-1)/b] - [(i-1)/(b+1)]$ is 1 when $mb < i \leqslant m(b+1)$ for some $1 \leqslant m \leqslant h = [b/2]$, and it is 0 for all other i in $1 \leqslant i \leqslant l/2$. Therefore,

$$C(2,b,b+1)\frac{B_{2k}}{4k} \equiv \sum_{m=1}^{h} \sum_{i=mb+1}^{m(b+1)} S\left(\frac{i-1}{l}, \frac{i}{l}\right) \equiv \sum_{m=1}^{h} S\left(\frac{mb}{l}, \frac{m(b+1)}{l}\right)$$

$$\equiv \sum_{m=1}^{h} S\left(\frac{m}{b+1}, \frac{m}{b}\right) \pmod{p}.$$

The total number of terms in the sums is about

$$\left(\frac{1}{b} - \frac{1}{b+1}\right)(1 + 2 + \cdots + h)p = \frac{h(h+1)}{2b(b+1)}p.$$

This quantity is $hp/4b = (b-1)p/8b < p/8$ when b is odd. It is $(h+1)p/4(b+1) = (b+2)p/8(b+1) > p/8$ when b is even. This completes the proof.

The following two propositions give the basic facts we need to manipulate congruences like the ones in Theorem 2. As usual, p is an odd prime and $p-1$ does not divide $2k$.

PROPOSITION 1. *Let d be a positive integer relatively prime to p. If $x < y$, then*

$$S(x,y) \equiv d^{2k-1} \sum_{i=0}^{d-1} S\left(\frac{x+i}{d}, \frac{y+i}{d}\right) \pmod{p}.$$

Proof. In the sum for i on the right side, s lies in the interval $(x+i)p/d < s < (y+i)p/d$. These inequalities are equivalent to $xp < ds - ip < yp$. Therefore, the right side equals

$$\sum_{i=0}^{d-1} \sum_{xp < ds - ip < yp} (ds)^{2k-1} = \sum_{i=0}^{d-1} \sum_{\substack{xp < t - ip < yp \\ d \mid t}} t^{2k-1}$$

$$\equiv \sum_{i=0}^{d-1} \sum_{\substack{xp < t - ip < yp \\ d \mid t}} (t - ip)^{2k-1} \pmod{p}.$$

Since $(p,d) = 1$, every s in $xp < s < yp$ is uniquely expressible in the form $t - ip$ with $d \mid t$ and $0 \leqslant i < d$. Hence, the right side is $\sum_{xp<s<yp} s^{2k-1} = S(x,y)$.

We will refer to an application of Proposition 1 as "splitting the interval (x,y) into d parts."

PROPOSITION 2. *If $x < y$, then $S(x,y) \equiv -S(1-y, 1-x) \pmod{p}$.*

Proof. Change variables and use $(p-s)^{2k-1} \equiv -s^{2k-1} \pmod{p}$.

The derivation of (7) from (5) is just an application of the two propositions, with $d = 2$:

$$S\left(\frac{1}{6}, \frac{1}{5}\right) + S\left(\frac{1}{3}, \frac{2}{5}\right) \equiv S\left(\frac{1}{6}, \frac{1}{5}\right) + 2^{2k-1}S\left(\frac{1}{6}, \frac{1}{5}\right) + 2^{2k-1}S\left(\frac{2}{3}, \frac{7}{10}\right)$$

$$\equiv (1 + 2^{2k-1})S\left(\frac{1}{6}, \frac{1}{5}\right) - 2^{2k-1}S\left(\frac{3}{10}, \frac{1}{3}\right).$$

In the proof of Theorem 3 we will use other simple properties of $S(x, y)$, such as this one, which we used already in the proof of Theorem 2: If $x < y < z$ and yp is not an integer, then $S(x, z) = S(x, y) + S(y, z)$.

THEOREM 3. *If p is a prime > 10 and $p - 1$ does not divide $2k$, then*

$$\begin{aligned} C(2,9,10)\frac{B_{2k}}{4k} \equiv{}& (1 + 2^{2k-1} + 3^{2k-1} + 4^{2k-1})S\left(\frac{1}{10}, \frac{13}{120}\right) \\ &+ (1 + 2^{2k-1} + 3^{2k-1} + 4^{2k-1} + 12^{2k-1})S\left(\frac{13}{120}, \frac{1}{9}\right) \\ &- 3^{2k-1}S\left(\frac{2}{9}, \frac{7}{30}\right) - (2^{2k-1} + 6^{2k-1})S\left(\frac{5}{18}, \frac{17}{60}\right) \\ &- 2^{2k-1}S\left(\frac{17}{60}, \frac{3}{10}\right) - (2^{2k-1} + 4^{2k-1} + 12^{2k-1})S\left(\frac{7}{18}, \frac{47}{120}\right) \\ &- (2^{2k-1} + 4^{2k-1})S\left(\frac{47}{120}, \frac{2}{5}\right) \pmod{p}. \end{aligned}$$

The total number of terms on the right side is about $p/18$.

Proof. All congruences in this proof have modulus p. Theorem 2 with $b = 9$ gives

$$C(2,9,10)\frac{B_{2k}}{4k} \equiv S\left(\frac{1}{10}, \frac{1}{9}\right) + S\left(\frac{1}{5}, \frac{2}{9}\right) + S\left(\frac{3}{10}, \frac{1}{3}\right) + S\left(\frac{2}{5}, \frac{4}{9}\right).$$

Split the third interval $(3/10, 1/3)$ into three parts:

$$S\left(\frac{3}{10}, \frac{1}{3}\right) \equiv 3^{2k-1}S\left(\frac{1}{10}, \frac{1}{9}\right) + 3^{2k-1}S\left(\frac{13}{30}, \frac{4}{9}\right) + 3^{2k-1}S\left(\frac{23}{30}, \frac{7}{9}\right).$$

By Proposition 2, $S(23/30, 7/9) \equiv -S(2/9, 7/30)$. Note that the intervals $(13/30, 4/9)$ and $(2/5, 4/9)$ overlap. When we combine the three congruences just stated, we find

$$\begin{aligned} C(2,9,10)\frac{B_{2k}}{4k} \equiv{}& (1 + 3^{2k-1})S\left(\frac{1}{10}, \frac{1}{9}\right) + S\left(\frac{1}{5}, \frac{2}{9}\right) - 3^{2k-1}S\left(\frac{2}{9}, \frac{7}{30}\right) \\ &+ S\left(\frac{2}{5}, \frac{13}{30}\right) + (1 + 3^{2k-1})S\left(\frac{13}{30}, \frac{4}{9}\right). \end{aligned}$$

Now we split the intervals $(2/5, 13/30)$ and $(13/30, 4/9)$ into two parts and apply Proposition 2 to the second parts:

$$\begin{aligned} S\left(\frac{2}{5}, \frac{13}{30}\right) &\equiv 2^{2k-1}S\left(\frac{1}{5}, \frac{13}{60}\right) + 2^{2k-1}S\left(\frac{7}{10}, \frac{43}{60}\right) \\ &\equiv 2^{2k-1}S\left(\frac{1}{5}, \frac{13}{60}\right) - 2^{2k-1}S\left(\frac{17}{60}, \frac{3}{10}\right), \\ S\left(\frac{13}{30}, \frac{4}{9}\right) &\equiv 2^{2k-1}S\left(\frac{13}{60}, \frac{2}{9}\right) + 2^{2k-1}S\left(\frac{43}{60}, \frac{13}{18}\right) \\ &\equiv 2^{2k-1}S\left(\frac{13}{60}, \frac{2}{9}\right) - 2^{2k-1}S\left(\frac{5}{18}, \frac{17}{60}\right). \end{aligned}$$

Since $S(1/5, 2/9) = S(1/5, 13/60) + S(13/60, 2/9)$, we have

$$\begin{aligned} C(2,9,10)\frac{B_{2k}}{4k} \equiv{}& (1 + 3^{2k-1})S\left(\frac{1}{10}, \frac{1}{9}\right) + (1 + 2^{2k-1})S\left(\frac{1}{5}, \frac{13}{60}\right) \\ &+ \left(1 + (1 + 3^{2k-1})2^{2k-1}\right)S\left(\frac{13}{60}, \frac{2}{9}\right) - 3^{2k-1}S\left(\frac{2}{9}, \frac{7}{30}\right) \\ &- (1 + 3^{2k-1})2^{2k-1}S\left(\frac{5}{18}, \frac{17}{60}\right) - 2^{2k-1}S\left(\frac{17}{60}, \frac{3}{10}\right). \end{aligned}$$

Finally, we split the intervals (1/5, 13/60) and (13/60, 2/9) into two parts and apply Proposition 2 to the second parts:

$$\begin{aligned} S\left(\frac{1}{5}, \frac{13}{60}\right) &\equiv 2^{2k-1}S\left(\frac{1}{10}, \frac{13}{120}\right) + 2^{2k-1}S\left(\frac{3}{5}, \frac{73}{120}\right) \\ &\equiv 2^{2k-1}S\left(\frac{1}{10}, \frac{13}{120}\right) - 2^{2k-1}S\left(\frac{47}{120}, \frac{2}{5}\right), \\ S\left(\frac{13}{60}, \frac{2}{9}\right) &\equiv 2^{2k-1}S\left(\frac{13}{120}, \frac{1}{9}\right) + 2^{2k-1}S\left(\frac{73}{120}, \frac{11}{18}\right) \\ &\equiv 2^{2k-1}S\left(\frac{13}{120}, \frac{1}{9}\right) - 2^{2k-1}S\left(\frac{7}{18}, \frac{47}{120}\right). \end{aligned}$$

When these expressions are substituted into the previous congruence and the overlap of the interval (1/10, 1/9) with (1/10, 13/120) and (13/120, 1/9) is noted, the formula in the statement of the theorem is obtained.

Using the same techniques and starting from (7), we can prove a congruence for B_{2k} modulo p with about $p/19.2$ terms in the sums. First split the interval (3/10, 1/3) into four parts. Then split the interval (13/40, 1/3) into four parts. With even more tedious arithmetic, we are able to prove a similar congruence for B_{2k} modulo p with fewer than about $p/22$ terms in the sums, but it is too complicated to describe here. We do not know whether there are other congruences of this type having $< \varepsilon p$ terms for arbitrarily small $\varepsilon > 0$, allowing sufficiently complicated coefficients, the way lacunary recurrence formulas for the Bernoulli numbers can be derived [3] having arbitrarily large gaps, allowing sufficiently complicated coefficients.

3. The Search for Irregular Primes. We used Theorem 3 (and, on the rare occasions when p divides $C(2, 9, 10)$, other congruences) to determine the irregular pairs $(p, 2k)$ with $125000 < p < 150000$. The following table lists the primes with *index of irregularity* greater than 3, that is, the primes for which there are more than 3 irregular pairs.

p	The $2k$ for which p divides B_{2k}			
125927	86088	92020	96554	105006
127247	26164	113554	123032	124714
135613	7274	94796	100336	121574
149287	27394	50226	137698	146452

Using the same methods that Wagstaff [6] used to prove FLT up to 125000, we proved FLT for all exponents in the interval $125000 < p < 150000$. No problems or unusual cases arose. Of the 2114 primes in this range, 1270 are regular and 844 are irregular. There are 656 primes which divide only one Bernoulli number, 145 which divide exactly two, 39 which divide exactly three and 4 (see the table) which divide four Bernoulli numbers. There are no primes in this range with index of irregularity > 4.

Our CYBER 205 program was written in ratfor and translated into FORTRAN on a VAX. The appropriate s's were stored in one vector and their squares in another vector. The program repeatedly multiplied the first vector componentwise

by the second vector modulo p. During this operation, the dot product of the two vectors was also computed. The vector instructions of the CYBER 205 provide an extraordinarily efficient way of coding these operations. The CYBER 205 program ran nearly 100 times faster than one [6] for the IBM 360/75, although the ratio of execution times for most programs on these two machines is much less than 100. The main reason for this superb performance is that vector multiplication is done in a pipeline on the CYBER 205, and is as fast as vector addition. See Section 2.3 of [1] for a description of the CYBER 205.

On page 575 of [5], Vandiver reports a device suggested by M. M. Abernathy to speed the computation of the right side of (7) when $p \equiv 1 \pmod 4$. For such primes, $(p-1)/2$ is even. Separate the terms on the right side into two sums, T_{QR} over quadratic residues $s \pmod p$ and T_{QNR} over quadratic nonresidues $s \pmod p$. Then the right side is just $T_{QR} + T_{QNR}$. Also, the right side for the exponent $2k - 1 + (p-1)/2$ is $T_{QR} - T_{QNR}$ by Euler's criterion. (We have ignored here the possible change in the coefficients, which is easy to handle.) Therefore, the right sides for exponents $2k-1$ and $2k-1+(p-1)/2$ may be evaluated together. The sums T_{QR} and T_{QNR} need be computed only for exponents $2k - 1 < p/2$. This trick nearly halves the effort required for a prime. It works for any congruence derived from Theorem 1. We used it in our program for the congruence of Theorem 3 whenever $p \equiv 1 \pmod 4$.

Occasionally, the coefficients $C(a, b, a+b-1)$ in (2)–(5) and the congruence of Theorem 3 all vanish modulo p. (For example, suppose $p \equiv 1 \pmod 4$, $2k = (p-1)/2$ and $a^{2k} \equiv 1 \pmod p$ for $a = 2, 3$, and 5. Then $a^{p-2k} \equiv a \pmod p$ for $a = 2, 3, 4, 5, 6, 8, 9$, and 10. For another example, suppose $p \equiv 3 \pmod 4$, $2k = (p+1)/2$ and $a^{p-2k} \equiv 1 \pmod p$ for $a = 2, 3$, and 5. Then $a^{p-2k} \equiv 1 \pmod p$ for $a = 2, 3, 4, 5, 6, 8, 9$, and 10.) In such a case, one may try E. Lehmer's congruence,

$$(8) \qquad (2^{2k-1} + 3^{2k-1} + 6^{2k-1} - 1)\frac{B_{2k}}{4k} \equiv \sum_{0<s<p/6} (p - 6s)^{2k-1} \pmod{p^2}.$$

In about half of these cases, the coefficient on the left side of (8) does not vanish modulo p, so that one may decide whether p divides B_{2k} by summing about $p/6$ terms modulo p. The sum must be computed modulo p^2 in the other cases. When p can fit in a computer word, but p^2 cannot, the latter calculation requires expensive double-precision integer arithmetic. We completely avoided the problems of (8) by using Theorem 2: When Theorem 3 and (2) could not decide whether p divided B_{2k}, the program determined the least odd $b > 2$ for which $C(2, b, b+1)$ was not 0 modulo p. Then it determined whether $(p, 2k)$ was regular by computing the right side of the congruence in Theorem 2, which entailed summing fewer than about $p/8$ terms modulo p. In each of the 439 instances of this case with $125000 < p < 150000$, some prime between 6 and 30 proved to be a suitable choice for b.

4. A Lower Bound on the Number of Terms in Certain Congruences. We now prove the result to which we adverted in Section 2, namely, that the right side of $\{a\} + \{b\} - \{a+b-1\}$ always has at least about $p/12$ terms. We will only sketch the proof because it is tedious and because the result is not needed elsewhere in this paper.

Throughout this section we assume that p is an odd prime, $k \geqslant 1$, $p-1$ does not divide $2k$ and $2 \leqslant a,\ b,\ a+b-1 < p$. We may assume with no loss of generality that $a \leqslant b$. The proof of Theorem 4 requires two lemmas.

LEMMA 1. *The right side of* $\{a\} + \{b\} - \{a+b-1\}$ *can be written* $\sum_i n_i S(x_i, y_i)$, *where* $n_i = 2$ *or* -2 *and the intervals* (x_i, y_i) *are pairwise disjoint.*

Proof. Let $0 < s < p/2$. If $(j-1)p/a < s < jp/a$ for some $1 \leqslant j \leqslant [a/2]$, then s^{2k-1} appears on the right side of $\{a\}$ with coefficient $a+1-2j$. But $j-1 = [as/p]$, so the coefficient is $a-1-2[as/p]$. Using this and analogous results for $\{b\}$ and $\{a+b-1\}$, we see that the coefficient of s^{2k-1} in $\{a\} + \{b\} - \{a+b-1\}$ is

$$2([(a+b-1)s/p] - [as/p] - [bs/p]).$$

It follows easily from the inequality $[x]+[y] \leqslant [x+y] \leqslant [x]+[y]+1$ that $-1 \leqslant [(a+b-1)s/p] - [as/p] - [bs/p] \leqslant 1$. Therefore, the coefficient of s^{2k-1} in $\{a\} + \{b\} - \{a+b-1\}$ is -2, 0 or $+2$. This concludes the proof.

The coefficient -2 occurs commonly, as in

$$C(3,5,7)\frac{B_{2k}}{2k} \equiv 2S\left(\frac{1}{7}, \frac{1}{5}\right) + 2S\left(\frac{2}{7}, \frac{1}{3}\right) - 2S\left(\frac{2}{5}, \frac{3}{7}\right) \pmod{p}.$$

Suppose we make the obvious cancellation of like terms in the right side of $\{a\} + \{b\} - \{a+b-1\}$, but do not transform the sum using Propositions 1 and 2. Then the form $\sum_i n_i S(x_i, y_i)$, with $n_i = 2$ or -2, is unique and we make these two definitions: Let $L(a,b) = \sum_i (y_i - x_i)$ and $H(a,b) = \sum_i n_i (y_i - x_i)$. (Theorem 2 asserts that $L(2,b) = (b-1)/8b$ when b is odd and $(b+2)/8(b+1)$ when b is even. Moreover, $H(2,b) = 2L(2,b)$ for all b because all $n_i = +2$ when $a = 2$.) We want to prove that $L(a,b) \geqslant 1/12$ for all a and b. We have introduced $H(a,b)$ because it is related to $L(a,b)$ and is easier to compute.

The next lemma is the analogue of Theorem 2 with $a = 2$ changed to $a = 3$.

LEMMA 2. *Assume* $b \geqslant 3$, p *is prime*, $p > b+2$, $k \geqslant 1$, *and* $p-1$ *does not divide* $2k$. *Then*

$$C(3,b,b+2)B_{2k}/4k \equiv \sum_{m=1}^{[(b-1)/3]} S\left(\frac{m}{b+2}, \frac{m}{b}\right) + S\left(\frac{[(b+2)/3]}{b+2}, \frac{1}{3}\right) - \sum_{m=[(b+2)/3]}^{[b/2]} S\left(\frac{m}{b}, \frac{m+1}{b+2}\right) \pmod{p}.$$

Also,

$$L(3,b) = \frac{1}{3} + \frac{[(b+1)/2][(b+2)/2] - 2[(2b+3)/3][(b+2)/3]}{b(b+2)}.$$

In other words,

$$L(3,b) = \frac{(b-1)(b+3)}{12b(b+2)} + \frac{2[(b+3)/6]^2}{b(b+2)}$$

when b is odd and

$$L(3,b) = \frac{1}{12} + \frac{2[b/6]([b/6]+1)}{b(b+2)}$$

when b is even. Finally, $\lim_{b\to\infty} L(3,b) = 5/36$.

Proof. Let $l = \mathrm{LCM}(3, b, b+2)$. All congruences are modulo p. As in the proof of Theorem 2, we find

$$C(3,b,b+2)\frac{B_{2k}}{2k} \equiv 2\sum_{i=1}^{[l/2]}\left(\left[\frac{i-1}{l/(b+2)}\right] - \left[\frac{i-1}{l/b}\right]\right)S\left(\frac{i-1}{l}, \frac{i}{l}\right) - 2S\left(\frac{1}{3}, \frac{[l/2]}{l}\right).$$

Now $[(i-1)/(l/(b+2))] - [(i-1)/(l/b)]$ is 1 if $ml/(b+2) < i \leqslant ml/b$ for some $1 \leqslant m \leqslant [b/2]$ or if $([b/2]+1)l/(b+2) < i \leqslant [l/2]$, and it is 0 for all other i in $1 \leqslant i \leqslant [l/2]$. Therefore,

$$C(3,b,b+2)\frac{B_{2k}}{4k} \equiv \sum_{m=1}^{[b/2]} S\left(\frac{m}{b+2}, \frac{m}{b}\right) + S\left(\frac{[b/2]+1}{b+2}, \frac{[l/2]}{l}\right) - S\left(\frac{1}{3}, \frac{[l/2]}{l}\right).$$

The term $-S(1/3, [l/2]/l)$ cancels the preceding term and the terms of the sum having $m > b/3$, but introduces new terms which are sums over the complementary intervals $(m/b, (m+1)/(b+2))$. The term $S([(b+2)/3]/(b+2), 1/3)$ in the statement of the lemma handles the transition at $b/3$. The formulas for $L(3,b)$ are obtained by adding the lengths of the intervals and considering the possible values of b modulo 6 as separate cases. The limit is a simple consequence of these formulas.

THEOREM 4. *Assume $2 \leqslant a \leqslant b$ and $a + b - 1 < p$. Then there are always at least about $p/12$ terms s^{2k-1} on the right side of the congruence $\{a\} + \{b\} - \{a+b-1\}$. That is, $L(a,b) \geqslant 1/12$ for all such a and b. Moreover, $L(2,3) = L(3,4) = 1/12$, and $L(a,b) = 1/12$ only in these two cases.*

Proof. Let $c = a + b - 1$. Note that

$$H(a,b) = \sum_{j=1}^{[a/2]}(a+1-2j)\frac{1}{a} + \sum_{j=1}^{[b/2]}(b+1-2j)\frac{1}{b} - \sum_{j=1}^{[c/2]}(c+1-2j)\frac{1}{c}.$$

Now $\sum_{j=1}^{[a/2]}(a+1-2j)/a = [a/2][(a+1)/2]/a$, which is $a/4$ when a is even and $(a^2-1)/4a$ when a is odd. Thus, $H(a,b)$ is given by this table:

Case	a	b	c	$H(a,b)$
1	even	even	odd	$\dfrac{a+b}{4(a+b-1)}$
2	even	odd	even	$\dfrac{b-1}{4b}$
3	odd	even	even	$\dfrac{a-1}{4a}$
4	odd	odd	odd	$\dfrac{(a+b)(a-1)(b-1)}{4ab(a+b-1)}$

By Lemma 1, the n_i in the definition of $H(a, b)$ are 2 or -2, so $L(a, b) \geqslant H(a, b)/2$. Consider the four cases in turn.

In Case 1, $L(a, b) \geqslant (a + b)/8(a + b - 1) > 1/8 > 1/12$.

In Case 2, $L(a, b) \geqslant (b - 1)/8b$, which is $1/12$ when $b = 3$ and $\geqslant 1/10 > 1/12$ when $b \geqslant 5$. Note that $a = 2$ when $b = 3$ in this case.

In Case 3, $L(a, b) \geqslant (a - 1)/8a$, which is $\geqslant 1/10 > 1/12$ when $a \geqslant 5$. If $a = 3$ and b is even, then $L(a, b) = 1/12 + 2[b/6]([b/6] + 1)/b(b + 2)$ by Lemma 2. We have $L(3, 4) = 1/12$ and $L(3, b) > 1/12$ when $b \geqslant 6$.

In Case 4, $L(a, b) \geqslant (a + b)(a - 1)(b - 1)/8ab(a + b - 1)$. This lower bound increases monotonically with b when a is fixed. If $a \geqslant 5$, then $b \geqslant 5$, so $L(a, b) \geqslant 4/45 > 1/12$. Finally, if $a = 3$ and b is odd, then

$$L(a, b) = \frac{(b - 1)(b + 3)}{12b(b + 2)} + \frac{2[(b + 3)/6]^2}{b(b + 2)}$$

by Lemma 2. We have $L(3, 3) = 1/5 > 1/12$. Now $[(b + 3)/6] \geqslant (b - 1)/6$ because b is odd. Hence, $L(3, b) \geqslant (b - 1)(5b + 7)/36b(b + 2)$, which is $\geqslant 32/315 > 1/12$ when $b \geqslant 5$. This completes the proof.

A computer search found that $L(2, 5) = L(4, 5) = L(5, 6) = 1/10$ and suggests that $L(a, b) < 3/28$ only in these three cases and the two mentioned in Theorem 4. To show this, one would have to prove analogues of Lemma 2 for $L(5, b)$ and $L(7, b)$.

School of Medicine
University of Pennsylvania
Philadelphia, Pennsylvania 19104

Department of Computer Sciences
Purdue University
West Lafayette, Indiana 47907

1. R. W. HOCKNEY & C. R. JESSHOPE, *Parallel Computers: Architecture, Programming and Algorithms*, Adam Hilger, Bristol, 1981.

2. WELLS JOHNSON, "p-adic proofs of congruences for the Bernoulli numbers," *J. Number Theory*, v. 7, 1975, pp. 251–265.

3. D. H. LEHMER, "Lacunary recurrence formulas for the numbers of Bernoulli and Euler," *Ann. of Math.*, v. 36, 1935, pp. 637–649.

4. JONATHAN W. TANNER, *Proving Fermat's Last Theorem for Many Exponents by Computer*, B. A. Thesis, Harvard University, 1985.

5. H. S. VANDIVER, "On Bernoulli's numbers and Fermat's last theorem," *Duke Math. J.*, v. 3, 1937, pp. 569–584.

6. SAMUEL S. WAGSTAFF, JR., "The irregular primes to 125000," *Math. Comp.*, v. 32, 1978, pp. 583–591.