ACTA ARITHMETICA
LXXI.4 (1995)

On the converse of Wolstenholme's Theorem

by

Richard J. McIntosh (Regina, Sask.)

1. Introduction. Gauss ([Disquisitiones Arithmeticae, 1801, art. 329]) wrote:

The problem of distinguishing prime numbers from composite numbers (...) *is known to be one of the most important and useful in arithmetic.* (...) *The dignity of the science itself seems to require that every possible means be explored for the solution of a problem so elegant and so celebrated.*

Wilson's Theorem states that if p is prime then $(p-1)! \equiv -1 \pmod{p}$. It is easy to see that the converse of Wilson's Theorem also holds. Thus Wilson's Theorem can be used to identify the primes. Another congruence identifying the primes is

$$(p+1)(2p+1)(3p+1)\dots((p-1)p+1) \equiv 0 \pmod{(p-1)!}.$$

(For a proof see [21].) It is not difficult to show that $\binom{2p-1}{p-1} \equiv 1 \pmod{p}$ for all primes p. In 1819 Babbage [5, p. 271] observed that the stronger congruence $\binom{2p-1}{p-1} \equiv 1 \pmod{p^2}$ holds for all primes $p \geq 3$, and Wolstenholme [5, p. 271], in 1862, proved that $\binom{2p-1}{p-1} \equiv 1 \pmod{p^3}$ for all primes $p \geq 5$. The congruence $\binom{2n-1}{n-1} \equiv 1 \pmod{n^3}$ has no composite solutions $n < 10^9$. J. P. Jones ([9, problem B31, p. 47], [23, p. 21] and [12]) has conjectured that there are no composite solutions. Unlike that of Wilson's Theorem the converse of Wolstenholme's Theorem is a very difficult problem.

A set S of positive integers is a *Diophantine set* if there exists a polynomial $P(n, x_1, \dots, x_m)$ with integer coefficients such that $n \in S$ if and only if there exist nonnegative integers $x_1, \dots, x_m$ for which $P(n, x_1, \dots, x_m) = 0$. If we define $Q(n, x_1, \dots, x_m) = n(1 - P(n, x_1, \dots, x_m)^2)$, then the set S is identical to the positive range of Q as $n, x_1, \dots, x_m$ range over the nonnegative integers. One of the most important results obtained in the investigation of Hilbert's tenth problem (which asks for an algorithm to decide whether a

1991 *Mathematics Subject Classification*: 11A07, 11A41.

polynomial equation in several variables has a solution in integers) is that S is Diophantine if and only if S is recursively enumerable. (See [17], [4], [19] and [13].) From this it follows that the set of all prime numbers is Diophantine. In 1977 Yuri Matijasevič [18] proved the existence of a polynomial in 10 variables whose positive range is exactly the set of all prime numbers. It is not known if the primes can be represented by a polynomial with less than 10 variables. However, if the converse of Wolstenholme's Theorem were true, this would imply the existence of a prime representing polynomial in 7 variables [12].

In this article criteria for solutions of $\binom{2n-1}{n-1} \equiv 1 \pmod{n^r}$ are given in terms of the p-adic digits of n, sums of reciprocal cubes and Bernoulli numbers. Using heuristic arguments we formulate several conjectures on the solutions of these congruences.

2. A generalization of Wolstenholme's Theorem. For positive integers n, define the modified binomial coefficient

$$\binom{2n-1}{n-1}' = \prod_{\substack{k=1 \\ (k,n)=1}}^{n} \frac{2n-k}{k}$$

and observe that for primes p, $\binom{2p-1}{p-1}' = \binom{2p-1}{p-1}$.

Gauss ([Disquisitiones Arithmeticae, 1801, art. 78] and [5, p. 65]) stated the generalization of Wilson's Theorem: The product of the positive integers $< n$ and prime to n is congruent modulo n to -1 if $n = 4$, p^m or $2p^m$, where p is an odd prime, but to $+1$ if n is not of one of these three forms.

Wolstenholme's Theorem has the following generalization.

THEOREM 1. *For $n \geq 3$,*

$$\binom{2n-1}{n-1}' \equiv 1 + n^2\varepsilon_n \pmod{n^3}, \tag{1}$$

where

$$\varepsilon_n = \begin{cases} n/2 & \text{if } n \text{ is a power of } 2, \\ (-1)^{r+1}n/3 & \text{if } n \equiv 0 \pmod 3 \text{ and } n \text{ has exactly} \\ & r \text{ distinct prime factors, each} \not\equiv 1 \pmod 6, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Let $\phi(n)$ be the Euler phi-function and let $a_1, \ldots, a_{\phi(n)}$ be the positive integers not exceeding n that are relatively prime to n. Let S_k be the kth elementary symmetric function on the set $\{a_1, \ldots, a_{\phi(n)}\}$. For $n \geq 3$, $\phi(n)$ is even, and therefore

$$S_{\phi(n)} = \prod_i a_i = \prod_i (n - a_i)$$
$$= n^{\phi(n)} - n^{\phi(n)-1} S_1 + \ldots + n^2 S_{\phi(n)-2} - n S_{\phi(n)-1} + S_{\phi(n)}.$$

Hence

$$0 = n^{\phi(n)} - n^{\phi(n)-1} S_1 + \ldots + n^2 S_{\phi(n)-2} - n S_{\phi(n)-1}.$$

Adding this equation to the identity

$$\prod_i (n + a_i) = n^{\phi(n)} + n^{\phi(n)-1} S_1 + \ldots + n^2 S_{\phi(n)-2} + n S_{\phi(n)-1} + S_{\phi(n)},$$

we obtain

$$\prod_i (n + a_i) = 2n^{\phi(n)} + 2n^{\phi(n)-2} S_2 + \ldots + 2n^2 S_{\phi(n)-2} + S_{\phi(n)}.$$

Thus

$$\prod_i (n + a_i) \equiv 2n^2 S_{\phi(n)-2} + S_{\phi(n)} \pmod{n^4}$$

and therefore

$$\binom{2n-1}{n-1}' = \prod_i \frac{n + a_i}{a_i} \equiv \frac{S_{\phi(n)} + 2n^2 S_{\phi(n)-2}}{S_{\phi(n)}}$$
$$= 1 + n^2 \sum_{i \neq j} a_i^{-1} a_j^{-1} = 1 + n^2 \Big\{ \Big(\sum_i a_i^{-1} \Big)^2 - \sum_i a_i^{-2} \Big\}$$
$$\equiv 1 - n^2 \sum_i a_i^{-2} \pmod{n^4},$$

because

$$\sum_i a_i^{-1} \equiv 0 \pmod{n},$$

which follows from the fact that $(a_1^{-1}, a_2^{-1}, \ldots, a_{\phi(n)}^{-1})$ is a permutation modulo n of $(a_1, \ldots, a_{\phi(n)})$ and

$$\sum_i a_i = \sum_{i=1}^{\phi(n)/2} a_i + \sum_{i=1}^{\phi(n)/2} (n - a_i) = \frac{\phi(n)}{2}\, n \equiv 0 \pmod{n}.$$

Again, using the fact that $(a_1^{-1}, a_2^{-1}, \ldots, a_{\phi(n)}^{-1})$ is a permutation modulo n of $(a_1, \ldots, a_{\phi(n)})$, we obtain

$$\binom{2n-1}{n-1}' \equiv 1 - n^2 \sum_i a_i^{-2} \equiv 1 - n^2 \sum_i a_i^2 \pmod{n^3}.$$

It remains to show that

$$\sum_i a_i^2 \equiv -\varepsilon_n \pmod{n},$$

where ε_n is defined in the statement of the theorem.

Since

$$\sum_{k=1}^{n} k^2 = \sum_{d|n} \sum_{\substack{k=1 \\ (k,n)=d}}^{n} k^2 = \sum_{d|n} d^2 \sum_{\substack{j=1 \\ (j,n/d)=1}}^{n/d} j^2 = \sum_{d|n} \left(\frac{n}{d}\right)^2 \sum_{\substack{j=1 \\ (j,d)=1}}^{d} j^2,$$

we have by Möbius inversion

$$\sum_i a_i^2 = \sum_{\substack{k=1 \\ (k,n)=1}}^{n} k^2 = \sum_{d|n} \left(\frac{n}{d}\right)^2 \mu\left(\frac{n}{d}\right) \sum_{k=1}^{d} k^2$$
$$= \sum_{d|n} \mu\left(\frac{n}{d}\right) \frac{n^2(d+1)(2d+1)}{6d}.$$

The value of the last sum modulo n depends on the divisors of n. It is congruent to 0 if n is relatively prime to 6. The other cases are more tedious; since they are not needed elsewhere in this paper their proofs are omitted. ∎

H. W. Brinkmann [1] in his partial solution to David Segal's conjecture observed the following relation between the ordinary binomial coefficient and the modified binomial coefficient:

$$\binom{2n-1}{n-1} = \prod_{d|n} \binom{2d-1}{d-1}'. \tag{2}$$

3. The congruence $\binom{2n-1}{n-1} \equiv 1 \pmod{n}$. By (1) and (2) it is not difficult to show that the congruence

$$\binom{2n-1}{n-1} \equiv 1 \pmod{n} \tag{3}$$

is satisfied by primes, squares of odd primes and cubes of primes ≥ 5.

A beautiful theorem of E. Lucas ([16] and [5, p. 271]) states that for every prime p,

$$\binom{n}{k} \equiv \binom{n_0}{k_0}\binom{n_1}{k_1}\binom{n_2}{k_2} \cdots \binom{n_r}{k_r} \pmod{p}$$

(with the usual convention that $\binom{a}{b} = 0$ if $a < b$), where the base p expansions of n and k are

$$n = n_0 + n_1 p + n_2 p^2 + \ldots + n_r p^r \quad (0 \leq n_i \leq p-1)$$

and

$$k = k_0 + k_1 p + k_2 p^2 + \ldots + k_r p^r \quad (0 \leq k_i \leq p-1).$$

E. Kummer ([14] and [5, p. 270]) proved that if p^m is the highest power of a prime p dividing $\binom{n}{k}$, then m is equal to the number of carries when adding k and $n-k$ in base p arithmetic. We immediately see that for odd primes p a necessary condition for

$$\binom{2n-1}{n-1} \equiv 1 \pmod{p}$$

is that each base p digit $n_i \le (p-1)/2$.

EXAMPLE. If $p \equiv 1 \pmod 4$ is prime and $n = (p-1)/2 + p^r$ for $r \ge 1$, then

$$\binom{2n-1}{n-1} \equiv \binom{p-2}{(p-3)/2}\binom{2}{1} = \binom{p-1}{(p-1)/2} \equiv 1 \pmod{p}.$$

The only solutions $n < 10^9$ of (3) that are not prime powers are 29×937 and 787×2543. Beyond this range we found one more solution: 69239×231433. None of these satisfy Wolstenholme's congruence.

4. The congruence $\binom{2p-1}{p-1} \equiv 1 \pmod{p^4}$. From (1) and (2) we see that for primes p the following are equivalent:

$$\binom{2p-1}{p-1} \equiv 1 \pmod{p^4}, \tag{4}$$

$n = p^2$ satisfies

$$\binom{2n-1}{n-1} \equiv 1 \pmod{n^2}, \tag{5}$$

and $n = p^4$ satisfies (3). The only composite solution $n < 10^9$ of (5) is $283686649 = 16843^2$. We conjecture that $n \ge 3$ satisfies (5) if and only if n is a prime or n is the square of a prime satisfying (4). We call primes satisfying (4) *Wolstenholme primes*. There are many equivalent conditions for Wolstenholme primes, some of which are very useful in the computer search for new Wolstenholme primes.

By the same method used in the proof of (1) we can show that for all primes $p \ge 7$,

$$\binom{2p-1}{p-1} \equiv 1 - p^2 \sum_{k=1}^{p-1} \frac{1}{k^2} \pmod{p^5}.$$

Thus we can determine if p is a Wolstenholme prime by summing reciprocal squares modulo p^2. Ernst Jacobsthal [2, p. 53] proved a more general congruence that simplifies with $m = 2$ and $n = 1$ to the congruence

$$\binom{2p-1}{p-1} \equiv 1 - 2p^2 \sum_{k=1}^{(p-1)/2} \frac{1}{k^2} - 2p^3 \sum_{k=1}^{(p-1)/2} \frac{1}{k^3} \pmod{p^5}$$

for all primes $p \geq 7$. For computational purposes this is not much better. Our computations would be much easier if we can work modulo p rather than modulo p^2. Using the Bernoulli numbers B_k defined by the generating function

$$\frac{x}{e^x - 1} = \sum_{k=0}^{\infty} B_k \frac{x^k}{k!}$$

we obtain a congruence very useful for computational purposes.

THEOREM 2. *For all primes* $p \geq 11$,

$$\binom{2p-1}{p-1} \equiv 1 - \frac{2}{3}p^3 B_{p-3} \equiv 1 - \frac{2}{63}p^3 \sum_{k=[p/6]+1}^{[p/4]} \frac{1}{k^3} \pmod{p^4}.$$

Proof. The first congruence is a special case of Glaisher's congruence ([7, p. 21], [8, p. 323])

$$\binom{hp-1}{p-1} \equiv 1 - \frac{1}{3}h(h-1)p^3 B_{p-3} \pmod{p^4}, \qquad h \geq 1.$$

Stafford and Vandiver [24] proved that

$$(4^{p-2k} + 3^{p-2k} - 6^{p-2k} - 1)\frac{B_{2k}}{4k} \equiv \sum_{j=[p/6]+1}^{[p/4]} j^{2k-1} \pmod{p}, \qquad 1 \leq k \leq (p-3)/2.$$

Setting $2k = p - 3$ and applying Fermat's Little Theorem we get for primes $p \geq 11$,

$$B_{p-3} \equiv \frac{1}{21} \sum_{j=[p/6]+1}^{[p/4]} \frac{1}{j^3} \pmod{p}.$$

Substituting this into the first congruence completes the proof of the theorem. ∎

There are many congruences similar to those above involving sums of like powers of numbers in arithmetic progression and Bernoulli numbers modulo prime powers. For an excellent source we refer the reader to a paper by Emma Lehmer [15].

COROLLARY. *For all primes* $p \geq 11$ *the following are equivalent*:

(i) p *is a Wolstenholme prime*,
(ii) p *divides the numerator of* B_{p-3}, *and*
(iii)

$$\sum_{k=[p/6]+1}^{[p/4]} \frac{1}{k^3} \equiv 0 \pmod{p}.$$

Condition (ii) appears in a criterion concerning Fermat's Last Theorem. A prime p is *regular* if and only if p does not divide the numerators of the Bernoulli numbers $B_2, B_4, \ldots, B_{p-3}$. For all such primes Fermat's Last Theorem is true (see [6, p. 244] and [22, p. 10]). This does not imply, of course, that Fermat's Last Theorem is false for irregular primes, but only that more powerful techniques are required. This is one of the main reasons for the search of irregular primes. J. Buhler, R. Crandall, R. Ernvall, and T. Metsänkylä [3] calculated all irregular primes up to 4×10^6 by evaluating sums of like powers of numbers in arithmetic progression and using congruences similar to the above congruence of Stafford and Vandiver.

The Wolstenholme primes are those irregular primes where p divides the numerator of B_{p-3}. Using the congruence in condition (iii) above we found only two Wolstenholme primes $< 2 \times 10^8$, namely, 16843 and 2124679. The first was found (though not explicitly reported) by Selfridge and Pollak (Notices Amer. Math. Soc. 11 (1964), 97), and later confirmed by W. Johnson [10] and S. S. Wagstaff (Notices Amer. Math. Soc. 23 (1976), A-53). The second was found by J. Buhler, R. Crandall, R. Ernvall, and T. Metsänkylä [3], and later, independently, by the author.

We conjecture that there are infinitely many Wolstenholme primes and provide the following heuristic argument. For each prime $p \geq 5$ define the Wolstenholme quotient W_p by

$$W_p = \frac{\binom{2p-1}{p-1} - 1}{p^3}.$$

Thus p is a Wolstenholme prime if and only if $W_p \equiv 0 \pmod{p}$. As numerical evidence suggests, we assume that the remainder modulo p of W_p is random. It follows from the prime number theorem that the number of Wolstenholme primes $\leq x$ is about $\ln(\ln x)$, which grows very slowly to infinity (see [23, p. 333]). A similar argument suggests that there are at most finitely many primes p satisfying

$$\binom{2p-1}{p-1} \equiv 1 \pmod{p^5}.$$

We conjecture that there are none. Observe that if p is prime and $n = p^2$ satisfies

$$\binom{2n-1}{n-1} \equiv 1 \pmod{n^3}$$

(a counterexample to the converse of Wolstenholme's Theorem), then by (1) and (2), p must satisfy

$$\binom{2p-1}{p-1} \equiv 1 \pmod{p^6},$$

a rather unlikely event.

In view of the numerical and probabilistic evidence the converse of Wolstenholme's Theorem is undoubtedly true, but a rigorous proof has not yet been obtained.

Acknowledgements. The author is grateful to J. P. Jones for introducing him to Hilbert's tenth problem and to Peter Montgomery for several of the computer programs used in the search for new Wolstenholme primes.

References

[1] H. W. Brinkmann, *Problem E.435*, Amer. Math. Monthly 48 (1941), 269–271.

[2] V. Brun, J. Stubban, J. Fjeldstad, R. Lyche, K. Aubert, W. Ljunggren and E. Jacobsthal, *On the divisibility of the difference between two binomial coefficients*, in: Den 11te Skandinaviske Matematikerkongress, Trondheim, 1949, 42–54.

[3] J. Buhler, R. Crandall, R. Ernvall and T. Metsänkylä, *Irregular primes and cyclotomic invariants to four million*, Math. Comp. 61 (1993), 151–153.

[4] M. D. Davis, *Hilbert's tenth problem is unsolvable*, Amer. Math. Monthly 80 (1973), 233–269.

[5] L. E. Dickson, *The History of the Theory of Numbers*, Vol. 1, Chelsea, New York, 1966.

[6] H. M. Edwards, *Fermat's Last Theorem*, Springer, New York, 1977.

[7] J. W. L. Glaisher, *Congruences relating to the sums of products of the first n numbers and to other sums of products*, Quart. J. Math. 31 (1900), 1–35.

[8] —, *On the residues of the sums of products of the first $p-1$ numbers, and their powers, to modulus p^2 or p^3*, ibid., 321–353.

[9] R. K. Guy, *Unsolved Problems in Number Theory*, Springer, New York, 1981.

[10] W. Johnson, *Irregular primes and cyclotomic invariants*, Math. Comp. 29 (1975), 113–120.

[11] —, *p-adic proofs of congruences for the Bernoulli numbers*, J. Number Theory 7 (1975), 251–265.

[12] J. P. Jones, Private correspondence, January 1994.

[13] J. P. Jones and Yu. V. Matijasevič, *Proof of recursive unsolvability of Hilbert's tenth problem*, Amer. Math. Monthly 98 (1991), 689–709.

[14] E. E. Kummer, *Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen*, J. Reine Angew. Math. 44 (1852), 93–146.

[15] E. Lehmer, *On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson*, Ann. of Math. 39 (1938), 350–360.

[16] E. Lucas, *Sur les congruences des nombres eulériens et des coefficients différentiels des fonctions trigonométriques, suivant un module premier*, Bull. Soc. Math. France 6 (1878), 49–54.

[17] Yu. V. Matijasevič, *Enumerable sets are diophantine*, Dokl. Akad. Nauk SSSR 191 (1970), 279–282 (in Russian); English transl. with addendum: Soviet Math. Dokl. 11 (1970), 354–357. MR 41, #3390.

[18] —, *Primes are non-negative values of a polynomial in 10 variables*, Zap. Nauch. Sem. Leningrad. Otdel. Mat. Inst. Akad. Nauk SSSR 68 (1977), 62–82 (in Russian); English transl.: J. Soviet Math. 15 (1981), 33–44.

[19] Yu. V. Matijasevič and J. Robinson, *Reduction of an arbitrary diophantine equation to one in 13 unknowns*, Acta Arith. 27 (1975), 521–553.
[20] R. J. McIntosh, *A generalization of a congruential property of Lucas*, Amer. Math. Monthly 99 (1992), 231–238.
[21] —, *Congruences identifying the primes*, Crux Mathematicorum 20 (1994), 33–35.
[22] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer, New York, 1979.
[23] —, *The Book of Prime Number Records*, 2nd ed., Springer, New York, 1989.
[24] E. T. Stafford and H. S. Vandiver, *Determination of some properly irregular cyclotomic fields*, Proc. Nat. Acad. Sci. U.S.A. 16 (1930), 139–150.
[25] J. W. Tanner and S. S. Wagstaff, Jr., *New congruences for the Bernoulli numbers*, Math. Comp. 48 (1987), 341–350.

DEPARTMENT OF MATHEMATICS AND STATISTICS
UNIVERSITY OF REGINA
REGINA, SASKATCHEWAN
CANADA S4S 0A2
E-mail: MCINTOSH@NINJA.MATH.UREGINA.CA

Received on 21.3.1994
and in revised form on 2.12.1994 (2580)