ANNALS OF MATHEMATICS
Vol. 39, No. 2, April, 1938

ON CONGRUENCES INVOLVING BERNOULLI NUMBERS AND THE QUOTIENTS OF FERMAT AND WILSON

BY EMMA LEHMER

(Received December 1, 1937)

In this paper we give the residues of Bernoulli numbers modulo p^2 in terms of sums of like powers of numbers in arithmetical progression. It will be seen that the results obtained are as simple as those given for the residues of Bernoulli numbers modulo p by Glaisher[1] and later by an entirely different method by Vandiver.[2] We shall follow here the method of Glaisher which depends on Bernoulli polynomials of fractional arguments, rather than that of Vandiver, although both methods are capable of producing the results given below. We will apply these results to congruences involving Fermat's and Wilson's quotients, and generalize some results obtained by Friedmann and Tamarkin, Mirimanoff, Lerch, and Vandiver. We express Wilson's quotient modulo p in terms of $(p-2)^{\text{nd}}$ powers of numbers in arithmetical progression, and give some criteria for the divisibility of the Fermat's quotients q_2 and q_3 by p^2, and also some criteria for the 1st case of Fermat's Last Theorem, in terms of sums of reciprocals of numbers in arithmetical progression, and in terms of certain binomial coefficients.

We define the Bernoulli polynomial $B_\nu(x)$ by

$$B_\nu(x) = \sum_{r=0}^{\nu} \binom{\nu}{r} B_r x^{\nu-r}, \tag{1}$$

where, in turn, B_r are the Bernoulli numbers defined by

$$B_0 = 1, \quad B_1 = -\tfrac{1}{2}, \quad B_2 = \tfrac{1}{6}, \quad B_{2k+1} = 0 \text{ for } k > 0,$$

$$B_r = \sum_{i=0}^{r} \binom{r}{i} B_i.$$

If in the familiar difference equation

$$B_{\nu+1}(x+1) - B_{\nu+1}(x) = (\nu+1)x^\nu,$$

we let $x = (p - rn)/n$, $\left(r = 1, 2, \cdots, \left[\frac{p}{n}\right]\right)$,[3] where n and p are integers and $n < p$, and add all the resulting equations, we obtain after cancellation

$$\sum_{r=0}^{[p/n]} (p - rn)^\nu = \frac{n^\nu}{\nu+1}\left\{B_{\nu+1}\left(\frac{p}{n}\right) - B_{\nu+1}\left(\frac{s}{n}\right)\right\}, \tag{2}$$

[1] Quarterly Journal of Mathematics, v. 32, pp. 271–305, (1901).
[2] Proceedings Nat. Acad of Sci. v. 16, pp. 139–144, (1930).
[3] Here $[u]$ denotes as usual, the greatest integer not exceeding u.

where we have written s for the least positive residue of p modulo n. Setting $\nu = 2k$, and $x = p/n$, where p is an odd prime $> n$, in (1) we get the congruence

$$B_{2k}\left(\frac{p}{n}\right) \equiv B_{2k} + \frac{p^2}{n^2}\binom{2k}{2} B_{2k-2} \pmod{p^3}, \tag{3}$$

since $B_{2k-3} = 0$, and all the other terms are multiples of p^4 by a Bernoulli number, and therefore, by the von Staudt-Clausen theorem, are at least multiples of p^3. By the same theorem B_{2k-2} will contain p in the denominator only when $2k - 2$ is divisible by $(p - 1)$. It follows therefore that

$$B_{2k}\left(\frac{p}{n}\right) \equiv B_{2k} \pmod{p^2} \quad 2k \not\equiv 2 \pmod{p-1}. \tag{4}$$

Similarily we find for $\nu = 2k + 1$

$$B_{2k+1}\left(\frac{p}{n}\right) \equiv p\,\frac{2k+1}{n}\,B_{2k} \pmod{p^3} \quad 2k \not\equiv 2 \pmod{p-1}. \tag{5}$$

Substituting these results in (2), we obtain the following congruences

$$\sum_{r=1}^{[p/n]} (p - rn)^{2k-1} \equiv \frac{n^{2k-1}}{2k}\left\{B_{2k} - B_{2k}\left(\frac{s}{n}\right)\right\} \pmod{p^2}, \tag{6}$$

and

$$\sum_{r=1}^{[p/n]} (p - rn)^{2k} \equiv \frac{n^{2k}}{2k+1}\left\{\frac{2k+1}{n}\,pB_{2k} - B_{2k+1}\left(\frac{s}{n}\right)\right\} \pmod{p^3}, \tag{7}$$

where s is the least positive residue of $p \pmod{n}$, and $2k \not\equiv 2 \pmod{p-1}$.

Since

$$\sum_{r=1}^{[p/n]} (p - nr)^{\nu} \equiv (-1)^{\nu}\left\{n^{\nu}\sum_{r=1}^{[p/n]} r^{\nu} - p\nu n^{\nu-1}\sum_{r=1}^{[p/n]} r^{\nu-1}\right\} \pmod{p^2},$$

congruences (6) and (7) may be combined to give sums of like powers of numbers less than $[p/n]$. We can write

$$\sum_{r=1}^{[p/n]} r^{2k-1} \equiv \frac{1}{2k}\left\{B_{2k}\left(\frac{s}{n}\right) - B_{2k}\right\} - \frac{p}{n}\,B_{2k-1}\left(\frac{s}{n}\right) \pmod{p^2}, \tag{8}$$

and

$$\sum_{r=1}^{[p/n]} r^{2k} \equiv -\frac{B_{2k+1}\left(\frac{s}{n}\right)}{2k+1} + \frac{p}{n}\,B_{2k}\left(\frac{s}{n}\right) \pmod{p^2}. \tag{9}$$

Formulas (6) and (7) may be thought of as generalizations of Glaisher's results, while formulas (8) and (9) give generalizations of Vandiver's results whenever possible. Both sets of formulas depend on the evaluation of $B_{\nu}\left(\frac{s}{n}\right)$. This

evaluation has been effected in terms of Bernoulli numbers for ν even and $n = 1, 2, 3, 4$, and 6, while for ν odd, $B_\nu\left(\frac{s}{n}\right) = 0$ for $n = 1$ and 2, and is given in terms of Eulerian numbers for $n = 4$. In case $n = 3$ and 6, $B_\nu\left(\frac{s}{n}\right)$ is given in terms of what Glaisher calls I numbers,[4] but we shall not consider these cases here. Obviously both sets of formulas are equivalent modulo p. With respect to the modulus p^2 however the form (6) is superior to (8), since for $n > 2$, (8) involves a value of a Bernoulli polynomial not expressible in Bernoulli numbers. In case $n = 4$, both (7) and (9) give residues of Eulerian numbers. The values of $B_\nu\left(\frac{s}{n}\right)$ can be tabulated as follows.

$$B_\nu(1) = B_\nu, \quad \nu > 1.$$

$$B_\nu\left(\frac{1}{2}\right) = (1 - 2^{\nu-1})\frac{B_\nu}{2^{\nu-1}}, \quad \nu \text{ even}; \qquad B_\nu\left(\frac{1}{2}\right) = 0, \quad \nu \text{ odd}.$$

$$B_\nu\left(\frac{1}{3}\right) = B_\nu\left(\frac{2}{3}\right) = (1 - 3^{\nu-1})\frac{B_\nu}{2\cdot 3^{\nu-1}}, \quad \nu \text{ even}.$$

$$B_\nu\left(\frac{1}{4}\right) = B_\nu\left(\frac{3}{4}\right) = (1 - 2^{\nu-1})\frac{B_\nu}{2^{2\nu-1}}, \quad \nu \text{ even}.$$

$$B_\nu\left(\frac{1}{4}\right) = -B_\nu\left(\frac{3}{4}\right) = -\frac{\nu E_{\nu-1}}{4^\nu}, \quad \nu \text{ odd}.$$

$$B_\nu\left(\frac{1}{6}\right) = B_\nu\left(\frac{5}{6}\right) = (1 - 2^{\nu-1})(1 - 3^{\nu-1})\frac{B_\nu}{2^\nu\cdot 3^{\nu-1}}, \quad \nu \text{ even}.$$

These evaluations of $B_\nu\left(\frac{s}{n}\right)$ are well known.[5] Substituting these values in (6) we get at once for[6] $2k \not\equiv 2 \pmod{p-1}$

$$(10) \quad \sum_{r=1}^{p-1/2} (p - 2r)^{2k-1} \equiv (2^{2k} - 1)\frac{B_{2k}}{2k} \pmod{p^2},$$

$$(11) \quad \sum_{r=1}^{[p/3]} (p - 3r)^{2k-1} \equiv (3^{2k} - 1)\frac{B_{2k}}{4k} \pmod{p^2}, \quad p > 3,$$

$$(12) \quad \sum_{r=1}^{[p/4]} (p - 4r)^{2k-1} \equiv (2^{2k} - 1)(2^{2k-1} + 1)\frac{B_{2k}}{4k} \pmod{p^2}, \quad p > 3,$$

$$(13) \quad \sum_{r=1}^{[p/6]} (p - 6r)^{2k-1} \equiv (6^{2k-1} + 3^{2k-1} + 2^{2k-1} - 1)\frac{B_{2k}}{4k} \pmod{p^2}, \quad p > 5.$$

---

[4] Quarterly Jour. v. 28, p. 157.

[5] See for example N. E. Norlund, *Differenzenrechnung*, Berlin 1924, pp. 22 and 29. $B_\nu\left(\frac{s}{n}\right)$ has not been evaluated for any other values of n. The values 1, 2, 3, 4, and 6 can be characterized by the fact that their totient does not exceed two. It would be of interest to attempt the evaluation of $B_\nu\left(\frac{s}{n}\right)$ when the quotient of n is 4. Namely for $n = 5$, 8, 10 and 12.

[6] In the exceptional case $2k \equiv 2 \pmod{p-1}$ the congruences are true modulo p.

These results reduce modulo p to the congruences given by Glaisher for sums of negative powers of numbers in arithmetical progression, since for a prime to p

$$a^{-\nu} \equiv a^{p-\nu-1} \pmod{p}$$

by Fermat's theorem. Modulo p^2 however,

$$a^{-\nu} \equiv 2a^{p-\nu-1} - a^{2p-\nu-2} \pmod{p^2},$$

so that sums of negative odd powers of numbers in arithmetical progression can be obtained from the congruences (10) to (13) as a linear combination of two Bernoulli numbers whose subscripts differ by $(p-1)$. As these formulas do not simplify in general we shall not take space to write them down. We shall return later to the special case of sums of reciprocals in arithmetical progression.

First we will give the results of substituting $B_\nu\left(\frac{s}{n}\right)$ in (8) and (9) for $n = 1$, 2, and 4.

If $n = 1$, (8) and (9) are of course the same as (6) and (7). Moreover since $B_{2k}(1) = B_{2k}$ and $B_{2k+1}(1) = 0$, it follows that

$$\sum_{r=1}^{p-1} r^{2k+1} \equiv 0 \pmod{p^2}.$$

But we may go a step further and use (3) instead of (4) in (2) obtaining, $k > 0$

$$\sum_{r=1}^{p-1} r^{2k+1} \equiv p^2 \frac{2k+1}{2} B_{2k} \pmod{p^3}, \quad 2k \not\equiv 2 \pmod{p-1}, \tag{14}$$

while from (7)

$$\sum_{r=1}^{p-1} r^{2k} \equiv pB_{2k} \pmod{p^3}, \quad 2k \not\equiv 2 \pmod{p-1}. \tag{15}$$

This pair of congruences is a generalization of the familiar statement

$$\sum_{r=1}^{p-1} r^{\nu} \equiv pB_\nu \pmod{p^2}, \quad \nu \not\equiv 1 \pmod{p-1}. \tag{16}$$

In passing we remark that from these congruences we may also calculate sums of negative powers and get[7]

$$\sum_{r=1}^{p-1} 1/r^{2k} \equiv p(2k/2k+1)B_{p-1-2k} \pmod{p^2}$$

and

$$\sum_{r=1}^{p-1} 1/r^{2k-1} \equiv p^2 k[(1-2k)/(1+2k)]B_{p-1-2k} \pmod{p^3}, \quad 2k \not\equiv p-2 \pmod{p-1},$$

[7] See also Glaisher, Quar. Jour. v. 31, p. 231, (1900).

If $n = 2$, (8) becomes

$$(17) \qquad \sum_{r=1}^{(p-1)/2} r^{2k-1} \equiv (1 - 2^{2k}) \frac{B_{2k}}{2^{2k} k} \pmod{p^2}, \quad 2k \not\equiv 2 \pmod{p-1},$$

a result given by Mirimanoff.[8] Since $B_{2k+1}(\frac{1}{2}) = 0$, (9) can easily be shown to be true modulo p^3 so that

$$(18) \qquad \sum_{r=1}^{(p-1)/2} r^{2k} \equiv p(1 - 2^{2k-1}) \frac{B_{2k}}{2^{2k}} \pmod{p^3}, \quad 2k \not\equiv 2 \pmod{p-1},$$

while (7) gives

$$(19) \qquad \sum_{r=1}^{(p-1)/2} (p - 2r)^{2k} \equiv p 2^{2k-1} B_{2k} \pmod{p^3}, \quad 2k \not\equiv 2 \pmod{p-1}.$$

To obtain residues of Eulerian numbers modulo p^3, we may use (7) which gives for $2k \not\equiv 2 \pmod{p-1}$

$$(20) \qquad \sum_{r=1}^{[p/4]} (p - 4r)^{2k} \equiv (-1)^{(p-1)/2} \frac{E_{2k}}{4} + p 4^{2k-1} B_{2k} \pmod{p^3}.$$

This congruence can be combined with (19) to eliminate the Bernoulli number. Modulo p, (20) reduces to the expression given by Glaisher for E_{2k}. In the exceptional case $2k \equiv 2 \pmod{p-1}$ all the congruences given above modulo p^α, hold modulo $p^{\alpha-1}$ as can be seen from (4) and (5).

We shall now pause in our discussion to recall some of the fundamental properties of Fermat's quotient

$$(21) \qquad q_a = (a^{p-1} - 1)/p$$

and Wilson's quotient

$$(22) \qquad w_p = [(p-1)! + 1]/p.$$

It follows readily from the fundamental congruence

$$q_{ab} \equiv q_a + q_b \pmod{p}$$

that Fermat's and Wilson's quotients are connected by the relation

$$(23) \qquad \sum_{a=1}^{p-1} q_a \equiv w_p \pmod{p}.$$

If we now write (16) with $\nu = t(p-1)$ we obtain, since

$$r^{t(p-1)} \equiv 1 + ptq_r \pmod{p^2},$$

the relation

$$(24) \qquad p - 1 + ptw_p \equiv pB_{t(p-1)} \pmod{p^2},$$

[8] Jour. fur. Math., v. 115 pp. 295-300, (1895). In a recent paper, L'Enseignement Math. v. 36, pp. 228-235, (1937), Mirimanoff points out some errors is this paper.

a congruence which is usually given with $t = 1$. We will use it here with $t = 1$ and 2 to obtain by subtraction

$$w_p = B_{2(p-1)} - B_{p-1} \pmod{p} \tag{25}$$

a result which will be of use later. As a complementary result when $\nu \not\equiv 0 \pmod{p-1}$ we will need the following well know congruence[9]

$$\frac{B_{\nu+p-1}}{\nu+p-1} \equiv \frac{B_\nu}{\nu} \pmod{p}, \quad \nu \not\equiv 0 \pmod{p-1}. \tag{26}$$

We are now in a position to transform the sums (10) to (20) into sums involving Fermat's quotients by means of the relation

$$a^{\nu+p-1} - a^\nu = pa^\nu q_a .$$

To begin with, (14) becomes

$$\begin{aligned} \sum_{r=1}^{p-1} r^{2k+1} q_r &\equiv p(2kB_{2k+p-1} - (2k+1)B_{2k})/2 \\ &\equiv -pB_{2k} \pmod{p^2} \quad 2k \not\equiv 0, 2 \pmod{p-1} \end{aligned} \tag{27}$$

by (26); while (15) gives

$$\sum_{r=1}^{p-1} r^{2k} q_r = B_{2k+p-1} - B_{2k} \pmod{p^2}. \tag{28}$$

Congruences (27) and (28) generalize the following congruence

$$\sum_{r=1}^{p-1} r^\nu q_r \equiv \begin{cases} -B_\nu/\nu \pmod{p} & \nu \not\equiv 0 \pmod{p-1} \\ w_p & \nu \equiv 0 \pmod{p-1}, \end{cases}$$

obtained by Friedmann and Tamarkin[10] from the consideration of sums of greatest integers. (27) is also given by Nielsen.[11] Similarly we may obtain from (17), if $2k \not\equiv 0, 2 \pmod{p-1}$

$$\sum_{r=1}^{(p-1)/2} r^{2k-1} q_r \equiv \frac{1-2^{2k}}{2^{2k-1}} \left(\frac{B_{2k+p-1}}{2k+p-1} - \frac{B_{2k}}{2k} \right) \Big/ p - q_2 \frac{B_{2k}}{2^{2k} k} \pmod{p}. \tag{29}$$

This congruence was given by Mirimanoff[12] in the special case when B_{2k} is divisible by p. It might be of interest to notice that if $2^{2k} - 1$ is divisible by p, then

$$\sum_{r=1}^{(p-1)/2} r^{2k-1} q_r \equiv -q_2 \frac{B_{2k}}{k} \pmod{p}.$$

---

[9] See for example Bachmann, *Niedere Zahlentheorie* v. 2, p. 41.

[10] Crelle v. 137, p. 148, (1909).

[11] *Traité Elémentaire des Nombres de Bernoulli*, p. 368, Paris, 1923.

[12] Loc. cit.

Similar results may be written down for the remaining congruences, but we will confine ourselves from now on to the special cases of sums of $(p-2)^{nd}$ powers of numbers in arithmetical progression, which will give us residues of Wilson's quotient, and to sums of reciprocals which will lead to some criteria for the first case of Fermat's Last Theorem.

For $2k = p - 1$, congruences (10) to (13) simplify by means of (24) written in the form

$$\frac{pB_{p-1}}{p-1} \equiv 1 + \frac{pw_p}{p-1} \equiv 1 - pw_p \pmod{p^2},$$

and we get

$$\sum_{r=1}^{(p-1)/2} (p-2r)^{p-2} \equiv q_2(1 - pw_p) \pmod{p^2}, \tag{30}$$

$$\sum_{r=1}^{[p/3]} (p-3r)^{p-2} \equiv q_3(1 - pw_p)/2 \pmod{p^2}, \tag{31}$$

$$\sum_{r=1}^{[p/4]} (p-4r)^{p-2} \equiv \{3q_2(1 - pw_p) + pq_2^2\}/4 \pmod{p^2}, \tag{32}$$

$$\sum_{r=1}^{[p/6]} (p-6r)^{p-2} \equiv \{(4q_2 + 3q_3)(1 - pw_p) + pq_2q_3\}/12 \pmod{p^2}, \tag{33}$$

while from (17)

$$\sum_{r=1}^{(p-1)/2} r^{p-2} \equiv -2q_2(1 - pw_p) + 2pq_2^2 \pmod{p^2}. \tag{34}$$

All these congruences (30) to (34) could be used for the calculation of the remainder of w_p modulo p. Congruence (33), having of course the least number of terms, is the most practical one to use. We would write (33) in the form

$$pw_p(3q_3 + 4q_2) \equiv -12 \sum_{r=1}^{[(p-1)/6]} (p-6r)^{p-2} + (3q_3 + 4q_2 + pq_2q_3) \pmod{p^2}. \tag{35}$$

For $p = 17$ for example $q_2 \equiv 98$, $q_3 \equiv 231$ (Mod 289), and there are only two terms in the sum, $5^{15} \equiv 41$ and $11^{15} \equiv 14 \pmod{289}$. Hence we have

$$14 \cdot 17\, w_{17} \equiv -12\,(41 + 14) + (115 + 103 + 17 \cdot 130) \pmod{289}$$

$$\equiv 2 \cdot 17 \pmod{289}$$

or

$$w_{17} \equiv 1/7 \equiv 5 \pmod{17}.$$

A formula equivalent to a combination of (12) and (13) modulo p was actually used by Vandiver for the calculations of the residues of Bernoulli numbers modulo p for $p < 600$ in his investigation of irregular primes in connection with Fermat's Last Theorem. In our case, however, it is debatable whether (34) is more practical for the calculation of the remainders of w_p modulo p for large values of p, than the factorial definition of w_p. w_p has been computed modulo p by Beeger[13] for $p < 300$ from the factorial definition, and for $p < 211$ by the author,[14] using (24), and the recently extended table of Bernoulli numbers.[15] The errors in Beeger's table were given later.[16] These tables show that for $p < 300$, $w_p \equiv 0 \pmod{p}$ only for $p = 5$ and 13. The above formulas give criteria for the divisibility of w_p by p in terms of q_2 and q_3 and sums of $(p-2)^{nd}$ powers, but do not throw any light on the problem of finding a $p > 13$ for which $w_p \equiv 0 \pmod{p}$. A set of congruences similar to (30)–(34) could be written down for $2k = 2(p-1)$, or in fact more generally for $2k = t(p-1)$, and since $a^{2(p-1)} - a^{p-1} = pq_a$ we obtain a set of congruences for w_p in terms of q's whose subscripts are in arithmetical progression.

$$\sum_{r=1}^{(p-1)/2} \frac{1}{r} q_{p-2r} \equiv 2q_2 w_p - q_2^2 \pmod{p}. \tag{36}$$

$$\sum_{r=1}^{[p/3]} \frac{1}{r} q_{p-3r} \equiv \frac{3}{2} q_3 w_p - \frac{3}{4} q_3^2 \pmod{p}, \quad p > 3. \tag{37}$$

$$\sum_{r=1}^{[p/4]} \frac{1}{r} q_{p-4r} \equiv 3q_2 w_p - \frac{5}{2} q_2^2 \pmod{p}, \quad p > 3. \tag{38}$$

$$\sum_{r=1}^{[p/6]} \frac{1}{r} q_{p-6r} \equiv \left(2q_2 + \frac{3}{2} q_3\right) w_p - \left(q_2^2 + \frac{3}{4} q_3^2 + \frac{1}{2} q_2 q_3\right) \pmod{p}, \quad p > 5. \tag{39}$$

and

$$\sum_{r=1}^{(p-1)/2} \frac{1}{r} q_r \equiv 2q_2 w_p + q_2^2 \pmod{p}. \tag{40}$$

Formula (39) might seem at first sight preferable to (34) for the calculation of w_p since it involves the same number of terms and gives w_p modulo p directly rather than pw_p modulo p^2. The calculation of q_a however involves the calculation of a^{p-1} modulo p^2 so there is really no saving of time or labor, but instead a loss of a valuable check modulo p which (34) affords.

We now return to the sums of reciprocals of numbers in arithmetical progression. These can be now obtained by subtracting the corresponding for-

---

[13] Mess. of Math. v. 49, pp. 177–8, (1920).
[14] Amer. Math. Monthly, v. 44, pp. 237–8, (1937).
[15] Duke Jour. v. 2, pp. 462–4, (1936).
[16] Amer. Math. Monthly, v. 44, p. 462, (1937).

mulas in the sets (30) to (34) and (36) to (40) since $\frac{1}{a} = a^{p-2} - p\frac{q_a}{a}$. In this way we obtain

$$(41) \qquad \sum_{r=1}^{(p-1)/2} \frac{1}{p-2r} \equiv q_2 - pq_2^2/2 \pmod{p^2}$$

$$(42) \qquad \sum_{r=1}^{[p/3]} \frac{1}{p-3r} \equiv \frac{q_3}{2} - \frac{pq_3^2}{4} \pmod{p^2}, \quad p > 3.$$

$$(43) \qquad \sum_{r=1}^{[p/4]} \frac{1}{p-4r} \equiv \frac{3}{4}q_2 - \frac{3}{8}pq_2^2 \pmod{p^2}, \quad p > 3.$$

$$(44) \qquad \sum_{r=1}^{[p/6]} \frac{1}{p-6r} \equiv \frac{1}{4}q_3 + \frac{1}{3}q_2 - p\left(\frac{1}{8}q_3^2 + \frac{1}{6}q_2^2\right). \pmod{p^2}, \quad p > 5,$$

and

$$(45) \qquad \sum_{r=1}^{(p-1)/2} \frac{1}{r} \equiv -2q_2 + pq_2^2 \pmod{p^2}.$$

Congruences (41) and (42) were given modulo p by Lerch,[17] while (41) and (43) were obtained modulo p by Glaisher.[18] Vandiver[19] stated (41) as follows:

$$q_2 \equiv 0 \pmod{p^2} \textit{ if and only if } \sum_{a=1}^{(p-1)/2} \frac{1}{p-2a} \equiv 0 \pmod{p^2}.$$

We can combine (41) with (43) to give a slightly stronger condition:

$$q_2 \equiv 0 \pmod{p^2} \textit{ if and only if } \sum_{a=1}^{[p/4]} \frac{1}{p-4a} \equiv \sum_{a=1}^{[p/4]} \frac{1}{p-2-4a} \equiv 0 \pmod{p^2},$$

while a similar condition for $q_3 \equiv 0 \pmod{p^2}$ can be read out of (42).

It follows from (41)–(43) that the assumption $q_2 \equiv q_3 \equiv 0 \pmod{p}$ implies

$$\sum_{r=1}^{[p/n]} \frac{1}{r} \equiv 0 \pmod{p}, \quad \text{for } n = 2, 3, 4, \text{ and } 6.$$

But $q_2 \equiv 0 \pmod{p}$ and $q_3 \equiv 0 \pmod{p}$ are respectively the criteria of Wieferich and Mirimanoff for the first case of Fermat's Last Theorem. We can therefore transform a combination of these criteria as follows:

The equation

$$(46) \qquad x^p + y^p + z^p = 0$$

has no solutions in integers x, y, z prime to p unless

$$\sum_{r=1}^{[p/n]} \frac{1}{r} \equiv 0 \pmod{p}, \quad n = 2, 3, 4, \text{ and } 6.$$

---

[17] Math. Annalen, v. 60, pp. 471–490, (1905).

[18] Quarterly Jour. v. 32, pp. 1–27, (1901).

[19] Annals of Math. v. 18, pp. 112, (1917).

Vandiver[20] derived the same condition in the case $n = 5$ using Kummer's criteria. Combining the conditions for $n = 5$ and 6 for instance we can state that $\sum_{r=[p/6]+1}^{[p/5]} \frac{1}{r} \equiv 0 \pmod{p}$ is a criterion for the first case of Fermat's Last Theorem.[21]

Vandiver[22] has also proved that if (46) has a solution in integers x, y, z, prime to p, then

$$\sum_{r=1}^{[p/3]} \frac{1}{r^2} \equiv 0 \pmod{p}. \tag{47}$$

It has been shown by Schwindt,[23] and can also be made to follow from (7) with $2k = p - 3$, and $n = 3$ and 6, that

$$5 \sum_{r=1}^{[p/3]} \frac{1}{r^2} \equiv \sum_{r=1}^{[p/6]} \frac{1}{r^2} \pmod{p}$$

so that

$$\sum_{r=1}^{[p/6]} \frac{1}{r^2} \equiv 0 \pmod{p} \tag{48}$$

is also a criterion for the first case of Fermat's Last theorem. These last two criteria can be restated in terms of Glaisher's I-numbers referred to above. If it were proved that $\sum_{r=1}^{[p/4]} \frac{1}{r^2} \equiv 0 \pmod{p}$ is also a criterion for the first case of Fermat's Last Theorem, then a criterion could be given in terms of Eulerian numbers, since from (20)

$$\sum_{r=1}^{[p/4]} \frac{1}{r^2} \equiv (-1)^{(p-1)/2} 4E_{p-3} \pmod{p}.$$

It follows further since $\frac{1}{p - nr} \equiv -\frac{1}{nr} - p\frac{1}{n^2r^2} \pmod{p^2}$, that, by substituting the criteria (47) and (48) together with $q_2 \equiv q_3 \equiv 0 \pmod{p}$, into (42) and (44), we obtain

$$\sum_{r=1}^{[p/3]} \frac{1}{r} \equiv -3 \sum_{r=1}^{[p/3]} \frac{1}{p - 3r} \equiv -\frac{3}{2} q_3 \pmod{p^2}$$

and

$$\sum_{r=1}^{[p/6]} \frac{1}{r} \equiv -6 \sum_{r=1}^{[p/6]} \frac{1}{p - 6r} \equiv -\frac{3}{2} q_3 - 2q_2 \pmod{p^2},$$

---

[20] Jour. für Math. v. 144, pp. 314–318, (1914).

[21] Frobenius, Berlin Sitz. 1914, pp. 653–81, gave similar criteria in terms of

$$s_k = \Sigma\, 1/r, \qquad ((k-1)p/n < r < kp/n)$$

for $n = 7$ and $n = 12$ (p. 676). Other criteria in terms of linear combinations of s_k can be derived from his results for $n \leqq 26$.

[22] Annals of Math. v. 26, pp. 88–94, (1924).

[23] Jahrber. Deutsche Math. Ver. v. 43, pp. 229–231, (1933–4).

if Fermat's equation has a solution in integers x, y, z, prime to p. Moreover since $\sum_{r=1}^{p-1} \frac{1}{r} \equiv 0 \pmod{p^2}$,

$$\sum_{r \equiv -p \pmod 3} \frac{1}{r} \equiv 0 \pmod{p^2}$$

is also a criterion for the first case of Fermat's Last Theorem.

In conclusion we apply our congruences (41)–(45) to the problem of finding the residues modulo p^2 and p^3 of certain binomial coefficients. Since[24]

$$\binom{p-1}{k} \equiv (-1)^k \left\{1 - p\sum_{r=1}^{k} \frac{1}{r} + \frac{p^2}{2}\left(\sum_{r=1}^{k} \frac{1}{r}\right)^2 - \frac{p^2}{2}\sum_{r=1}^{k} \frac{1}{r^2}\right\} \pmod{p^3}$$

it follows from (45) that[25] for $p > 3$

$$\binom{p-1}{(p-1)/2} \equiv (-1)^{(p-1)/2}\{1 - p(-2q_2 + pq_2^2) + 2p^2q_2^2\} \pmod{p^3} \tag{49}$$

$$\equiv (-1)^{(p-1)/2}(1 + pq_2)^2 \equiv (-1)^{(p-1)/2}4^{p-1}$$

while using (41)–(44) modulo p we obtain for $p > 3$

$$\binom{p-1}{[p/3]} \equiv (-1)^{[p/3]}\left(\frac{3}{2}pq_3 + 1\right) \equiv (-1)^{[p/3]}(3^p - 1)/2 \pmod{p^2} \tag{50}$$

$$\binom{p-1}{[p/4]} \equiv (-1)^{[p/4]}(3pq_2 + 1) \equiv (-1)^{[p/4]}(3\cdot 2^{p-1} - 2) \pmod{p^2} \tag{51}$$

and for $p > 5$

$$\binom{p-1}{[p/6]} \equiv (-1)^{[p/6]}\left(2pq_2 + \frac{3}{2}pq_3 + 1\right) \equiv (-1)^{[p/6]}(2^{p+1} + 3^p - 5)/2 \pmod{p^2}. \tag{52}$$

It follows from these congruences that some of the criteria for Fermat's Last Theorem given above can be restated in terms of binomial coefficients as follows

The Fermat Equation (46) *has no solutions in integers x, y, z, prime to p unless*

$$\binom{p-1}{[p/n]} \equiv (-1)^{[p/n]} \pmod{p^2}$$

for $n = 2, 3, 4, 5,$ *and* 6.

Furthermore it follows from the criteria (47) and (48) that if Fermat's equation has a solution in integers x, y, z prime to p, then (50) and (52) are true modulo p^3.

BETHLEHEM, PA.

[24] This follows from the identity

$$\binom{p-1}{k} = (-1)^k\{(1 - pS_1 + p^2S_2 - + \cdots + (-1)^k p^k S_k)\}$$

where S_ν is the ν-th elementary symmetric function of $\left(\frac{1}{1}, \frac{1}{2}, \frac{1}{3}, \cdots, \frac{1}{k}\right)$.

[25] This is equivalent to a result given by Nielsen: K. Danske Vidensk. Selsk. Skrifter, (7), v. 10, (1913), p. 353, formula (9).