

ON SOME NEW CONGRUENCES IN THE THEORY OF BERNOULLI'S NUMBERS

N. G. W. H. BEEGER

For Bernoulli's numbers the following relations are known:

$$(h + 1)^n = h^n; \quad n > 1, \quad h_1 = -\frac{1}{2}, \quad B_n = (-1)^{n-1}h_{2n};$$

$$h_{2n+1} = 0 \text{ for } n > 0.$$

For the symbol $k^n = h^{n+1}/(n+1)$ Kummer proved the congruence

$$(1) \quad k^a(1 - k^b)^c \equiv 0 \pmod{(p^a, p^{ec})},$$

p being a prime, $b = p^{e-1}(p-1)b_1$, $a+1 \not\equiv 0 \pmod{(p-1)}$. G. Frobenius* has given another proof of this congruence, without using infinite series. I shall now prove the congruence

$$(2) \quad (-1)^{i-1}k^{a+mb} \equiv \sum_{s=1}^i (-1)^{s-1}C_{m,s-1}C_{m-s,i-s}k^{a+(s-1)b} \pmod{p^i},$$

$$b = p - 1,$$

which is equivalent to

$$(3) \quad (-1)^{i-1} \frac{B_{n+m\mu}}{2n + 2m\mu} \equiv \sum_{s=1}^i (-1)^{s-1+(m-s+1)\mu}$$

$$\cdot C_{m,s-1}C_{m-s,i-s} \frac{B_{n+(s-1)\mu}}{2n + 2(s-1)\mu} \pmod{p^i},$$

$$C_{m,0} = 1, m \geq i, i < 2n - 1, 2n \not\equiv 0 \pmod{(p-1)}, \mu = (p-1)/2.$$

Take, in (1), $b = p - 1$, $c = i$, $a = 2n - 1$; then (1) gives

$$(-1)^{i-1}k^{a+bi} \equiv \sum_{s=1}^i (-1)^{s-1}C_{i,s-1}k^{a+(s-1)b} \pmod{p^i}.$$

Hence (2) is proved for the case $m = i$. Now suppose that (2) is proved for $m = i, i+1, i+2, \dots, m$. From (1) it follows that

$$(4) \quad (-1)^m k^{a+(m+1)b} \equiv \sum_{s=1}^i (-1)^{s-1}C_{m+1,s-1}k^{a+(s-1)b}$$

$$+ \sum_{s=i+1}^{m+1} (-1)^{s-1}C_{m+1,s-1}k^{a+(s-1)b} \pmod{p^{m+1}}.$$

* Sitzungsberichte der Preussischen Akademie, vol. 39 (1910), p. 809

By substituting, for each term of the second sum in the right-hand side of (4), the series from (2), we obtain

$$\begin{aligned}
 (-1)^m k^{a+(m+1)b} &\equiv \sum_{s=1}^i (-1)^{s-1} k^{a+(s-1)b} (C_{m+1,s-1} \\
 (5) \quad &- C_{m+1,i} C_{i,s-1} C_{i-s,i-s} + C_{m+1,i+1} C_{i+1,s-1} C_{i-s+1,i-s} \\
 &- \dots \pm C_{m+1,m} C_{m,s-1} C_{m-s,i-s}) \pmod{p^i}.
 \end{aligned}$$

Let the coefficient of k^a be denoted by S_m . Then

$$\begin{aligned}
 (6) \quad S_m &= 1 - C_{m+1,i} C_{i-1,i-1} + C_{m+1,i+1} C_{i,i-1} \\
 &- \dots + (-1)^{m+i-1} C_{m+1,m} C_{m-1,i-1},
 \end{aligned}$$

and, using the known relation

$$C_{m+1,c} - C_{m,c} = C_{m,c-1},$$

we have

$$\begin{aligned}
 (7) \quad S_m - S_{m-1} &= \sum_{j=i}^{m-1} (-1)^{j-i+1} C_{m,j-1} C_{j-1,i-1} + (-1)^{m+i-1} C_{m+1,m} C_{m-1,i-1} \\
 &= C_{m,i-1} \sum_{j=i}^{m-1} (-1)^{j-i+1} C_{m-i+1,m-j+1} \\
 &+ (-1)^{m+i-1} C_{m+1,m} C_{m-1,i-1} \\
 &= (-1)^{m-i+1} (C_{m,i-1} + C_{m-1,i-1}).
 \end{aligned}$$

From (6) it follows that $S_i = -i$; hence from (7) we have

$$\begin{aligned}
 (8) \quad S_m - S_i &= C_{i,i-1} - C_{i+1,i-1} + \dots + (-1)^{m-i+1} C_{m-1,i-1} \\
 &+ (C_{i+1,i-1} - C_{i+2,i-1} + \dots + (-1)^{m-i+1} C_{m,i-1}), \\
 S_m &= (-1)^{m-i+1} C_{m,i-1}.
 \end{aligned}$$

Let further the coefficient of k^{a+ib} in the second member of (5) be denoted by S'_m ; then

$$\begin{aligned}
 S'_m &= C_{m+1,j} - C_{m+1,j} C_{i,j} C_{i-j-1,i-j-1} + \dots \pm C_{m+1,m} C_{m,j} C_{m-j-1,i-j-1} \\
 &= C_{m+1,j} (1 - C_{m-j+1,i-j} C_{i-j-1,i-j-1} + C_{m-j+1,i-j+1} C_{i-j,i-j-1} \\
 &- \dots \pm C_{m-j+1,m-j} C_{m-j-1,i-j-1});
 \end{aligned}$$

hence

$$S'_m = C_{m+1,j} S_{m-j} = C_{m+1,j} C_{m-j,i-j-1} (-1)^{m-i+1}$$

by (8). From (5) the congruence (2) is now proved for $(m+1)$; hence (2) is true in general for all numbers $m = i, i+1, \dots$.

In order to get a congruence analogous to (2) and (3), but for a modulus which is a higher power of p than p^a , take, in (2), $a + jb$ in place of a , and replace $(m + j)$ by m . We have

$$(9) \quad (-1)^{i-1} k^{a+mb} \equiv \sum_{s=1}^i (-1)^{s-1} C_{m-j, s-1} C_{m-j-s, i-s} k^{a+(s+j-1)b} \pmod{p^i},$$

$$m \geq i + j, i \leq a + jb, a + 1 \not\equiv 0 \pmod{p - 1},$$

with the equivalent relation

$$(10) \quad (-1)^{i-1} \frac{B_{n+m\mu}}{2n+2m\mu} \equiv \sum_{s=1}^i (-1)^{s-1+(m-s+1)\mu}$$

$$\cdot C_{m-j, s-1} C_{m-j-s, i-s} \frac{B_{n+(s+j-1)\mu}}{2n+2\mu(s+j-1)} \pmod{p^i},$$

$$m \geq i + j, i \leq 2n - 1 + j(p - 1), 2n \not\equiv 0 \pmod{p - 1}.$$

A prime $p > 3$ is said to be irregular if it divides one of the numbers $B_1, B_2, \dots, B_{\mu-1}$, say B_n . It is known by (1) that in this case each number $B_{n+m\mu}$ is divisible by p .

THEOREM. *If p is an irregular prime, and if $k^a \equiv 0 \pmod{p}$, then for each number i the positive integers $m_1, m_2, \dots, m_{i-1} < p$, can be determined uniquely by the chain of congruences*

$$k^a \equiv m_1 P \pmod{p^2},$$

$$k^{a+m_1 b} \equiv m_2 p P \pmod{p^3},$$

$$k^{a+(m_1+m_2 p)b} \equiv m_3 p^2 P \pmod{p^4},$$

$$\dots,$$

$$k^{a+(m_1+m_2 p+\dots+m_{i-2} p^{i-3})b} \equiv m_{i-1} p^{i-2} P \pmod{p^i},$$

provided that

$$P = k^a - k^{a+b} \not\equiv 0 \pmod{p^2};$$

consequently

$$k^{a+(m_1+m_2 p+\dots+m_{i-1} p^{i-2})b} \equiv 0 \pmod{p^i}.$$

In the above k is defined as at the beginning of the article, and $b = p - 1$.

PROOF. In the congruence (2) take $i = 2$; this gives

$$(11) \quad -k^{a+mb} \equiv (m - 1)k^a - m k^{a+b} \pmod{p^2},$$

$$k^{a+mb} \equiv k^a - m(k^a - k^{a+b}) \pmod{p^2}.$$

The congruence

$$k^a - m(k^a - k^{a+b}) \equiv 0 \pmod{p^2},$$

wherein k^a and k^{a+b} are divisible by p , has one solution $m_1 < p$ if and only if $P = k^a - k^{a+b} \not\equiv 0 \pmod{p^2}$, and it follows from (11) that

$$k^{a+m_1b} \equiv 0 \pmod{p^2}.$$

Hence the theorem is proved for $i = 2$. Suppose that it is proved for $2, 3, 4, \dots, i$, and put

$$m_1 + m_2p + \dots + m_{i-2}p^{i-3} = m';$$

then $k^{a+m'b} \equiv 0 \pmod{p^i}$. Now take the congruence (9) for $(i+1)$ in place of i , which gives

$$(-1)^i k^{a+mb} \equiv \sum_{s=1}^{i+1} (-1)^{s-1} C_{m-j, s-1} C_{m-j-s, i+1-s} k^{a+(s+j-1)b} \pmod{p^{i+1}}.$$

Let the polynomial in the right-hand side be denoted by $G(m)$. Then

$$(11a) \quad G(m' + p^{i-1}x) \equiv G(m') + p^{i-1}xG'(m') \pmod{p^{i+1}};$$

also

$$G(m') \equiv (-1)^i k^{a+m'b} \pmod{p^{i+1}}$$

from the definition of G , and (2) gives, for $i = 2$,

$$G(m) = (-1)^i k^{a+mb} \equiv (-1)^{i-1} \{ (m-1)k^a - mk^{a+b} \} \pmod{p^2};$$

hence

$$G'(m) \equiv (-1)^{i-1} \{ k^a - k^{a+b} \} \pmod{p^2},$$

and setting $m = m'$ in this relation, we get from (11a)

$$G(m' + p^{i-1}x) \equiv (-1)^i k^{a+m'b} + (-1)^{i-1} p^{i-1} x (k^a - k^{a+b}) \pmod{p^{i+1}},$$

and hence

$$(-1)^i k^{a+(m'+p^{i-1}x)b} \equiv (-1)^i k^{a+m'b} + (-1)^{i-1} p^{i-1} x (k^a - k^{a+b}) \pmod{p^{i+1}}.$$

Now $k^{a+m'b} \equiv 0 \pmod{p^i}$. The congruence

$$k^{a+m'b} - p^{i-1}x(k^a - k^{a+b}) \equiv 0 \pmod{p^{i+1}}$$

has therefore one solution $x = m_i < p$ if and only if $k^a - k^{a+b} \not\equiv 0 \pmod{p^2}$, and then $k^{a+(m'+p^{i-1}m_i)b} \equiv 0 \pmod{p^{i+1}}$. The theorem is proved for $(i+1)$ and hence is true for all values of i .

It follows immediately from this theorem that for each number i , as large as we please, the numbers m_1, m_2, \dots, m_{i-1} can be deter-

mined so that if $B_n \equiv 0 \pmod{p}$, $n < p$, p an irregular prime, then

$$B_{n+(m_1+m_2p+\dots+m_{i-1}p^{i-2})\mu} \equiv 0 \pmod{p^i},$$

if

$$\frac{B_n}{2n} \not\equiv (-1)^{(p-1)/2} \frac{B_{n+(p-1)/2}}{2n+p-1}.$$

Pollaczek* calculated, in the cases $n = 16, p = 37; n = 22, p = 59;$ and $n = 29, p = 67$, the number m_1 for which $B_{n+m_1\mu} \equiv 0 \pmod{p^2}$. His calculations gave me the idea to construct my congruences (3) and (10) and to formulate the theorem.

The substitution of $m = 2n$ in (3) gives the result

$$(12) \quad (-1)^{i-1} \frac{B_{np}}{np} \equiv \sum_{s=1}^i (-1)^{(s-1)(\mu+1)} C_{2n,s-1} C_{2n-s,i-s} \cdot \frac{B_{n+(s-1)\mu}}{2n+2(s-1)\mu} \pmod{p^i}, \quad 2n \not\equiv 0 \pmod{p-1}.$$

The case $i = 2$ is of special interest. H. S. Vandiver and his collaborators, in their researches about the second case of Fermat's last theorem,† have made very extensive calculations to find the residues of B_{np} , modulo p^3 , p being an irregular prime less than 211, not knowing the congruence (12). For $B_n \equiv 0 \pmod{p}$, we have $n < \mu$; then $B_{np} \equiv 0 \pmod{p^2}$, and (12) gives, for $i = 2$,

$$B_{np} \equiv -\frac{p}{2n-1} \{ (2n-1)^2 B_n - (-1)^{(p-1)/2} (2n)^2 B_{n+\mu} \} \pmod{p^3}.$$

Using the existing tables of Bernoulli's numbers we can obtain from this congruence the residue of B_{np} , modulo p^3 , after a simple calculation. Thus I have checked the results of Vandiver (except for $p = 157$ and 149; B_{133} and B_{139} not being in the tables) and have found them all correct.

AMSTERDAM, HOLLAND

* *Mathematische Zeitschrift*, vol. 21 (1924), pp. 28–31. Some of his results are wrong. They should be $B_{22} \equiv 50 \cdot 59, B_{51} \equiv 42 \cdot 59 \pmod{59^2}, B_{62} \equiv 37 \cdot 67 \pmod{67^2}$.

† *Transactions of this Society*, vol. 31 (1929), pp. 613, 639–642.