



An Arithmetical Theory of the Bernoulli Numbers

H. S. Vandiver

Transactions of the American Mathematical Society, Vol. 51, No. 3 (May, 1942),
502-531.

Stable URL:

<http://links.jstor.org/sici?sici=0002-9947%28194205%2951%3A3%3C502%3AAATOTB%3E2.0.CO%3B2-J>

Transactions of the American Mathematical Society is currently published by American Mathematical Society.

Your use of the JSTOR archive indicates your acceptance of JSTOR's Terms and Conditions of Use, available at <http://www.jstor.org/about/terms.html>. JSTOR's Terms and Conditions of Use provides, in part, that unless you have obtained prior permission, you may not download an entire issue of a journal or multiple copies of articles, and you may use content in the JSTOR archive only for your personal, non-commercial use.

Please contact the publisher regarding any further use of this work. Publisher contact information may be obtained at <http://www.jstor.org/journals/ams.html>.

Each copy of any part of a JSTOR transmission must contain the same copyright notice that appears on the screen or printed page of such transmission.

JSTOR is an independent not-for-profit organization dedicated to creating and preserving a digital archive of scholarly journals. For more information regarding JSTOR, please contact support@jstor.org.

AN ARITHMETICAL THEORY OF THE BERNOULLI NUMBERS

BY

H. S. VANDIVER

In the present paper we shall describe a method which enables us to find many new types of relations concerning the Bernoulli and allied numbers. The scheme might be described as ultra-arithmetical in character. It depends mainly on the following idea. Let a and b be rational with $a \equiv b$, modulo p , where p is any prime integer. If a and b do not depend on p , it then follows, since there is an infinity of primes, that $a = b$.

A similar method has been employed in other parts of mathematics; for example, Hasse⁽¹⁾ in a paper on algebraic geometry uses the method and comments upon the success it has had in various lines.

Perhaps the simplest looking formula in which a Bernoulli number appears alone on one side of the relation is as follows, if $S_n(p) = 1^n + \dots + (p-1)^n$,

$$\frac{S_n(p)}{p} \equiv b_n \pmod{p},$$

where $n+1 < p$, in which case, of course, the left-hand member of the congruence is an integer. In order to take advantage of this simplicity we employ extensively the function which we have called in a previous paper the Mirimanoff polynomial⁽²⁾, namely, the relation (1) which follows. This is connected with the previous congruence, if we note that

$$f_n^{(p)}(1) = S_n(p).$$

In general we employ more or less obvious identities involving one or more indeterminates, then operate thereon, using the method of formal exponential differentiation explained in another paper⁽³⁾. The elementary function from which the Mirimanoff polynomials are generated by this process is

$$\frac{x^m - 1}{x - 1}.$$

Presented to the Society, September 5, 1941; received by the editors April 5, 1941.

⁽¹⁾ *Abhandlungen Göttingen*, vol. 18 (1937), pp. 51-55; cf. also Vandiver, *Bulletin of the American Mathematical Society*, vol. 31 (1925), p. 348; in particular, the proof of II. There is a misprint in the first congruence involving H . The right-hand member should read a_c in lieu of a^c .

⁽²⁾ Vandiver, *Duke Mathematical Journal*, vol. 3 (1937), p. 570; so-called because Mirimanoff, it appears, first investigated its properties extensively in an article in *Crelle's Journal*, vol. 128 (1905), pp. 45-68.

⁽³⁾ Vandiver, *On formal exponential differentiation in rings*, *Proceedings of the National Academy of Sciences*, vol. 28 (1942), pp. 24-27.

In view of the congruence (68) below it seems to me that the theory of Mirimanoff polynomials has often been obscured by the theory of the Euler polynomials defined in (12) and (13). I think that this is unfortunate, as the Mirimanoff polynomial has a much simpler algebraic form. Each type is generalized in §2 of this paper. In (19) instead of a congruence we derive an equation involving the two types of polynomials.

If in place of the simple congruence involving $S_n(p)$ given above we employ a known congruence such as the following:

$$\frac{(n^i - 1)b_i}{i} \equiv y_a a^{i-1} \pmod{p},$$

where $y_a \equiv -a/p \pmod{n}$, we are forced to use an extension of the Mirimanoff polynomials and relations involving the number

$$\frac{(m^n - 1)b_n}{n}$$

in lieu of b_n itself. The former number has appeared in a great number of investigations concerning Bernoulli numbers, but its properties seem to be quite different in many connections; for example, I quote Frobenius as follows: “. . . die Tangentenkoeffizienten deren Theorie man in den bisherigen Darstellungen nicht scharf genug von der eigentlichen Bernoullischen Zahlen geschieden hat.”

In a previous paper⁽⁴⁾ the writer introduced the idea of Bernoulli numbers of various orders such that we call $b_n(m, k) = (mb + k)^n$, $m \neq 0$, a *generalized Bernoulli number of the first order*; and a number of the form, for $r > 1$,

$$(m_r b^{(r)} + m_{r-1} b^{(r-1)} + \dots + m_1 b' + m_0)^n = b_n(m_r, m_{r-1}, \dots, m_0),$$

where this expression is expanded in full by the multinomial theorem and b_a substituted for $b_a^{(i)}$, $i = 1, 2, \dots, r$, and where the m 's are integers, $m_i \neq 0$, a *Bernoulli number of the r th order*. This is an extension of the definition of Lucas of the ultra-Bernoulli numbers⁽⁵⁾.

Bernoulli numbers of the first order are considered in §§3 to 11 of this paper. In §5 a generalization of the von Staudt-Clausen theorem is derived which applies to Bernoulli numbers of the first order (Theorem I). In another

(4) Vandiver, Proceedings of the National Academy of Sciences, vol. 23 (1937), p. 555.

(5) Frobenius, *Berlin Sitzungsberichte*, 1910, p. 810. “Die Bezeichnung der Werte

$$(b + b')^n, \dots, (b + b^{(1)} + b^{(2)} + \dots + b^{(n)})^n,$$

als Bernoullische Zahlen höherer Ordnung oder gar als ultra-bernoullische Zahlen scheint mir wenig glücklich gewählt und mehr von abschreckender Wirkung zu sein.”

The writer differs from Frobenius regarding this. These numbers, as well as the generalizations of them considered in this paper are shown to be natural analogues of the ordinary Bernoulli numbers.

paper⁽⁶⁾ a generalization of certain congruence properties of the numerators of Bernoulli numbers is obtained which applies to the numerators of any Bernoulli number of the first order. It is noteworthy that these generalizations are very little more complicated in statement than those theorems which apply to the ordinary Bernoulli numbers.

In order to illustrate the varied applications of our method and to develop a connected theory, we give new proofs of several known theorems. In particular, although Theorem I was proved in previous papers⁽⁶⁾, we give two new proofs of the same, as the result and the material in the proofs are both important in our theory.

The properties of the Bernoulli numbers of the second order are considered in §11 to §15. It seems to me that from many standpoints this type of Bernoulli number is the most remarkable. For example, we note from Theorem III that the only prime factors occurring in the denominator of such a number, say $(kb + jb' + h)^n$, n even, are divisors of jk and are also found among the von Staudt-Clausen primes of order n . As noted in §16, this property does not carry over to Bernoulli numbers of higher order. Also (Theorem IV, Corollary I), any Bernoulli number of the above type can be expressed as a linear combination of Bernoulli numbers of the first order with coefficients whose denominators divide the integers k and j . In particular cases the equivalent of this result may be expressed in terms of the roots of unity (Theorem V). Results of an entirely new type are given in Corollary I and Corollary II to Theorem V.

Since congruence methods are employed throughout this paper, one might imagine that many new congruences concerning the Bernoulli numbers could be obtained aside from those given here. Such is indeed the case, but their statement will be reserved for other papers.

1. **Euler and Mirimanoff polynomials.** We write the Mirimanoff polynomials in the form

$$(1) \quad f_a^{(m)}(x) = 0^a + 1^a x + 2^a x^2 + \cdots + (m-1)^a x^{m-1},$$

where $0^0 = 1$.

We shall first show that, for $n > 0$,

$$(2) \quad x[(f(x) + 1)^n] \equiv f_n(x) \pmod{p},$$

where $f_i(x) = f_i^{(p)}(x)$, p is prime, and the left bracket symbol in the left-hand member signifies that the n th power of $(f(x) + 1)$ is to be taken symbolically, that is, after development by the binomial theorem the exponents are de-

⁽⁶⁾ Vandiver, *On simple explicit expressions for generalized Bernoulli numbers of the first order*, Duke Mathematical Journal, vol. 8 (1941), pp. 575-584; Carlitz, *Generalized Bernoulli and Euler numbers*, *ibid.*, pp. 586-587.

graded to subscripts and, in particular, the last term is expressed as $f_0(x)$. Also for $n=0$ any such expression is taken as unity.

Consider

$$(3) \quad x(1 + x + x^2 + \cdots + x^{p-1}) = x + x^2 + \cdots + x^p.$$

Now employ formal exponential differentiation (Vandiver⁽³⁾). Differentiating this expression n times with respect to x , we obtain

$$(4) \quad \begin{aligned} x[(f(x) + 1)^n &= x + 2^n x^2 + \cdots + (p-1)^n x^{p-1} + p^n x^p \\ &= f_n(x) + p^n x^p, \end{aligned}$$

from which (2) follows.

Now consider

$$(5) \quad x + x^2 + \cdots + x^p = (1 - x^p)x/(1 - x).$$

Differentiate this n times, where \bar{d} denotes exponential differentiation; we find

$$x + 2^n x^2 + \cdots + p^n x^p = (1 - x^p) \left[\frac{\bar{d}^n}{dx^n} \left(\frac{x}{1-x} \right) \right] + \frac{pF(x)}{(1-x)^n},$$

$$f_n(x) + p^n x^p = (1 - x^p) \left[\frac{\bar{d}^n}{dx^n} \left(\frac{x}{1-x} \right) \right] + \frac{pF(x)}{(1-x)^n},$$

or

$$(6) \quad f_n(x) = (1 - x^p) \left[\frac{\bar{d}^n}{dx^n} \left(\frac{x}{1-x} \right) \right] + p \frac{G(x)}{(1-x)^n}.$$

We then have, for $n > 0$,

$$(7) \quad f_n(x) \equiv (1 - x^p) \left[\frac{\bar{d}^n}{dx^n} \left(\frac{x}{1-x} \right) \right] \pmod{p},$$

where we write $M(x)/N(x) \equiv 0 \pmod{p}$, if $M(x)$ and $N(x)$ are polynomials in which each coefficient of $M(x)$ is divisible by p , while not all the coefficients of $N(x)$ are so divisible.

We write

$$H_n(x) = \frac{1-x}{x} \left[\frac{\bar{d}^n}{dx^n} \left(\frac{x}{1-x} \right) \right],$$

so that

$$(8) \quad f_n(x) \equiv (-1)^n \frac{(1-x^p)x}{1-x} H_n(x) \pmod{p}.$$

Now consider

$$x^{-1}(1 + x + x^2 + \cdots + x^{p-1}) = 1 + x + x^2 + \cdots + x^{p-1} - x^{p-1} + x^{-p} \cdot x^{p-1}.$$

Differentiating n times, we obtain

$$\frac{1}{x} [(f(x) - 1)^n \equiv f_n(x) + (p-1)^n x^{p-1} x^{-p} - (p-1)^n x^{p-1} \pmod{p}],$$

whence

$$(9) \quad [(f(x) - 1)^n \equiv x f_n(x) + (-1)^n (1 - x^p) \pmod{p}].$$

We now express each $f_n(x)$ in this relation in terms of $H_n(x)$ by using (8), and this gives⁽⁷⁾, modulo p ,

$$(10) \quad x \frac{1-x^p}{1-x} \left[(-H-1)^n - (-1)^n + (-1)^n \frac{1-x^p}{1-x} \right] \\ \equiv (-1)^n x^2 \frac{1-x^p}{1-x} H_n + (-1)^n (1-x^p),$$

or

$$(11) \quad (-1)^n \left[x \frac{1-x^p}{1-x} \{ [(H+1)^n - 1] + \frac{1-x^p}{1-x} \} \right] \\ \equiv (-1)^n \left[x^2 \frac{1-x^p}{1-x} H_n + (1-x^p) \right].$$

Divide (11) by $(-1)^n$ and $(1-x^p)$ and multiply by $1-x$ to get

$$x[(H+1)^n - x + 1 \equiv x^2 H_n + 1 - x \pmod{p}],$$

or

$$x[(H+1)^n \equiv x^2 H_n \pmod{p}],$$

whence

$$[(H+1)^n \equiv x H_n \pmod{p}].$$

But this relation is independent of p , an arbitrary prime, hence is an equation, and we have⁽⁸⁾

$$(12) \quad [(H+1)^n = x H_n, \quad n > 0.]$$

Taking $H_0 = 1$, we obtain,

$$H_1 = 1/(x-1), \\ H_2 = (1+x)/(x-1)^2,$$

⁽⁷⁾ In (10) we substitute the H_0 terms $(-1)^n$ of the $(-H-1)^n$ expansion and add $f_0 = (1-x^p)/(1-x)(-1)^n$ of the $(f+1)^n$ expansion, because (8) does not hold for $n=0$.

⁽⁸⁾ Frobenius, *Berlin Sitzungsberichte*, 1910, p. 828.

$$\begin{aligned}
 H_3 &= (1 + 4x + x^2)/(x - 1)^3, \\
 H_4 &= (1 + 11x + 11x^2 + x^3)/(x - 1)^4, \\
 H_5 &= (1 + 26x + 66x^2 + 26x^3 + x^4)/(x - 1)^5.
 \end{aligned}$$

Now write

$$(13) \quad H_n = R_n(x)/(x - 1)^n.$$

The $R_n(x)$ are the *Euler polynomials*,

$$\begin{aligned}
 R_1 &= 1, \\
 R_2 &= 1 + x, \\
 &\dots \dots \dots
 \end{aligned}$$

Putting (8) in (2) we obtain

$$\begin{aligned}
 x^2 \frac{1 - x^p}{1 - x} \{ [(-H + 1)^n - 1] + x \frac{1 - x^p}{1 - x} &\equiv (-1)^n x \frac{1 - x^p}{1 - x} H_n \pmod{p}, \\
 x^2 \{ [(-H + 1)^n - 1] + x &\equiv (-1)^n x H_n \pmod{p}, \\
 (14) \quad x^2 \{ [(H - 1)^n - (-1)^n] + (-1)^n x &\equiv x H_n, \\
 x[(H - 1)^n - x(-1)^n + (-1)^n &\equiv H_n \pmod{p}, \\
 x[(H - 1)^n - x(-1)^n + (-1)^n &= H_n,
 \end{aligned}$$

which is another recursion formula for the H 's.

We also have

$$\begin{aligned}
 [(k + (H + 1))^n] &= k^n + C_{n,1}k^{n-1}(H + 1) \\
 (15) \quad &+ C_{n,2}k^{n-2}(H + 1)^2 + \dots + (H + 1)^n \\
 &= k^n + C_{n,1}k^{n-1}xH_1 + C_{n,2}k^{n-2}xH_2 + \dots + xH_n,
 \end{aligned}$$

and

$$(16) \quad [(k + H)^n] = k^n + C_{n,1}k^{n-1}H_1 + C_{n,2}k^{n-2}H_2 + \dots + H_n.$$

Multiply (16) by x and subtract from (15). We then obtain⁽⁸⁾

$$(17) \quad [(k + H + 1)^n] - x[(k + H)^n] = k^n(1 - x).$$

Setting $k = 0, 1, 2, \dots, r$ in (9), we obtain

$$\begin{aligned}
 [(H + 1)^n - xH_n &= 0, \\
 [(H + 2)^n - x[(H + 1)^n] &= 1^n(1 - x), \\
 [(H + 3)^n - x[(H + 2)^n] &= 2^n(1 - x), \\
 &\dots \dots \dots, \\
 [(H + r)^n - x[(H + r - 1)^n] &= (r - 1)^n(1 - x).
 \end{aligned}$$

Now multiply the first of these by x^{r-1} , the second by x^{r-2} , and so on, and add. We then obtain

$$(18) \quad \begin{aligned} [(H+r)^n - x^r H_n &= (1-x)[1^n x^{r-2} + 2^n x^{r-3} + 3^n x^{r-4} + \dots \\ &+ (r-2)^n x + (r-1)^n] \\ &= (1-x)x^{r-1} f_n \left(\frac{1}{x} \right). \end{aligned}$$

Using a similar scheme, we obtain⁽⁹⁾ from (14)

$$(19) \quad x^{r+1} [(H-r)^n - x H_n = (-1)^n (x-1) f_n^{(r+1)}(x).$$

This is a rather curious relation; the expression on the left involves quotients of polynomials, while $f_n(x)$ is a polynomial for each r .

2. Generalization of the Mirimanoff and Euler polynomials and a related formula. Set

$$(20) \quad \begin{aligned} f_a(x, m, k) &= k^a + (k+m)^a x + (k+2m)^a x^2 + \dots \\ &+ (k+(p-1)m)^a x^{p-1}. \end{aligned}$$

We now consider

$$(21) \quad \frac{y^k(1-y^{mp}x^p)}{1-y^m x} = y^k + y^{(k+m)}x + \dots + y^{(k+(p-1)m)}x^{p-1}.$$

Differentiate this expression a times exponentially with respect to y and set $y=1$. We then obtain (20) on the right; on the left we differentiate in the form

$$(22) \quad \frac{y^k(1-y^{mp}x^p)}{1-y^m x} = (1-y^{mp}x^p) \left(\frac{y^k}{1-y^m x} \right),$$

and we then obtain

$$(23) \quad f_n(x, m, k) \equiv (1-x^p) \left[\frac{\bar{d}^n}{dy^n} \left(\frac{y^k}{1-xy^m} \right) \right]_{y=1} \pmod{p}.$$

We now set

$$(24) \quad \left[\frac{\bar{d}^n}{dy^n} \left(\frac{y^k}{1-xy^m} \right) \right]_{y=1} = \frac{\bar{H}_n(x, m, k)}{1-x} (-1)^n.$$

We now seek a recursion formula for this function. We have

$$(25) \quad \begin{aligned} &\frac{y^{-m}}{x} (y^k + xy^{k+m} + \dots + (x^{p-1}y^{k+(p-1)m})) \\ &= \frac{1}{x} y^{k-m} + (y^k + xy^{k+m} + \dots + x^{p-1}y^{k+(p-1)m}) - x^{p-1}y^{k+(p-1)m}. \end{aligned}$$

⁽⁹⁾ This result was obtained by Dr. A. M. Mood, following a suggestion by the writer.

Differentiate this relation n times exponentially and put $y=1$. We obtain

$$(26) \quad [(f(x, m, k) - m)^n \equiv x f_n(x, m, k) + (k - m)^n(1 - x^p) \pmod{p}].$$

Now (24) with (23) gives

$$(27) \quad f_n(x, m, k) \equiv (-1)^n \frac{1 - x^p}{1 - x} \overline{H}_n(x, m, k) \pmod{p},$$

which, applied to (26), gives

$$(28) \quad [(\overline{H} + m)^n = x \overline{H}_n + (m - k)^n(1 - x)].$$

The first three H 's given by this recursion formula are

$$\begin{aligned} \overline{H}_1 &= \frac{(m - k)(x - 1) + m}{x - 1} = \frac{k(1 - x) + mx}{x - 1}, \\ \overline{H}_2 &= \frac{[(m - k)(x - 1) + m]^2 + m^2 x}{(x - 1)^2}, \\ \overline{H}_3 &= \frac{[(m - k)(x - 1) + m]^3 + m^2 x^2(4m - 3k) + m^2 x(m + 3k)}{(x - 1)^3}. \end{aligned}$$

Now (28) is not a direct extension of (12). To obtain such an extension of the latter formula we use

$$y^k + x y^{k+m} + \dots + x^{p-1} y^{k+(p-1)m} - y^k + x^p y^k y^{pm} = \frac{y^{k+m} x(1 - y^{pm} x^p)}{1 - x y^m},$$

which, differentiated n times with $y=1$, gives

$$(29) \quad f_n(x, m, k) - k^n(1 - x^p) \equiv x(1 - x^p) \left[\frac{\overline{d}^n}{d y^n} \left(\frac{y^{k+m}}{1 - x y^m} \right) \right]_{y=1} \pmod{p}.$$

Putting

$$(30) \quad H_n(x, m, k) = (-1)^n (1 - x) \left[\frac{\overline{d}^n}{d y^n} \left(\frac{y^{k+m}}{1 - x y^m} \right) \right]_{y=1},$$

we then obtain

$$(31) \quad -f_n(x, m, k) - k^n(1 - x^p) \equiv (-1)^n x \frac{1 - x^p}{1 - x} H_n(x, m, k) \pmod{p}.$$

Using this in connection with (26), we find

$$(32) \quad [(H + m)^n = x H_n + (-k)^n(1 - x)].$$

For $k=0$, $m=1$, this reduces to (12).

3. Bernoulli numbers. Set

$$S_n(p) = 0^n + 1^n + 2^n + \cdots + (p-1)^n; \quad 0^0 = 1,$$

where p is a prime. If $n < p-1$, it is known that $S_n(p) \equiv 0 \pmod{p}$. We then write under this restriction

$$(33) \quad S_n(p) \equiv pa_n \pmod{p^2},$$

where a_n is some integer.

Consider

$$(34) \quad (1 + x + x^2 + \cdots + x^{p-1})x = x + x^2 + \cdots + x^p.$$

We now differentiate exponentially with respect to x , using Leibnitz's theorem. We obtain

$$(35) \quad \sum_{i=0}^n C_{n,i} x^i f_i(x) = x + 2^n x^2 + 3^n x^3 + \cdots + p^n x^p.$$

Restrict n to be greater than 1. Now (35) can be written

$$(36) \quad \sum_{i=0}^n C_{n,i} x^i f_i(x) = f_n^{(p)}(x) + p^n x^p.$$

Setting $x=1$, we have

$$(37) \quad \sum_{i=0}^n C_{n,i} S_i(p) = S_n(p) + p^n,$$

which, in view of (33) and of the fact that $n > 1$, is then

$$(38) \quad \sum_{i=0}^n C_{n,i} p a_i \equiv pa_n \pmod{p^2}.$$

Dividing through by p , we may write in symbolic form

$$(39) \quad [(a+1)^n \equiv a_n \pmod{p}].$$

Now consider the recursion formula

$$(40) \quad [(b+1)^n = b_n$$

for $n < p-1$. If we determine b_1, b_2, \dots, b_{n-1} in turn with the use of this, each denominator of the fractions so obtained will be prime to p . In view of (39) we may also obtain a_n in the same manner. Consequently, we may write

$$(41) \quad S_n(p) \equiv pb_n \pmod{p^2}.$$

It is known that $S_n(p) \equiv 0 \pmod{p^2}$ if n is odd, greater than 1, and less than $p-1$. Consequently,

$$pb_n \equiv 0 \pmod{p^2}, \quad b_n \equiv 0 \pmod{p}$$

for any $p > n + 1$; hence.

$$b_n = 0, \quad \text{for } n \text{ odd and greater than 1.}$$

4. We have, obviously,

$$(42) \quad \frac{x^p - 1}{x - 1} x^k = \frac{x^{(p+k)} - 1}{x - 1} - \frac{x^k - 1}{x - 1},$$

which may be written

$$(43) \quad (1 + x + x^2 + \dots + x^{p-1})x^k = 1 + x + \dots + x^{p-1} + x^p(1 + x + \dots + x^{k-1}) - (1 + x + \dots + x^{k-1}).$$

Differentiating this relation exponentially n times with respect to x and collecting the terms whose coefficients are divisible by p^2 , we obtain

$$(44) \quad [(f(x) + k)^n = f_n(x) + x^p f_n^{(k)}(x) + np x^p f_{n-1}^{(k)}(x) + p^2 P(x) - f_n^{(k)}(x),$$

where $P(x)$ is a polynomial in x with integral coefficients. Put $x = 1$; we then obtain

$$(45) \quad [(S(p) + k)^n = S_n(p) + np S_{n-1}(k) + p^2 W,$$

where W is an integer. We employ (41) in connection with (45) for each S occurring in the expansion of the left-hand member and for each S occurring in the right-hand member; after dividing the resulting expression through by p , we obtain the relation

$$(46) \quad [(b + k)^n \equiv b_n + n S_{n-1}(k) \pmod{p}.$$

As none of the terms in this congruence depends on p , we obtain the Bernoulli summation formula

$$(47) \quad [(b + k)^n - b_n = n S_{n-1}(k).$$

With (46) as a base we shall now prove the formula^(6, 10)

$$(48) \quad [(mb + sm + k)^n - [mb + k]^n = nm \sum_{i=0}^{s-1} (k + im)^{n-1}.$$

Consider

$$(49) \quad \begin{aligned} &(1 + x^m + \dots + x^{m(p-1)})x^{sm+k} - (1 + x^m + \dots + x^{m(p-1)})x^k \\ &= x^p m(x^k + x^{k+m} + \dots + x^{k+(s-1)m}) \\ &\quad - (x^k + x^{k+m} + \dots + x^{k+(s-1)m}), \end{aligned}$$

⁽¹⁰⁾ Due to Glaisher, Quarterly Journal of Mathematics, vol. 31 (1900), pp. 193-199. For another proof by the writer see American Mathematical Monthly, vol. 36 (1929), pp. 36-37.

where the k and m can be in any ring including the rational field. Employing the concept of generalized exponents used by the writer (Vandiver⁽³⁾) the exponential differentiation with respect to x gives

$$\begin{aligned}
 & [(f(x^m) + (sm + k))^n - (f(x^m) + k)^n \\
 (50) \quad &= n\phi m x^{pm} (k^{n-1} x^k + (k + m)^{n-1} x^{k+m} + \dots \\
 &+ (k + (s - 1)m^{n-1}) x^m) + \phi^2 P(x),
 \end{aligned}$$

from which we easily obtain (48), after using (41).

Various arithmetical results not involving explicitly the Bernoulli numbers may be derived by the exponential methods we have been employing. For example, if a is an integer such that

$$a^d \equiv 1 \pmod{\phi^\alpha},$$

then

$$(51) \quad (xa^d - 1)^n = \sum_{i=0}^n C_{n,i} x^i (-1)^i a^{id}.$$

Differentiating exponentially, with respect to x , k times for $k < m$, we find

$$(52) \quad P(x)(xa^d - 1)^{n-k} = \sum_{i=0}^n C_{n,i} x^i i^k (-1)^i a^{id},$$

where P is a polynomial in x . Put $x = 1$. Then we obtain

$$(53) \quad P(a^d - 1)^{n-k} = \sum_{i=0}^n C_{n,i} i^k (-1)^i a^{id},$$

whence

$$(54) \quad \sum_{i=0}^n C_{n,i} i^k (-1)^i a^{id} \equiv 0 \pmod{\phi^{\alpha(n-k)}}$$

for $k < n$. Putting

$$d = \phi - 1, \quad \alpha = 1, \quad n = 1,$$

we have Fermat's theorem.

5. Generalized Bernoulli numbers of the first order. In (48) set $s = \phi$, a prime. Then expand the left-hand member according to powers of ϕ . The result can be expressed in the form

$$\begin{aligned}
 (55) \quad S_{n-1}(m, k, \phi) = & C_{n,1} \left[(mb + k)^{n-1} \frac{\phi}{n} + C_{n,2} \left[(mb + k)^{n-2} \frac{\phi^2 m}{n} + \dots \right. \right. \\
 & \left. \left. + \frac{\phi^r m^{p-1}}{r + 1} C_{n-1,r} \phi \left[(mb + k)^{n-1-r} + \dots + \frac{\phi^n}{n} \right] \right].
 \end{aligned}$$

From this we may show that for $p > 2$ and $(mb + k)^0 = 1$

$$(56) \quad S_n(m, k, p) \equiv [(mb + k)^n p \pmod{p}].$$

To obtain a proof by induction assume that in (55) for $i < n - 1$, $[(mb + k)^i]$ may be expressed as a fraction with the denominator prime to p . Also for $r > 0$ and p odd we have

$$(57) \quad \frac{p^r}{r + 1} \equiv 0 \pmod{p},$$

since $p^r > r + 1$ for p odd, as is seen from

$$p^r \geq (1 + 2)^r \geq 1 + 2r.$$

Hence (55) gives (56). For p even and $n = 2$, (56) also holds, since we may verify that

$$(58) \quad 2(mb + k)^2 \equiv S_2(m, k, 2) \pmod{2}.$$

For brevity set

$$h_n = [(mb + k)^n].$$

Now for n odd, p odd, and m prime to p , the expression on the left of (56) is divisible by p , for n is not a multiple of $\overline{p-1}$ since $\overline{p-1}$ is even, and for $m \equiv 0 \pmod{p}$, $S_n(m, k, p)$ is obviously $\equiv 0 \pmod{p}$. Hence h_n does not have p as a factor of its denominator, except possibly when $p = 2$.

Now for $p = 2$ (57) holds for $r > 1$, so that

$$2^r = (1 + 1)^r > 1 + r$$

for $r > 1$. Hence (55) gives for $p = 2$, $n > 1$ and odd,

$$(59) \quad \sum_{s=0}^1 (sm + k)^n \equiv 2h_n + \frac{m}{n+1} C_{n+1,2} h_{n-1} 2^2 \pmod{2},$$

$$k^n + (m + k)^n \equiv 2h_n + mn(2h_{n-1}) \pmod{2}.$$

Since $k^n \equiv k \pmod{2}$, for m odd we have

$$(60) \quad 1 \equiv 2h_n + (2h_{n-1}) \pmod{2},$$

and for m odd, n even, we have

$$(60a) \quad 1 \equiv 2h_n \pmod{2}.$$

Now from this we cannot have both h_n and h_{n-1} with 2 in the denominator for n odd. Also for m even 2 will not appear in the denominator for n either odd or even. Now since 2 is in the denominator of h_2 for m odd by (58), h_3 is integral from (60). Hence (60) and (60a) give h_n integral for n odd and greater than 1.

Consequently,

$$[(bm + k)^n$$

is integral except when $n = 1$ with m odd, and also

$$(61) \quad S_n(m, k, 2) \equiv h_n \cdot 2 \pmod{2}$$

for n even.

Consider

$$(62) \quad h_n - \sum \frac{S_n(m, k, p)}{p},$$

where the p 's range over all the distinct primes less than or equal to $n + 1$. For a particular p , say p' , of this type the fraction

$$b_n - \frac{S_n(m, k, p')}{p'}$$

may be expressed with a denominator prime to p' by (56) and (61), and the remainder of the expression in (62) obviously has the same property. Hence (62) must have no primes in its denominator and is therefore an integer. Also,

$$S_n(m, k, p) \equiv 0 \pmod{p}$$

for m prime to p and $n \not\equiv 0 \pmod{p-1}$, and obviously also holds for $m \equiv 0 \pmod{p}$. For $n \equiv 0 \pmod{p-1}$ and m prime to p

$$S_n(m, k, p) \equiv p - 1 \equiv -1 \pmod{p},$$

whence the theorem follows⁽¹¹⁾.

THEOREM I. *If m and k are integers, then if n is even and greater than 0,*

$$\left[(mb + k)^n = A_n - \sum_{i=1}^s \frac{1}{p_i}, \right.$$

where p_1, p_2, \dots, p_s are the distinct primes which are prime to m and such that $n \equiv 0 \pmod{p_i - 1}$, A_n being some integer. If n is odd, then $[(mb + k)^n$ is an integer except when $n = 1$ with m odd.

6. In another paper⁽¹²⁾ the writer obtained the formulas

⁽¹¹⁾ This theorem was first stated by the writer without proof in Proceedings of the National Academy of Sciences, vol. 23 (1937), p. 556, and the present proof was there briefly indicated. Another proof was given in Duke Mathematical Journal, loc. cit., Theorem III. A third proof is given in §7 of the present paper, but the ordinary von Staudt-Clausen theorem is assumed therein.

⁽¹²⁾ Vandiver, Annals of Mathematics, (2), vol. 27 (1926), p. 174 (10); p. 175 (13).

$$\begin{aligned}
 (63) \quad & (x^m - 1) \sum_{n=0}^{a-1} C_{a,n} k^{a-n} m^{n+1} b_n f_{a-n}(x) \\
 & \equiv \sum_{\rho} \frac{x(\rho^k - 1)(x^p - 1)(x^m - 1)F_a(\rho)}{p(x - \rho^k)(x - 1)} \\
 & \quad - axm(x^m - 1) \sum_{\rho} \sum_{l=0}^{k-1} \frac{\rho^l h_{a-1}^{(k,l)}(x)}{x - \rho^k} \pmod{p},
 \end{aligned}$$

and

$$(64) \quad F_n(\rho) = (n - 1)p \frac{m f_{n-1}(\rho)}{\rho^p - 1} + p^2 C(\rho).$$

Applying the second formula to the first, dividing the first through by x and setting $x = 0$, we find

$$(65) \quad t_n(m, k) \equiv \sum_{\rho}' \frac{(-1)^{n+1} \rho^k f_{n-1}(\rho)}{1 - \rho^p} + \sum_{l=0}^{k-1} \sum_{\rho} l^{n-1} \rho^{l-k} \pmod{p},$$

where \sum_{ρ}' indicates summation over all the m th roots of unity except unity, and \sum_{ρ} indicates summation over all the distinct roots of unity; and where

$$(66) \quad \frac{[(mb + k)^n - b_n]}{n} = t_n(m, k).$$

When $k \geq m$, $(m, p) = 1$, $m > 1$, the relation (65) may also be given in the form

$$(67) \quad t_n(m, k) \equiv \sum_{\rho}' \frac{(-1)^{n+1} \rho^k f_{n-1}(\rho)}{1 - \rho^p} + m \sum_{s=1}^{[k/m]} (k - sm)^{n-1} \pmod{p}.$$

This is a companion formula to (47), but the latter is not obtainable⁽¹³⁾ from (67), as (67) does not hold for $n = 1$. Using (8) and (13), we find

$$(68) \quad f_n(x) \equiv x(1 - x)^{p-n-1} R_n(x) \pmod{p}.$$

Applying this to (67), we find the equality

$$(69) \quad t_n(m, k) = \sum_{\rho}' \frac{(-1)^{n+1} \rho^{k+1} R_{n-1}(\rho)}{(1 - \rho)^n} + m \sum_{s=1}^{[k/m]} (k - sm)^{n-1}.$$

In the relation (65) suppose that $m > k$. Then the last term on the right becomes zero, so that we obtain⁽¹⁴⁾

$$(70) \quad t_n(m, k) = \sum_{\rho}' \frac{(-1)^{n+1} \rho^{k+1} R_{n-1}(\rho)}{(1 - \rho)^n} = - \sum_{\rho}' \frac{\rho^{k+1} R_{n-1}(\rho)}{(\rho - 1)^n}.$$

⁽¹³⁾ Relations (65) and (67) were given without proof in another paper by the writer, Proceedings of the National Academy of Sciences, vol. 25 (1939), p. 200.

⁽¹⁴⁾ Frobenius, loc. cit., p. 827.

7. Application of some relations due to Frobenius⁽¹⁴⁾. We have

$$(71) \quad \frac{m}{\rho - 1} = \sum_{s=1}^{m-1} s\rho^s,$$

and from (69)

$$(72) \quad \begin{aligned} m^n t_n(m, k) &= - \sum' \left(\frac{m}{\rho - 1} \right)^n \rho^{k+1} R_{n-1}(\rho) + I \\ &= - \sum' \left(\sum_{s=1}^{m-1} s\rho^s \right)^n \rho^{k+1} R_{n-1}(\rho) + I, \end{aligned}$$

where I is an integer. The expression on the right is a polynomial in ρ with integral coefficients and when summed over all roots of unity except 1 will be an integer, as $\rho + \rho^2 + \dots + \rho^{m-1} = -1$. Hence $m^n t_n(m, k)$ is an integer.

To show that $m((mb+k)^n - b^n)$ is an integer we note that

$$\frac{m^n}{n} [(mb+k)^n - b^n]$$

is an integer; expanding this, we obtain

$$(73) \quad \frac{m^n}{n} [(m^n - 1)b_n + k^n + m(R)] = \frac{m^n}{n} K.$$

Since (73) is an integer, the fractions with denominators prime to m will cancel out and we shall be concerned only with primes in the denominators which divide m . By the von Staudt-Clausen theorem these appear only to the first power, hence in (73) $m(R)$ is an integer.

Let d denote the denominator of b_n ; then

$$(74) \quad \frac{m'}{n} (K)$$

is an integer in which $m' = (m^n, nd)$. But mn is divisible by m' , since prime factors of d occur only to the first power; hence we can replace m' by mn in (74) and obtain the desired result.

We shall now show that $[(mb+k)^n]$ is an integer for n odd and greater than 1 as in Theorem I. First note that $m[(mb+k)^n]$ is an integer, since b_n is zero for n odd and greater than 1. Now if $[(mb+k)^n]$ were a fraction, it would have a denominator which divided m . Hence, since every term of $[(mb+k)^n]$ contains m except the final term k^n , we see that $[(mb+k)^n]$ is an integer, except in the case when $n=1$ and m is odd. In the latter case we have $mb+k = -(1/2)m+k$.

8. We shall now give another proof of our Theorem I, using the von Staudt-Clausen theorem in the expansion of $[(mb+k)^n]$, that is,

$$(75) \quad [(mb + k)^n = m^n b_n + nm^{n-1} b_{n-1} k + \dots + k^n,$$

and obtaining

$$(76) \quad \left[(mb + k)^n = I + \sum \frac{m_i}{r_i}, \right.$$

where the m_i are integers less than r_i . Now

$$(77) \quad m [(mb + k)^n - b_n] = I_i,$$

where I_i represents an integer. Hence,

$$(78) \quad mI + m \sum \frac{m_i}{r_i} - m\alpha_n + m \sum \frac{1}{q_t} = I_1,$$

or

$$(79) \quad m \left(\sum \frac{m_i}{r_i} + \sum \frac{1}{q_t} \right) = I_2,$$

where I_2 represents an integer which combines mI , $m\alpha_n$, and terms wherein q_t and r_i divide m . Now in (79) no q_t or r_i divides m , hence

$$\left(\sum \frac{m_i}{r_i} + \sum \frac{1}{q_t} \right)$$

must be an integer I_3 ; therefore no r_i is different from some q_t and vice versa, and hence

$$\sum \frac{m_i + 1}{q_t} = I_3.$$

Since each term in this sum must be an integer and since $|m_i| < q_t$, we obtain $m_i = -1$. Thus, we have proved Theorem I.

9. Illustration of our congruence methods. In order to illustrate our congruence methods further we show how a known property of the generalized b 's may be easily derived. By direct expansion we find that

$$\sum_{s=0}^{p-1} (k + sm)^n = \sum_{i=0}^n C_{n,i} S_i(p) m^i k^{n-i}.$$

Now let $n+1 < p$; using (41) we find that

$$(80) \quad p \left[(mb + k)^n \equiv \sum_{s=0}^{p-1} (k + sm)^n \pmod{p^2}, \right.$$

whence

$$p \sum_{i=0}^{m-1} \left[(mb + i)^n = \sum_{i=0}^{m-1} \sum_{s=0}^{p-1} (ms + i)^n = \sum_{i=0}^{mp-1} i^n = S_n(mp) \equiv mp b_n \pmod{p^2}. \right.$$

Consequently⁽¹⁵⁾,

$$(81) \quad \sum_{i=0}^{m-1} [(mb + i)^n = mb_n,$$

10. We now develop some congruences of a novel character involving the Mirimanoff polynomials, and leading to congruences of a new type relating to the Bernoulli numbers. Obviously,

$$(x^k - 1) \frac{x^p - 1}{x - 1} = (x^p - 1) \frac{x^k - 1}{x - 1},$$

whence, for p an odd prime,

$$(x^k - 1)f_{p-1}(x) - kx^k f_{p-2}(x) + k^2 x^{2k} f_{p-3}(x) - \cdots + x^k k^{p-1} f_0(x) \\ \equiv (x^p - 1) \sum_{l=1}^{k-1} l^{p-1} x^l \pmod{p},$$

or, if $[u]$ is the greatest integer in u ,

$$- k f_{p-2}(x) + k^2 f_{p-3}(x) + \cdots + k^{p-1} f_0(x) \\ \equiv (x^p - 1) \sum_{l=1}^{k-1} l^{p-1} x^{l-k} + (x^{-k} - 1) \frac{x - x^p}{1 - x} \pmod{p} \\ \equiv \frac{(x^{p-k} - x^{-k})(x - x^k)}{1 - x} + \frac{(x^{-k} - 1)(x - x^p)}{1 - x} \\ - (x^p - 1)(x^{p-k} + x^{2p-k} + \cdots + x^{p[k/p]-k}) \pmod{p}, \\ \equiv 1 - x^{p-k} - (x^p - 1)(x^{p-k} + x^{2p-k} + \cdots + x^{p[k/p]-k}) \pmod{p},$$

where we understand that the second member is zero if $[k/p] = 0$. Assume $p > n + 1$, replace k by kr and multiply by r^{p-1-n} , let r take on $1, 2, \dots, p-1$, and add. We have, after dividing by $(1 - x^p)$

$$(82) \quad \frac{(-1)^{n+1} k^n f_{p-n-1}(x)}{1 - x^p} \equiv \sum_{r=1}^{p-1} \frac{1 - x^{p-kr}}{1 - x^p} (r)^{p-1-n} \\ + \sum_{r=1}^{p-1} r^{p-1-n} (x^{p-kr} + \cdots + x^{p[kr/p]-kr}) \\ \equiv - \frac{x^p f_{p-n-1}(x^{-k})}{1 - x^p} \\ + \sum_{r=1}^{p-1} r^{p-1-n} (x^{p-kr} + \cdots + x^{p[kr/p]-kr}).$$

⁽¹⁵⁾ Kummer, Crelle's Journal, vol. 40 (1850), pp. 119-121; Blissard, Quarterly Journal of Mathematics, vol. 4 (1861), p. 288. There are also later references.

Let $x = \rho$, an m th root of unity different from 1, $(m, p) = 1$ and let \sum' indicate summation over all ρ 's $\neq 1$, and set $k = 2$. We obtain, modulo p ,

$$(83) \quad \sum' \frac{(-1)^{n+1} f_{p-n-1}(\rho) k^n}{1 - \rho^p} \equiv \sum' f_{p-n-1}(\rho^{-k}) - \sum' \frac{f_{p-n-1}(\rho^{-k})}{1 - \rho^p} + \sum' \sum_{s=(p+1)/2}^{p-1} s^{p-1-n} \rho^{p-sk}.$$

Let $m < (p-1)/2$ and $(m, 2) = 1$, $p > 2$ and $m > 2$, and consider the expression

$$\sum_{s=(p+1)/2}^{p-1} s^{p-1-n} \rho^{p-sk},$$

and we shall determine the terms in which the exponents of ρ are $\equiv 0 \pmod{m}$. If l is one such, then

$$p - lk \equiv 0 \pmod{m},$$

where l is in the set $(p+1)/2, \dots, p-1$. From the above congruence $(p+m)/2$ is a solution, but $(p-m)/2$, although it satisfies the congruence, is not in the set mentioned. Hence the solutions we need for $[p/m]$ odd are:

$$\frac{p+m}{2}, \frac{p+3m}{2}, \dots, \frac{p+[p/m]m}{2}.$$

For $[p/m]$ even, it is replaced by $([p/m]-1)$ in the above.

$$(84) \quad \sum' \sum_{s=(p+1)/2}^{p-1} s^{p-1-n} \cdot \rho^{p-sk} \equiv - \sum_{s=(p+1)/2}^{p-1} s^{p-1-n} + m \sum_{v=1}^h \left(\frac{p+vm}{2} \right)^{p-1-n},$$

where $h = [p/m]$ or $[p/m]-1$ according as $[p/m]$ is odd or even.

Now

$$\frac{p+jm}{2} \equiv \frac{jm}{2} \pmod{p},$$

so that the last term on the right is congruent, modulo p , to

$$m^{p-n} \left(\left(\frac{p+1}{2} \right)^{p-1-n} + \left(\frac{p+3}{2} \right)^{p-1-n} + \dots + \left(\frac{p+h}{2} \right)^{p-1-n} \right),$$

where h is defined as above.

If in (83) we employ (67) where the k used in the latter congruence equals zero, we obtain new relations involving Bernoulli numbers in view of (66).

11. Bernoulli numbers of the second order. We employ the identity⁽¹⁶⁾

⁽¹⁶⁾ Vandiver, Annals of Mathematics, (2), vol. 29 (1928), p. 171.

$$(85) \quad \frac{x^j - y^k}{(x-1)(y-1)} = \frac{\sum_{n=0}^{j-1} x^n y^{k-a_n}}{y-1} - \frac{\sum_{l=0}^{k-1} y^l x^{j-b_l}}{x-1},$$

where $a_n = [nk/j]$, $b_l = [lj/k]$, $[u]$ is the greatest integer in u , j and k are positive integers, x and y arbitrary. Multiply by $(x^p-1)(y^p-1)$, where p is a prime greater than n , set $x = xz^k$, $y = yz^j$, divide by z^{jk} , differentiate exponentially a times with respect to z and set $z = 1$. We then have, reducing the right-hand member, modulo p^3 , and where $h_a^{(m,k)}(x)$ is the $f_a(x, m, k)$ of (20),

$$(86) \quad \begin{aligned} (x^j - y^k) \left[(kf(x) + jf(y))^a \right] &\equiv y^k (x^p - 1) \sum_{n=0}^{j-1} x^n y^{-a_n} h_a^{(j, c_n)}(y) \\ &\quad + \sum_{n=0}^{j-1} akx^{p+n} y^{k-a_n} p h_{a-1}^{(j, c_n)}(y) \\ &\quad + C_{a,2} k^2 x^p y^{k-a_n} \sum_{n=0}^{j-1} p^2 h_{a-2}^{(j, c_n)}(y) \\ &\quad - x^j (y^p - 1) \sum_{l=0}^{k-1} y^l x^{j-b_l} h_a^{(k, d_l)}(x) \\ &\quad - apj \sum_{l=0}^{k-1} y^{p+l} x^{j-b_l} h_{a-1}^{(k, d_l)}(x) \\ &\quad - C_{a,2} j^2 p^2 \sum_{l=0}^{k-1} h_{a-2}^{(k, d_l)}(x) \pmod{p^3}, \end{aligned}$$

where c_n denotes the least positive or zero residue of nk , modulo j , while d_l denotes the least positive or zero residue of lj , modulo k . Now set $x = xz^k$ and differentiate once with respect to z ; we then have, modulo p^3 , after setting $z = 1$,

$$(87) \quad \begin{aligned} &kjx^j [(kj(x) + jf(y))^a + (x^j - y^k) [\overline{D}_z [(kf(x) + jf(y))^a]]_{z=1} \\ &\equiv y^k (x^p - 1) \left[\overline{D}_z \left(\sum_{n=0}^{j-1} x^n z^{nk} y^{-a_n} h_a^{(j, c_n)}(y) \right) \right]_{z=1} \\ &\quad + pkx^p y^k \sum_{n=0}^{j-1} x^n y^{-a_n} h_a^{(j, c_n)}(y) + \sum_{n=0}^{j-1} ak^2 (p+n) y^{k-a_n} p h_{a-1}^{(j, c_n)}(y) \\ &\quad - apj \sum_{l=0}^{k-1} y^{p+l} x^{j-b_l} h_a^{(k, d_l)}(x) - apj^2 \sum_{l=0}^{k-1} (k-l) y^{p+l} x^{j-b_l} h_{a-1}^{(k, d_l)}(x) \end{aligned}$$

plus terms of the form $p^2g(x)$, where each g is divisible by some $h_i(x)$.

Setting $x = y = 1$, dividing through by p^2 , and using

$$(88) \quad \begin{aligned} p(rb + s)^n &\equiv s^n + (r + s)^n + (2r + s)^n + \dots \\ &\quad + ((p-1)r + s)^n \pmod{p^2}, \end{aligned}$$

which follows from (55) for $p > n$, we find, since the result is independent of p ,

$$(89) \quad kj \left[(kb + jb')^a = k \sum_{n=0}^{j-1} (jb + c_n)^a + a \sum_{n=0}^{j-1} k^2 n \left[(jb + c_n)^{a-1} \right. \right. \\ \left. \left. - aj \sum_{l=0}^{k-1} (kb + d_l)^a - aj^2 \sum_{l=0}^{k-1} [(kb + d_l)^{a-1} (k - l)], \right. \right.$$

or since by (81)

$$(90) \quad \sum_{n=0}^{j-1} (jb + c_n)^a = jb_a; \quad \sum_{l=0}^{k-1} (kb + d_l)^a = kb_a,$$

we may write

$$(91) \quad kj \left[(kb + jb')^a = jk(1 - a)b_a - ak^2 j^2 b_{a-1} + a \sum_{n=0}^{j-1} k^2 n \left[(jb + c_n)^{a-1} \right. \right. \\ \left. \left. + a \sum_{l=0}^{k-1} j^2 l \left[(kb + d_l)^{a-1}. \right. \right. \right.$$

For $h = 2, j = 1$, we find⁽¹⁷⁾

$$(92) \quad 2[(2b + b')^a = 2(1 - a)b_a - 4ab_{a-1} + a(2b + 1)^{a-1}.$$

Now since $(-b)^n = b^n$ except for $n = 1$, we have

$$(93) \quad [(kb - jb')^a = [(kb + jb')^a + ajk^{a-1}b_{a-1},$$

whence from (91)

$$(94) \quad kj \left[(kb - jb')^a = jk(1 - a)b_a - ak^2 j^2 b_{a-1} + ajk^{a-1}b_{a-1} \right. \\ \left. + a \sum_{n=0}^{j-1} k^2 n \left[(jb + c_n)^{a-1} + a \sum_{l=0}^{k-1} j^2 l \left[(kb + d_l)^{a-1}. \right. \right. \right.$$

Setting $j = k = 1$ in (91) and (94), we obtain the well known relations

$$(95) \quad [(b + b')^a = (1 - a)b_a + ab_{a-1},$$

and

$$(96) \quad [(b - b')^a = (1 - a)b_a.$$

Now for a odd we have

$$(97) \quad [(kb + jb')^a = akb_1(jb)^{a-1} + a(kb)^{a-1}jb_1,$$

so that from (91) we have the formula

⁽¹⁷⁾ Bell, these Transactions, vol. 24 (1922), p. 106.

$$\begin{aligned}
 ak^2b_1b_{a-1}j^a + aj^2b_1b_{a-1}k^a &= ab_1b_{a-1}(k^2j^a + j^2k^a) \\
 (98) \qquad \qquad \qquad &= -ak^2j^2b_{a-1} + a \sum_{n=0}^{j-1} k^2n \left[(jb + c_n)^{a-1} \right. \\
 &\qquad \qquad \qquad \left. + a \sum_{l=0}^{k-1} j^2l \left[(kb + d_l)^{a-1} \right. \right.
 \end{aligned}$$

There is an analogous relation from (94).

12. If h is any integer, we have from (91)

$$\begin{aligned}
 (99) \qquad \left[(kb + jb' + h)^n \right] &= \sum_{a=0}^n C_{n,a} \left[(kb + jb')^a h^{n-a} \right. \\
 &= jk \sum_{a=0}^n C_{n,a} b_a h^{n-a} - jk \sum_{a=0}^n C_{n,a} ab_a h^{n-a} \\
 &\quad - k^2j^2 \sum_{a=1}^n aC_{n,a} h^{n-a} b_{a-1} + \sum_{a=1}^n \sum_{i=0}^{j-1} k^2iaC_{n,a} \left[(jb + c_i)^{a-1} h^{n-a} \right. \\
 &\quad \left. + \sum_{a=1}^n \sum_{i=0}^{k-1} j^2laC_{n,a} \left[(kb + d_i)^{a-1} \right. \right. \\
 &= jk \left[(b + h)^n - jkn \sum_{a=1}^n C_{n-1,a-1} h^{n-a} b_a \right. \\
 &\quad - k^2j^2n \sum_{a=1}^n C_{n-1,a-1} h^{n-a} b_{a-1} \\
 &\quad \left. + \sum_{a=1}^n \sum_{i=1}^{j-1} k^2inC_{n-1,a-1} \left[(jb + c_i)^{a-1} h^{n-a} \right. \right. \\
 &\quad \left. \left. + \sum_{a=1}^n \sum_{l=0}^{k-1} j^2lnC_{n-1,a-1} \left[(kb + d_l)^{a-1} h^{n-a} \right. \right. \right.
 \end{aligned}$$

where we have changed the notation employed in (91). n now takes the place of a and c_i denotes the least positive or zero residue of ik , modulo j . Now

$$(100) \qquad \sum_{a=1}^n C_{n-1,a-1} b_a h^{n-a} = \left[b(h + b)^{n-1}, \right.$$

and

$$(101) \qquad [b(h + b)^{n-1}] = [(h + b)^n - h[(h + b)^{n-1}],$$

and we have this theorem:

THEOREM II. *If h, j and k are integers, $k > 0, j > 0$; c_i represents the least positive or zero residue of $ik \pmod{j}$; d_l represents the least positive or zero residue of $lj \pmod{k}$; $n > 0$; then*

$$\begin{aligned}
 (102) \quad jk[(kb + jb' + h)^n &= jk[(b + h)^n - jkn[(b + h)^n \\
 &\quad + jknh[(b + h)^{n-1} - k^2j^2n[(b + h)^{n-1} \\
 &\quad + k^2n \sum_{i=0}^{j-1} i \left[(jb + c_i + h)^{n-1} \right. \\
 &\quad \left. + j^2n \sum_{l=0}^{k-1} l \left[(kb + d_l + h)^{n-1} \right. \right.
 \end{aligned}$$

Now since $(-b)^a = b^a$ except for $a = 1$, we have

$$(103) \quad [(kb - jb' + h)^n = [(kb + jb' + h)^n + nj[(kb + h)^{n-1}.$$

This formula with (102) gives the following theorem:

THEOREM III. *If h, j and k are integers, n even and greater than 0, then*

$$(104) \quad jk \left[(kb + jb' + h)^n = I - (1 - n)jk \sum_{i=1}^s \frac{1}{p_i}, \right.$$

where the p 's are the distinct primes such that $n \equiv 0 \pmod{p_i - 1}$, I being some integer.

This is an analogue of the generalized von Staudt-Clausen theorem (I).

Now for n odd, (102) and (103) give

THEOREM IV. *If $(n+1)$ is odd, then for n greater than zero*

$$(105) \quad jk \left[(kb + jb' + h)^{n+1} = I_1 + (n+1)jk \left(\frac{j}{2} + \frac{k}{2} - h \right) \sum_{i=1}^s \frac{1}{p_i}, \right.$$

where I_1 is some integer, k, j and h are integers, kj is odd and the p 's are defined as in Theorem III.

It is not clear that this result is an analogue of any theorem involving the Bernoulli numbers of the first order.

We also have from (102) and (103) the

COROLLARY I. *Any Bernoulli number of the second order can be expressed as a linear combination of Bernoulli numbers of the first order with coefficients whose denominators divide the integers occurring in the original number.*

COROLLARY II. *The expression*

$$(106) \quad jk[(kb + jb' + h)^n + jk(n-1)[(b + h)^n$$

is an integer if n is even, j, k and h integers.

The relation (102) gives, employing Theorem II of another paper⁽¹⁸⁾ the congruence

⁽¹⁸⁾ Vandiver, Duke Mathematical Journal, loc. cit.

$$(107) \quad jk[(kb + jb' + h)^n \equiv 0 \pmod{p^\alpha},$$

where n is odd, p prime, $n-1 = p^\alpha r$, $(r, p) = 1$, $(p, p_i) = 1$, p_i being any von Staudt-Clausen prime of order $n-1$. If n is even, this relation also holds if $n \equiv 0 \pmod{p^\alpha}$, $(p, q) = 1$, where q is any von Staudt-Clausen prime of order n .

13. We shall now prove that

$$(108) \quad b_{a-1}(j^2 - j^a) \equiv 2 \sum_{i=0}^{j-1} i \left[(jb + c_i)^{a-1},$$

with a odd and c_i denoting the least positive or zero residue of $ik \pmod{j}$. Assuming (108) true for all values of k such that $k < j$, $(k, j) = 1$, we have from (91)

$$(109) \quad -b_{a-1}(k^2 j^a + j^2 k^a) + 2k^2 j^2 b_{a-1} \\ = 2 \sum_{i=0}^{j-1} k^2 i \left[(jb + c_i)^{a-1} + 2 \sum_{l=0}^{k-1} j^2 l \left[(kb + d_l)^{a-1},$$

and also

$$(110) \quad -b_{a-1}(k^2 j^a + j^2 k^a - 2k^2 j^2) = 2 \sum_{i=0}^{j-1} k^2 i \left[(jb + c_i)^{a-1} + j^2(k^2 - k^a) b_{a-1},$$

using $c_i = c_r$ where $d_l = d_r$ with $r \equiv l \pmod{k}$, $(r, k) = 1$, $r < k$; whence, the result.

14. Let $\rho^j = 1$; then

$$(111) \quad \left[(jb + c_n)^a \equiv b_a + (-1)^{a+1} a \sum' \frac{\rho^{cn} f_{a-1}(\rho)}{1 - \rho^p} \pmod{p}, \quad a > 1;$$

where \sum' indicates summation over all distinct j th roots of unity different from 1; then

$$(112) \quad \frac{1}{2} b_a (j^2 - j^{a+1}) \equiv \sum_{n=1}^{j-1} n \left[(jb + c_n)^a \\ \equiv \sum_{n=1}^{j-1} n b_a + (-1)^{a+1} a \sum_{n=1}^{j-1} \sum' \frac{n \rho^{cn} f_{a-1}(\rho)}{1 - \rho^p} \pmod{p},$$

or

$$(113) \quad \frac{j - j^{a+1}}{2} b_a \equiv (-1)^{a+1} a \sum_{n=1}^{j-1} \sum' \frac{n \rho^{cn} f_{a-1}(\rho)}{1 - \rho^p},$$

$$(114) \quad \frac{(1 - j^a) b_a}{2a} \equiv \sum' \frac{f_{a-1}(\rho)}{(1 - \rho^k)(1 - \rho^p)}, \quad a \text{ even and greater than 1.}$$

The latter relation may be proved directly by noting that if $(k, j) = 1$,

$$(115) \quad \frac{f_{a-1}(\rho)}{(1 - \rho^k)(1 - \rho^p)} = \frac{\rho^{-k}(-1)^{a-1}f_{a-1}(\rho^{-1})}{(\rho^k - 1)(\rho^{-p} - 1)}.$$

Hence

$$(116) \quad \sum' \frac{f_{a-1}(\rho)}{(1 - \rho^k)(1 - \rho^p)} = \sum' \frac{-\rho^k f_{a-1}(\rho)}{(1 - \rho^k)(1 - \rho^p)},$$

and

$$(117) \quad \begin{aligned} \sum' \left(\frac{f_{a-1}(\rho)}{(1 - \rho^k)(1 - \rho^p)} + \frac{-\rho^k f_{a-1}(\rho)}{(1 - \rho^k)(1 - \rho^p)} \right) \\ = \sum' \frac{f_{a-1}(\rho)}{1 - \rho^p} \equiv (-1)^a \frac{(1 - j^a)b_a}{a} \pmod{p}. \end{aligned}$$

15. Take the obvious identity

$$\frac{x - y}{(x - 1)(y - 1)} = \frac{y}{y - 1} - \frac{x}{x - 1}$$

((85) reduces to this for $k=1, j=1$). We may then write

$$(118) \quad (x - y)f_0^{(kp)}(x)f_0^{(jp)}(y) = y(x^{kp} - 1)f_0^{(jp)}(y) - x(y^{jp} - 1)f_0^{(kp)}(x).$$

Set $x = xz, y = yz$, divide by z , then differentiate each member exponentially a times with respect to z , and reduce the terms, modulo p^2 ; after setting $z = 1$, we find

$$(119) \quad \begin{aligned} (x - y)[(f(x) + f(y))^a] &\equiv (x^{kp} - 1)yf_a^{(jp)}(y) + akpx^{kp}yf_{a-1}^{(jp)}(y) \\ &+ C_{n,2}k^2p^2x^{kp}yf_{a-2}^{(jp)}(y) - (y^{jp} - 1)xf_a^{(kp)}(x) \\ &- ajpy^{jp}xf_{a-1}^{(kp)}(x) \\ &- C_{n,2}j^2p^2y^{jp}xf_{a-2}^{(kp)}(x) \pmod{p^3}. \end{aligned}$$

Set $x = \zeta$, a k th root of unity, and $y = \rho$, a j th root of unity, let p be a prime greater than a , and then sum each member over all values of ζ and ρ except when ζ and ρ are simultaneously 1. We obtain

$$(120) \quad \sum_{\rho, \zeta} \left[\frac{1}{p^2} (f^{(kp)}(\zeta) + f^{(jp)}(\rho))^a \right] \equiv \sum_{\rho, \zeta} \left\{ \frac{ak\rho f_{a-1}^{(jp)}(\rho)}{p(\zeta - \rho)} + \frac{aj\zeta f_{a-1}^{(kp)}(\zeta)}{p(\zeta - \rho)} \right\} \pmod{p}.$$

We note that this is symmetric in j and k , hence we need consider only the first term on the right (call it T_1) and obtain T_2 , the second term, by interchanging j and k . First, in T_1 we sum $1/(\zeta - \rho)$ with respect to ζ for $\rho \neq 1$. To effect this we employ the identity

$$x^k - 1 = (x - 1)(x - \zeta) \cdots (x - \zeta^{k-1}),$$

where ζ now represents a primitive k th root of unity. Ordinary differentiation of this with respect to x gives

$$kx^{k-1} = \frac{x^k - 1}{x - 1} + \frac{x^k - 1}{x - \zeta} + \cdots + \frac{x^k - 1}{x - \zeta^{k-1}}.$$

Dividing by $x^k - 1$; putting $x = \rho$; and changing signs, we have

$$\frac{k\rho^{k-1}}{1 - \rho^k} = \frac{1}{1 - \rho} + \frac{1}{\zeta - \rho} + \cdots + \frac{1}{\zeta^{k-1} - \rho},$$

which is the desired sum. Hence

$$(121) \quad T_1 = \sum_{\rho} \frac{ak^2 \rho^k f_{a-1}^{(ip)}(\rho)}{p(1 - \rho^k)} + \sum_{\zeta} \frac{ak f_{a-1}^{(ip)}(1)}{p(\zeta - 1)}.$$

Now, using (71), we have

$$(122) \quad \begin{aligned} \sum_{\zeta} \frac{ak f_{a-1}^{(ip)}(1)}{p(\zeta - 1)} &= - \frac{ak(k - 1)}{2} \cdot \frac{f_{a-1}^{(ip)}(1)}{p} \\ &= - \frac{1}{2} ak(k - 1) \frac{S_{a-1}(jp)}{p} \\ &\equiv - \frac{1}{2} ak(k - 1)jb_{a-1} \pmod{p} \end{aligned}$$

for $a < p$. To transform the other term in T_1 we employ the relation, with $n > 0$,

$$x^p(-1)^n f_n\left(\frac{1}{x}\right) \equiv f_n(x) \pmod{p},$$

together with⁽¹⁹⁾

$$f_n^{(ip)}(\rho) \equiv -njp \frac{f_{n-1}(\rho)}{1 - \rho^p} \pmod{p^2}.$$

In this way we obtain for $a > 2$, modulo p ,

$$\begin{aligned} \sum_{\rho} \frac{\rho^k f_{a-1}(\rho)}{p(1 - \rho^k)} &\equiv \sum_{\rho} \frac{(a - 1)j\rho^k f_{a-2}(\rho)}{(1 - \rho^k)(\rho^p - 1)} \\ &\equiv \sum_{\rho} \frac{(a - 1)j(-1)^{a-2}\rho^p \cdot \rho^k f_{a-2}(\rho^{-1})}{(1 - \rho^k)(\rho^p - 1)} \\ &\equiv \sum_{\rho} \frac{(a - 1)j(-1)^{a-2} f_{a-2}(\rho^{-1})}{(\rho^{-k} - 1)(1 - \rho^{-p})}, \end{aligned}$$

⁽¹⁹⁾ Vandiver, *Annals of Mathematics*, (2), vol. 27 (1926), p. 175.

that is,

$$(123) \quad \sum_{\rho} \frac{\rho^k f_{a-1}(\rho)}{\rho(1-\rho^k)} \equiv \sum_{\rho} \frac{(a-1)j(-1)^{a-2} f_{a-2}(\rho)}{(\rho^k-1)(1-\rho^{\rho})} \pmod{\rho}.$$

Using (122) and (123) in connection with (121), we obtain

$$T_1 \equiv \sum_{\rho} \frac{ak^2(a-1)j(-1)^{a-2} f_{a-2}(\rho)}{(\rho^k-1)(1-\rho^{\rho})} - \frac{ak(k-1)}{2} j b_{a-1} \pmod{\rho},$$

and T_2 is obtained from this by interchanging j and k together with ρ and ζ . Add the quantity

$$(124) \quad \frac{1}{\rho^2} [(f^{(k\rho)}(1) + f^{(j\rho)}(1))^a] \equiv [(b + b')^a] j k \pmod{\rho}$$

to both members of (120); after employing

$$\sum_{\rho} f_n^{(k\rho)}(\rho) \equiv k^{n+1} b_n \rho \pmod{\rho^2}$$

and the corresponding relation involving j , we then obtain (using (95))

$$(125) \quad \frac{[(kb + jb')^a]}{a(a-1)} + \frac{b_{a-1}}{2(a-1)}(k+j) + \frac{b_a}{a} \\ \equiv k \sum_{\rho} \frac{(-1)^a f_{a-2}(\rho)}{(\rho^k-1)(1-\rho^{\rho})} + j \sum_{\zeta} \frac{(-1)^a f_{a-2}(\zeta)}{(\zeta^j-1)(1-\zeta^{\rho})} \pmod{\rho},$$

where $j > 1, k > 1, 2 < a < \rho$, with j, k and ρ prime each to each. Employing (68) for $x = \rho, n = a - 2$, we obtain the following theorem:

THEOREM V. *If $j > 1, k > 1, a > 2$, with $(j, k) = 1, \rho$ a j th root of unity different from 1, ζ a k th root of unity different from 1, then*

$$(126) \quad \frac{[(kb + jb')^a]}{a(a-1)} + \frac{b_{a-1}}{2(a-1)}(k+j) + \frac{b_a}{a} \\ = k \sum_{\rho} \frac{\rho R_{a-2}(\rho)}{(1-\rho^k)(\rho-1)^{a-1}} + j \sum_{\zeta} \frac{\zeta R_{a-2}(\zeta)}{(1-\zeta^j)(\zeta-1)^{a-1}},$$

where the summations extend over each distinct value of ρ and ζ , respectively, and the R 's are defined as in (13).

We shall now show how to obtain (91) from (125), but subject to the restrictions on the latter relation. Using (71) we have

$$\frac{j}{\rho^k - 1} = \sum_{i=1}^{j-1} i \rho^{ik},$$

and letting c_i as before be the least positive or zero residue of $ik \pmod j$, and employing (65), we have

$$(127) \sum_{\rho} \frac{(a-1)j(-1)^{a-2}f_{a-2}(\rho)}{(\rho^k-1)(1-\rho^p)} \equiv \sum_{i=1}^{j-1} i \left[(jb+c_i)^{a-1} - b_{a-1} \frac{j(j-1)}{2} \pmod p \right],$$

with a similar expression for the other term in the right-hand member of (125); if we substitute in (125) we have (91), after noting that the resulting terms are independent of p .

Using Theorem V, we obtain the corollary:

COROLLARY I. *The expression*

$$k^a j^a \left(\frac{[(kb+jb')^a]}{a(a-1)} + \frac{b_{a-1}}{2(a-1)}(k+j) + \frac{b_a}{a} \right)$$

is an integer with the restrictions on j, k and a given in Theorem V.

We also have this corollary:

COROLLARY II. *If j, k and a are restricted as in Theorem V, we have, if $(jk, a(a-1)) = 1$,*

$$2[(kb+jb')^a + ab_{a-1}(k+j) + 2(a-1)b_a \equiv 0 \pmod{a(a-1)}].$$

These results indicate certain analogies between the properties of T_n in (69) and the number expressed by the left-hand member of (125).

16. Bernoulli numbers of higher order. Bernoulli numbers of higher order than the second, namely, numbers of the form

$$(128) \quad [(m_r b^{(r)} + m_{r-1} b^{(r-1)} + \dots + m_1 b' + m_0)^n = b_n(m_r, m_{r-1}, \dots, m_0),$$

for $r \geq 3; m_i \neq 0; i = 1, 2, \dots, r,$

do not have properties as simple as those of the first and second order, since other primes than the von Staudt-Clausen primes appear as factors in the denominators of such numbers. This may be illustrated in the case of the number

$$[(b^{(1)} + b^{(2)} + \dots + b^{(s)})^n.$$

This may be reduced as follows. Consider first

$$[(b + b' + b'')^n = b_n + nb_{n-1}(b' + b'') + \dots + C_{n,2}b_{n-2}(b' + b'')^2 + \dots.$$

Then

$$[(b' + b'')^k = (1 - k)b_k - kb_{k-1},$$

so that

$$\begin{aligned}
 (129) \quad & \left[(b + b' + b'')^n = \sum_{r=0}^n C_{n,r} b'_{n-r} ((1-r)b_r - r b_{r-1}) \right. \\
 & \left. = \sum_{r=0}^n C_{n,r} b'_{n-r} b_r - \sum_{r=0}^n C_{n,r} r b'_{n-r} b_r - \sum_{r=0}^n C_{n,r} r b'_{n-r} b_{r-1}. \right.
 \end{aligned}$$

Now

$$(130) \quad \sum_{r=0}^n C_{n,r} b'_{n-r} b_r = \left[(b + b')^n. \right.$$

Also,

$$(131) \quad \sum_{r=0}^n r C_{n,r} b'_{n-r} b_r = n \sum_{r=1}^n C_{n-1,r-1} b'_{n-r} b_{r-1} b = n \sum \left[b(b + b')^{r-1}. \right.$$

Now

$$\left[b(b + b')^{r-1} = (1/2) [(b + b')(b + b')^{r-1} = (1/2) [(b + b')^r, \right.$$

so that

$$(132) \quad \sum_{r=0}^n r C_{n,r} b'_{n-r} b_r = \frac{n}{2} \left[(b + b')^r. \right.$$

Also,

$$(133) \quad \sum_{r=0}^n C_{n,r} r b'_{n-r} b_{r-1} = n \sum_{r=1}^n C_{n-1,r-1} b'_{n-r} b_{r-1} = n \left[(b + b')^{r-1}. \right.$$

Hence, using (130), (131), (132), and (133) with (129), we have

$$(134) \quad \left[(b + b' + b'')^n = \left(1 - \frac{n}{2} \right) \left[(b + b')^n - n \left[(b + b')^{n-1}. \right. \right. \right.$$

We shall now prove, by induction on s , the formula ($n > 0$)

$$\begin{aligned}
 (135) \quad & \left[(b^{(1)} + b^{(2)} + \dots + b^{(s)})^n = \left(1 - \frac{n}{s-1} \right) \left[(b^{(1)} + b^{(2)} + \dots + b^{(s-1)})^n \right. \right. \\
 & \left. \left. - n \left[(b^{(1)} + b^{(2)} + \dots + b^{(s-1)})^{n-1}. \right. \right.
 \end{aligned}$$

Assume for $s > 2$

$$\begin{aligned}
 (136) \quad & \left[(b^{(1)} + b^{(2)} + \dots + b^{(s-1)})^n = \left(1 - \frac{n}{s-2} \right) \left[(b^{(1)} + b^{(2)} + \dots + b^{(s-2)})^n \right. \right. \\
 & \left. \left. - n \left[(b^{(1)} + b^{(2)} + \dots + b^{(s-2)})^{n-1}; \right. \right.
 \end{aligned}$$

then

$$(137) \quad \left[(b^{(1)} + b^{(2)} + \dots + b^{(s)})^n = \sum_{r=0}^n C_{n,r} \left[b_{n-r}(b^{(1)} + \dots + b^{(s-1)})^r, \right.$$

and by (144)

$$\begin{aligned} &= \sum_{r=0}^n C_{n,r} \left[b_{n-r}(b^{(1)} + \dots + b^{(s-2)})^r \right. \\ &\quad - \sum_{r=0}^n \frac{r}{s-2} C_{n,r} \left[b_{n-r}(b^{(1)} + \dots + b^{(s-2)})^r \right. \\ &\quad \left. \left. - \sum_{r=0}^n r C_{n,r} \left[b_{n-r}(b^{(1)} + \dots + b^{(s-2)})^{n-1}; \right. \right. \end{aligned}$$

or by previous methods this reduces to

$$\begin{aligned} &\left[(b' + \dots + b^{(s)})^n \right. \\ &= \left[(b' + \dots + b^{(s-1)})^n \right. \\ &\quad - \frac{n}{s-2} \left[(b^{(1)} + \dots + b^{(s-2)})(b^{(1)} + \dots + b^{(s-1)})^{n-1} \right. \\ (138) \quad &\quad \left. - \sum_{r=1}^n n C_{n-1,r-1} \left[b_{n-r}(b' + \dots + b^{(s-2)})^{n-1} \right. \right. \\ &= \left[(b' + \dots + b^{(s-1)})^n - \frac{n}{s-2} \cdot \frac{s-2}{s-1} (b^{(1)} + \dots + b^{(s-1)})^n \right. \\ &\quad \left. - n[(b^{(1)} + \dots + b^{(s-1)})^n, \right. \end{aligned}$$

which is the result.

Employing (136), we find

$$(139) \quad [(b + b' + b'')^n = \frac{1}{2}(n-1)(n-2)b_n + \frac{3}{2}n(n-2)b_{n-1} + n(n-1)b_{n-2}.$$

Repeated application of (135) gives easily

$$(140) \quad \left[(b + b' + \dots + b^{(r)})^n = (-1)^r \frac{1}{r!} n(n-1)(n-2) \dots (n-r) \sum_{i=0}^r \sigma_{ri} \frac{b_{n-i}}{n-i}, \right.$$

where the σ_{ri} are the elementary symmetric functions of the numbers 1, 2, 3, \dots , r , taken i at a time⁽²⁰⁾.

⁽²⁰⁾ This result is due to Lucas, *Bulletin de la Société Mathématique de France*, vol. 6 (1877), pp. 57-68. The proof given here is due to Dr. A. M. Mood. The proof of relation (144) was found independently by the writer.

Suppose $n \leq r$ in (140); then all the terms will be zero except the one for $i = n$, hence

$$\left[(b + b' + b^{(r)})^n = (-1)^r \frac{n!}{r!} (-1)^{r-n} (r-n)! \sigma_{rn}, \right.$$

hence

$$(141) \quad \sigma_{rn} = (-1)^n C_{r,n} (b + b' + \dots + b^{(r)})^n.$$

This gives another form for (148) as follows:

$$(142) \quad \left[(b + b' + \dots + b^{(r)})^n \right. \\ \left. = (-1)^r \frac{1}{r!} n(n-1) \dots (n-r) \sum_{i=0}^r (-1)^i C_{r,i} \left[(b + b' + \dots + b^{(r)})^i \frac{b_{n-i}}{n-i} \right]. \right.$$

UNIVERSITY OF TEXAS,
AUSTIN, TEXAS.