BERNOULLI NUMBERS*

L. CARLITZ
Duke University, Durham, North Carolina

1. INTRODUCTION

The purpose of this paper is to discuss some of the properties of the Bernoulli and related numbers and to indicate the relationship of these numbers to cyclotomic fields. We shall use the notation of Nörlund [25].

The Bernoulli numbers may be defined by means of

$$\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} B_n \frac{x^n}{n!} \qquad (|x| < 2\pi) \quad . \tag{1.1}$$

This is equivalent to

$$\sum_{r=0}^{n} \binom{n}{r} B_r = B_n \quad (n > 1) \, . \tag{1.2}$$

together with $B_0 = 1$.

It is convenient to write (1.2) in the following symbolic form:

$$(B + 1)^n = B^n \qquad (n > 1) \tag{1.3}$$

where it is understood that after expansion of the left member we replace B^k by B_k.

We next define the Bernoulli polynomial $B_n(a)$ by means of

$$\frac{xe^{ax}}{e^x - 1} = \sum_{n=0}^{\infty} B_n(a) \frac{x^n}{n!} \quad . \tag{1.4}$$

It follows that

*Supported in part by NSF Grant GP 1593.

$$B_n(a) = \sum_{r=0}^{n} \binom{n}{r} B_r a^{n-r} \tag{1.5}$$

or symbolically

$$B_n(a) = (B + a)^n \ . \tag{1.6}$$

Moreover, we have from (1.4)

$$B_n(0) = B_n \ , \tag{1.7}$$

$$B_n(a + 1) - B_n(a) = na^{n-1} \ , \tag{1.8}$$

$$B_n'(a) = nB_{n-1}(a) \ . \tag{1.9}$$

The polynomial $B_n(a)$ is uniquely determined by means of (1.7) and (1.8). Additional properties of interest are

$$B_n(1 - a) = (-1)^n B_n(a) \tag{1.10}$$

and the multiplication theorem.

$$B_n(ka) = k^{n-1} \sum_{s=0}^{k-1} B_n\left(a + \frac{s}{k}\right) \tag{1.11}$$

valid for all integral $k \geq 1$. Nielsen [24] has observed that if a polynomial $f_n(a)$ satisfies

$$f_n(ka) = k^{n-1} \sum_{s=0}^{k-1} f_n\left(a + \frac{s}{k}\right)$$

for some $k > 1$ then we have

$$f_n(a) = C_n \cdot B_n(a) ,$$

where C_n is independent of a.

It is not difficult to show that

$$B_{2n+1} = 0 \quad (n > 0) \tag{1.12}$$

and that

$$(-1)^{n-1}B_{2n} > 0 \quad (n > 0) . \tag{1.13}$$

The Euler numbers E_n may be defined by means of

$$\frac{2}{e^x + e^{-x}} = \sum_{n=0}^{\infty} E_n \frac{x^n}{n!} , \tag{1.14}$$

which is equivalent to

$$(E + 1)^n + (E - 1)^n = \begin{cases} 2 & (n = 0) \\ 0 & (n > 0) \end{cases} . \tag{1.15}$$

It follows that

$$E_{2n+1} = 0 \quad (n \geq 0) \tag{1.16}$$

while

$$(-1)^n E_{2n} > 0 \quad (n \geq 1) ; \tag{1.17}$$

the E_{2n} are odd integers.

The Euler polynomial $E_n(a)$ is defined by means of

$$\frac{2e^{ax}}{e^x + 1} = \sum_{n=0}^{\infty} E_n(a) \frac{x^n}{n!} \tag{1.18}$$

It follows that

$$E_n = 2^n E_n(1/2) \tag{1.19}$$

Clearly

$$E_n(a+1) + E_n(a) = 2a^n \tag{1.20}$$

Corresponding to (1.10) and (1.11) we have

$$E_n(1-a) = (-1)^n E_n(a) , \tag{1.21}$$

$$E_n(kx) = k^n \sum_{s=0}^{k-1} (-1)^s E_n\left(a + \frac{s}{k}\right) \quad (k \text{ odd}) , \tag{1.22}$$

$$E_n(kx) = \frac{-2k^n}{n+1} \sum_{s=0}^{k-1} (-1)^s E_{n+1}\left(a + \frac{s}{k}\right) \quad (k \text{ even}) . \tag{1.23}$$

2. THE STAUDT-CLAUSEN THEOREM

The B_n are rational numbers, as is evident from the definition. The denominator of B_{2n} is determined by the following remarkable theorem.

Theorem 1. We have, for $n \geq 1$,

$$B_{2n} = G_{2n} - \sum_{p-1 \mid 2n} \frac{1}{p} , \tag{2.1}$$

where G_{2n} is an integer and the summation on the right is over all primes p (including 2) such that $p - 1$ divides $2n$.

For example, we have

$$B_2 = \frac{1}{6} = 1 - \frac{1}{2} - \frac{1}{3} , \quad B_4 = \frac{-1}{30} = 1 - \frac{1}{2} - \frac{1}{3} - \frac{1}{5} ,$$

$$B_6 = \frac{1}{42} = 1 - \frac{1}{2} - \frac{1}{3} - \frac{1}{7} .$$

We shall sketch a proof of Theorem 1. It follows from (1.1) that

$$B_n = \sum_{k=0}^{n} \frac{1}{k+1} \sum_{s=0}^{k} (-1)^s \binom{k}{s} s^n \,. \tag{2.2}$$

Now it is familiar that

$$\frac{1}{k!} \sum_{s=0}^{k} (-1)^{k-s} \binom{k}{s} s^n$$

is an integer (Stirling number of the second kind). Thus (2.2) becomes

$$B_n = \sum_{k=0}^{n} \frac{k!}{k+1} c(n,k) \,,$$

where $c(n,k)$ is an integer. In the next place if $a \geq 2$, $b \geq 2$, $ab > 4$, we can easily verify that $(ab-1)!/ab$ is integral. Hence in the right member of (2.2) it is only necessary to consider $k = 4$ and k equal to a prime p. Since

$$\sum_{s=0}^{p-1} (-1)^s \binom{p-1}{s} s^n \equiv \sum_{s=0}^{p-1} s^n$$

$$\equiv \begin{cases} -1 \pmod p & (p-1 \mid n, \ n > 0) \\ 0 \pmod p & (p-1 \nmid n) \,, \end{cases}$$

(2.2) reduces to

$$B_{2n} = G'_{2n} - \sum_{p-1 \mid 2n}{}' \frac{1}{p} + \frac{1}{4} \sum_{s=0}^{3} (-1)^s \binom{3}{s} s^{2n} \,, \tag{2.3}$$

where G'_{2n} is an integer. But

$$\sum_{s=0}^{3}(-1)^s \binom{3}{s} s^{2n} \equiv -3 - 3^{2n} \equiv 0 \pmod 4$$

so that (2.3) reduces to (2.1).

Hurwitz [12] has proved the following elegant analog of the Staudt-Clausen theorem. Let $\zeta(u)$ be the lemniscate function defined by means of

$$\zeta'^2(u) = 4\zeta^3(u) - 4\zeta(u) . \tag{2.4}$$

We may put

$$\zeta(u) = \frac{1}{u^2} + \sum_{1} \frac{2^{4n}E_n}{4n} \frac{u^{4n-2}}{(4n-2)!} \tag{2.5}$$

(The E_n in (2.5) should not be confused with the Euler number defined by (1.14).) Corresponding to (2.1) we have

$$E_n = G_n + \frac{1}{2} + \frac{(2a)^{4n/(p-1)}}{p} , \tag{2.6}$$

where G_n is an integer and the sum on the right is over all primes $p \equiv 1 \pmod 4$ such that $p - 1$ divides $4n$; moreover, a is uniquely determined by means of

$$p = a^2 + b^2, \quad a \equiv b + 1 \pmod 4 .$$

Hurwitz's proof makes use of the complex multiplication of the function $\zeta(u)$. However the present writer [7] has proved the following generalized Staudt-Clausen theorem in an elementary manner.

Put

$$f(x) = \sum_{n=1}^{\infty} a_n x^n/n! \quad (a_1 = 1) , \tag{2.7}$$

where the a_n are arbitrary rational integers and assume that the inverse function is of the type

$$\lambda(x) = \sum_{n=1}^{\infty} c_n x^n / n \qquad (c_1 = 1), \tag{2.8}$$

where the c_n are integers. Note that the denominator in (2.8) is n, not n!. Now put

$$\frac{x}{f(x)} = \sum_{0}^{\infty} \beta_n x^n / n! \ . \tag{2.9}$$

Then we have

$$\beta_n = G_n - \sum_{p-1 \mid n} \frac{1}{p} c_p^{n/(p-1)} \ , \tag{2.10}$$

where G_n is integral and the summation is over all primes p such that p - 1 divides n.

When $f(x) = e^x - 1$, $\lambda(x) = \log(1 + x)$, (2.10) reduces to (2.1).

3. KUMMER'S CONGRUENCES

Kummer obtained certain congruences for both the Bernoulli and Euler numbers that are of considerable importance in applications. We state first the result for Euler numbers.

Theorem 2. Let $r \geq 1$, $n \geq r$ and let p denote an arbitrary odd prime. Then

$$\sum_{s=0}^{r} (-1)^s \binom{r}{s} E_{n+s(p-1)} \equiv 0 \pmod{p^r} \ . \tag{3.1}$$

A more general result is contained in Theorem 3. Let $r \geq 1$, $e \geq 1$, $n \geq re$ and put $w = p^{e-1}(p-1)$, where p is an odd prime. Then

$$\sum_{s=0}^{r} (-1)^s \binom{r}{s} E_{n+sw} \equiv 0 \pmod{p^{re}}. \tag{3.2}$$

For the Bernoulli numbers we have Theorem 4. Let $r \geq 1$, $e \geq 1$, $n > re$ and put $w = p^{e-1}(p-1)$, where p is a prime such that $p - 1 \nmid n$. Then

$$\sum_{s=0}^{r} (-1)^s \binom{r}{s} \frac{B_{n+sw}}{n+sw} \equiv 0 \pmod{p^{re}}. \tag{3.3}$$

For proof of these theorems see Nielsen [24, Ch. 14] or Bachmann [26]. Note that $p = 2$ is excluded in Theorems 2 and 3. Frobenius [9] has proved a result for the case $p = 2$. There is a fallacious proof in Bachmann's book.

Vandiver [19] obtained a result like (3.3) without the denominator $n + sw$ but under more restrictive hypotheses. He proved that

$$\sum_{s=0}^{r} (-1)^s \binom{r}{s} B_{(a+s)(p-1)} \equiv 0 \pmod{p^{r-1}}, \tag{3.4}$$

where

$$a > 0, \quad r > 0, \quad a + r \leq p - 1.$$

For more general results in this direction see [3].

The quotient B_n/n occurring in (3.3) is integral (mod p) provided $p - 1 \nmid n$. More precisely we state

Theorem 5. If p is prime and $p - 1 \nmid 2n$, $p^r \mid n$ then the numerator of B_{2n} is divisible by p^r.

The case $p - 1 \mid 2n$ is covered by the following supplementary theorem.

Theorem 6. Let $p^r (p-1) \mid n$. Then p^r divides the numerator of

$$B_{2n} + \frac{1}{p} - 1 .$$

For proof of Theorem 6, see [3].

4. RECURRENCES

In addition to the fundamental recurrence (1.2), the B_n satisfy many more recurrences. Many are derived in Nielsen's book. The following two occur in a paper by D. H. Lehmer [13].

$$\sum_{r=0}^{n} \binom{6n+3}{6r} B_{6r} = 2n + 1 , \tag{4.1}$$

$$\sum_{r=0}^{n} \binom{6n+5}{6r+2} B_{6r+2} = \frac{1}{3}(6n+5) . \tag{4.2}$$

In all the known recurrences the number of terms is of order An, where A is a positive constant. Thus it is of interest to ask whether B_n can satisfy a relation of the form

$$\sum_{r=0}^{k} A_r(n) B_{n-r} = A(n) ,$$

where the $A_j(n)$ and $A(n)$ satisfy certain restrictions and k is independent of n.

We may state

Theorem 7. The equation

$$\sum_{r=0}^{k} A_r(n) B_{n-r} = A(n) \quad (n > No) \tag{4.3}$$

where $A_0(n)$ is a polynomial in n with integral coefficients, $A_1(n), \cdots, A_k(n)$, $A(n)$ are arbitrary integral-valued functions of n and k is independent of n, is impossible.

Theorem 8. The equation

$$\sum_{r=0}^{k} A_r(n)E_{n-r} = A(n) \qquad (n > No), \tag{4.4}$$

where $A_0(n)$, $A_1(n)$, $\cdots$, $A_k(n)$, $A(n)$ are polynomials in n with integral coefficients and k is independent of n, is impossible.

Theorem 7 is proved by means of the Staudt-Clausen Theorem; Theorem 8 by means of Kummer's Congruences. For these and more general results, see [5], [6].

5. IRREGULAR PRIMES

A prime p is said to be regular if it does not divide the numerator of any of the numbers

$$B_2, B_4, \cdots, B_{p-3}. \tag{5.1}$$

The prime p is irregular if it does divide the numerator of at least one of the numbers (5.1). The motivation for these definitions will appear presently.

The first few irregular primes are

37, 59, 67, 101, 103, 131, 149, 157, 233, 257, 263, 271, 283, 293.

It might appear that the irregular primes are relatively rare. Actually, it is not known whether infinitely many regular primes exist. In the opposite direction we have

Theorem 9. The number of irregular primes is infinite.

This theorem is due to Jensen; for the proof see [23, p. 82]. A simpler proof is given in [2]. Jensen proved a slightly stronger result, namely that there exist infinitely many irregular primes congruent to 5 (mod 6). This result has very recently been improved by Montgomery [14].

Theorem 10. Let T be a fixed integer >2. Then there exist infinitely many irregular primes that are not congruent to 1 (mod T).

Paralleling the above definition, we may say that a prime p is irregular relative to the Euler numbers provided it divides at least one of the Euler numbers

$$E_2, E_4, \cdots, E_{p-3}. \tag{5.2}$$

Theorem 11. There exist inifinitely many primes that are irregular relative to the Euler numbers.

For proof see [2]. Here again nothing is known about the number of regular primes relative to the Euler numbers. Also it is not known how the two kinds of regular primes are related.

6. CONNECTION WITH CLASS NUMBERS AND FERMAT'S LAST THEOREM

Let p denote a fixed odd prime and put $\zeta = e^{2\pi i/p}$. Let $h = h(\zeta)$ denote the class number of the cyclotomic field $Q(\zeta)$. It is customary to put

$$h = AB; \tag{6.1}$$

A is called the first factor of the class number and B is called the second factor. The number B appears as the quotient of two determinants involving logarithms of units; it is equal to the class number of the real field $Q(\zeta + \zeta^{-1})$.

It is of considerable interest to know when h is divisible by p. We have the following criterion.

Theorem 12. The class number of $Q(\zeta)$ is divisible by p if and only if p is irregular.

It can be proved that if p divides B then necessarily p divides A. This yields

Theorem 13. $p|h \Leftrightarrow p|A$.

Vandiver [18] has proved

Theorem 14. Let $n \geq 1$. Then A satisfies

$$A \equiv 2^{-1/2(p-3)} p \prod_{s} B_{sp^n+1} \pmod{p^n}, \tag{6.2}$$

where the product is over $s = 1, 3, 5, \cdots, p - 2$.

When $n = 1$, (6.2) reduces to

$$A \equiv 2^{-1/2(p-3)} p \prod_s B_{sp+1} \pmod{p} \quad .$$

Now by Theorem 4 with $r = 1$ we have

$$\frac{B_{sp+1}}{sp+1} = \frac{B_{s+1}}{s+1} \pmod{p} \quad (1 \leq s < p - 2) ;$$

for $s = p - 2$ we have by the Staudt-Clausen Theorem

$$pB_{p(p-2)+1} = pB_{(p-1)^2} \equiv -1 \pmod{p} \quad .$$

Thus (6.2) reduces to

$$A \equiv \frac{-4}{(1/2(p-3))!} \prod_{s=1}^{1/2(p-3)} B_{2s} \pmod{p}. \tag{6.3}$$

Kummer has proved the following result concerning Fermat's last theorem.

Theorem 15. If p is regular the equation

$$\alpha^p + \beta^p + \nu p = 0 \quad (\alpha, \beta, \nu \in Q(\zeta)) \tag{6.4}$$

has only the trivial solution $\alpha = \beta = \nu = 0$.

Nicol, Selfridge and Vandiver [16] have proved that Fermat's last theorem holds for prime exponents less than 4002.

The equation (in rational integers)

$$x^p + y^p + z^p = 0 \qquad (p \nmid xyz) \tag{6.5}$$

is known as the first case of Fermat's last theorem.

It has been proved that if (6.5) is satisfied then

$$2^p \equiv 2 \pmod{p^2} \tag{6.6}$$

and

$$3^p \equiv 3 \pmod{p^2} \tag{6.7}$$

Indeed considerably more is known in this direction.

It has also been proved that if (6.5) holds then

$$B_{p-3} \equiv B_{p-5} \equiv B_{p-7} \equiv B_{p-9} \equiv 0 \pmod{p}. \tag{6.8}$$

Finally we state some criteria involving the Euler numbers. Vandiver [20] has proved that if (6.5) is satisfied then

$$E_{p-3} \equiv 0 \pmod{p}. \tag{6.9}$$

M. Gut [10] has proved that if

$$x^{2p} + y^{2p} = z^{2p} \quad (p \nmid xyz) \tag{6.10}$$

is satisfied, then

$$E_{p-3} \equiv E_{p-5} \equiv E_{p-7} \equiv E_{p-9} \equiv E_{p-11} \equiv 0 \pmod{p}. \tag{6.11}$$

7. CONCLUDING REMARKS

The references that follow include mainly papers that have been referred to above. Vandiver in his expository paper [22] remarks that some 1500 papers on Bernoulli numbers have been published!

For Fermat's last theorem, the reader is referred to Vandiver's expository paper [21] as well as Dickson [8], Hilbert [11] and Vandiver-Wahlin [23].

For the Euler numbers and related matters see Salie [17].

We conclude with some remarks about real quadratic fields. Let p be a prime $\equiv 1 \pmod 4$ and let $E = 1/2(t + u\sqrt{p}) > 1$ denote the fundamental unit of $Q(\sqrt{p})$. Ankeny, Artin and Chowla [1] have conjectured that $u \not\equiv 0 \pmod p$; Mordell [15] has proved the following results:

(1) If p is regular then $u \not\equiv 0 \pmod p$.

(2) If $p \equiv 5 \pmod 8$ then $u \equiv 0 \pmod p$ if and only if $B_{(p-1)}/2 \equiv 0 \pmod p$. Chowla had proved (2) for all $p \equiv 1 \pmod 4$.

REFERENCES

1. N. C. Ankeny, E. Artin and S. Chowla, "The Class Numbers of Real Quadratic Number Fields," Annals of Mathematics (2), Vol. 56 (1952), pp. 479-493.
2. L. Carlitz, "A Note on Irregular Primes," Proceedings of the American Mathematical Society, Vol. 5 (1954), pp. 329-331.
3. L. Carlitz, "Some Congruences for the Bernoulli Numbers," American Journal of Mathematics, Vol. 75 (1953), pp. 163-172.
4. L. Carlitz, "The Staudt-Clausen Theorem," Mathematics Magazine, Vol. 34 (1961), pp. 131-146.
5. L. Carlitz, "Recurrences for the Bernoulli and Euler Numbers," Journal für die reine und angawandte Mathematik, Vol. 215/215 (1964), pp. 184-191.
6. L. Carlitz, "Recurrences for the Bernoulli and Euler Numbers," Mathematische Nachrichten, Vol. 29 (1965), pp. 151-160.
7. L. Carlitz, "The Coefficients of the Reciprocal of a Series," Duke Mathematical Journal, Vol. 8 (1941), pp. 689-700.
8. L. E. Dickson, History of the Theory of Numbers, Vol. 2, Stechert, New York.
9. G. Frobenius, Über die Bernoullischen Zahlen und die Eulerschen Polynome, Berliner Sitzungsberichte, 1910, pp. 809-847.
10. M. Gut, "Eulersche Zahlen und grosser Fermat'scher Satz," Commentarii Math. Helvetici, Vol. 24 (1950), pp. 73-99.
11. D. Hilbert, "Die Theorie der Algebraischen Zahlkörper," Jahresbericht der Deutscher Mathematiker-Vereinigung, Vol. 4 (1894-95), pp. 517-525.
12. A. Hurwitz, "Über die Entwickelungs Coeffizienten der Lemniscatischen Functionen," Mathematische Annalen, Vol. 51 (1898), pp. 196-226 (Mathematische Werke, 1933, II, pp. 342-373).
13. D. H. Lehmer, "Lacunary Recurrences for the Bernoulli Numbers," Annals of Mathematics (2), Vol. 36 (1935), pp. 637-649.
14. H. L. Montgomery, "Distribution of Irregular Primes," Illinois Journal of Mathematics, Vol. 9 (1965), pp. 553-558.

15. L. J. Mordell, "On a Pellian Equation Conjecture," Acta Arithmetica, Vol. 6 (1960), pp. 137-144.
16. C. A. Nichol, J. L. Selfridge, H. S. Vandiver, "Proof of Fermat's Last Theorem for Exponents Less than 4002," Proceedings of the National Academy of Sciences, Vol. 41 (1955), pp. 970-973.
17. H. Salie, "Eulersche Zahlen, Sammelband zu Ehren des 250. Geburtstages Leonhard Eulers," pp. 293-319. Akademie-Verlag, Berlin, 1959.
18. H. S. Vandiver, "On the First Factor of the Class Number of a Cyclotomic Field," Bulletin of the American Mathematical Society, Vol. 25 (1918), pp. 458-461.
19. H. S. Vandiver, "Certain Congruences Involving the Bernoulli Numbers," Duke Mathematical Journal, Vol. 5 (1939), pp. 548-551.
20. H. S. Vandiver, "Note on Euler Number Criteria for the First Case of Fermat's Last Theorem," American Journal of Mathematics, Vol. 62 (1940), pp. 79-82.
21. H. S. Vandiver, "Fermat's Last Theorem," American Mathematical Monthly, Vol. 53 (1946), pp. 555-578.
22. H. S. Vandiver, "On Developments in an Arithmetic Theory of the Bernoulli and Allied Numbers," Scripta Mathematica, Vol. 25 (1960), pp. 273-303.
23. H. S. Vandiver and G. E. Wahlin, "Algebraic Numbers," Bulletin of the National Research Council, No. 62, 1928.
24. N. Nielsen, Traité élémentaire des nombres de Bernoulli, Paris, 1923.
25. N. E. Nörlund, Vorlesungen über Differenzenrechnung, Berlin, 1924.
26. P. Bachmann, Niedere Zahlentheorie, Leipzig, 1892.
27. E. Landau, Vorlesungen über Zahlentheorie, Vol. 3, Leipzig, 1927.

* * * * *

BELATED ACKNOWLEDGEMENT

The first use of the Q-matrix to generate the Fibonacci Numbers appears in an abstract of a paper by Professor J. L. Brenner by the title "Lucas' Matrix." This abstract appeared in the March, 1951 American Mathematical Monthly on pages 221 and 222. The basic exploitation of the Q-matrix appeared in 1960 intthe San Jose State College Master's thesis of Charles H. King with the title 'Some Further Properties of the Fibonacci Numbers. Further utilization of the Q-matrix appears in the Fibonacci Primer sequence parts I-V.

Verner E. Hoggatt, Jr.