ON LUCAS-BERNOULLI NUMBERS

Paul Thomas Young

Department of Mathematics, College of Charleston, Charleston, SC 29424

e-mail: paul@math.cofc.edu

(Submitted February 2005-Final Revision October 2005)

ABSTRACT

In this article we investigate the Bernoulli numbers $\hat{B}_n$ associated to the formal group laws whose canonical invariant differentials generate the Lucas sequences $\{U_n\}$ and $\{V_n\}$. We give explicit expressions for these numbers and prove analogues of Kummer congruences for them.

1. INTRODUCTION

The Bernoulli numbers B_n are the rational numbers defined by the generating function

$$\frac{t}{e^t-1}=\sum_{n=0}^{\infty} B_n \frac{t^n}{n!}. \tag{1.1}$$

Among the many important properties of these numbers are the Kummer congruences, a strong form of which read as follows: Let p be an odd prime, assume that $p-1$ does not divide m, and that $(p-1)p^a$ divides c for some $a \geq 0$. Then for all $k \geq 0$,

$$\sum_{j=0}^{k}(-1)^{k-j}\binom{k}{j}\frac{B_{m+jc}}{m+jc} \equiv 0 \qquad (\bmod\ p^A\mathbb{Z}_{(p)}), \tag{1.2}$$

where $A=\min\{m-1, k(a+1)\}$ and $\mathbb{Z}_{(p)}$ denotes the ring of rational numbers with denominator relatively prime to p (cf. [2]).

The Bernoulli numbers have been generalized in many ways, and analogues of the congruences (1.2) hold for many of these generalizations ([1], [6], [8]). For one type of generalization, let $c_1, c_2, ...$ be indeterminates and consider the formal power series

$$\lambda(t)=t+\sum_{i=1}^{\infty} c_i \frac{t^{i+1}}{i+1} \tag{1.3}$$

in $\mathbb{Q}[c_1, c_2, ...][[t]]$. Let ε denote the formal compositional inverse of λ in $\mathbb{Q}[c_1, c_2, ...][[t]]$, and define the *universal Bernoulli numbers* $\hat{B}_n$ in $\mathbb{Q}[c_1, c_2, ...]$ by

$$\frac{t}{\varepsilon(t)}=\sum_{n=0}^{\infty} \hat{B}_n \frac{t^n}{n!} \tag{1.4}$$

(cf. [3]). In this generalization each $\hat{B}_n$ is actually a polynomial of degree n in $c_1, c_2, ..., c_n$ with rational coefficients. Recently Adelberg [1] has proved that if $c=l(p-1)$ where p^a divides l, $m \geq a+2$, and $m \not\equiv 0, 1 \pmod{p-1}$, then

$$\frac{\hat{B}_{m+c}}{m+c}-c_{p-1}^{l}\frac{\hat{B}_m}{m} \equiv 0 \qquad (\bmod\ p^{a+1}\mathbb{Z}_{(p)}[c_1, c_2, ...]), \tag{1.5}$$

whereas if $m \equiv 1 \pmod{p-1}$ and $m \geq a+2$ then

$$\frac{\hat{B}_{m+c}}{m+c} - c_{p-1}^{l} \frac{\hat{B}_m}{m} \equiv c_{p-1}^{l+q-2} \left(c_{p-1} c_1^p - c_{2p-1}\right) l/2 \qquad \left(\mathrm{mod}\ p^{a+1}\mathbb{Z}_{(p)}[c_1, c_2, ...]\right) \tag{1.6}$$

where $q = (m-1)/(p-1)$. Note that (1.5) is similar to the $k=1$ case of (1.2). The analogy may be seen by mapping $c_i \mapsto (-1)^i$ in (1.3), so $\lambda(t) \mapsto \log(1+t)$ and in turn $\varepsilon(t) \mapsto e^t - 1$, whence $\hat{B}_n \mapsto B_n$ by comparison of (1.4) with (1.1).

In this paper we examine the rational numbers $\hat{B}_n$ obtained in (1.4) by mapping $c_i \mapsto U_{i+1}$ or $c_i \mapsto V_{i+1}$ in (1.3), where $\{U_n\}$ and $\{V_n\}$ are Lucas sequences of the first and second kind. We will call the numbers $\hat{B}_n$ thus obtained *Lucas-Bernoulli numbers.* We'll give congruences analogous to (1.2), and stronger than the general congruences (1.5), (1.6) for these numbers. Specifically, we show that if p is an odd prime, $p-1$ does not divide m, and the increment $c = l(p-1)$ where p^a divides l for some $a \geq 0$, then for all $k \geq 0$,

$$\sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} c_{p-1}^{(k-j)l} \frac{\hat{B}_{m+jc}}{m+jc} \equiv 0 \qquad \left(\mathrm{mod}\ p^A \mathbb{Z}_{(p)}\right), \tag{1.7}$$

where $A = \min\{m-1, k(a+1)\}$. One may use the explicit formula ([1], eq. (3.1)) for the polynomials $\hat{B}_n/n$ in terms of the indeterminates c_i to express the congruences (1.7) as nonstandard congruences for the Lucas numbers U_n, V_n.

The polynomials $\hat{B}_n \in \mathbb{Q}[c_1, c_2, ...]$ defined in (1.4) are called universal Bernoulli numbers because the power series λ in (1.3) is the formal logarithm of the *universal formal group law* ([3], [5]). It appears to us that the congruences (1.2), (1.7) one obtains for the specializations $c_i \mapsto (-1)^i$, $c_i \mapsto U_{i+1}$, or $c_i \mapsto V_{i+1}$ are stronger than those in (1.5), (1.6) because these specializations make λ into the logarithm of an *integral* formal group law, whereas the universal formal group law is not integral. These considerations are discussed in section 5 below.

2. PRELIMINARIES

Let P and Q be integers, and define sequences $\{U_n\}$ and $\{V_n\}$ by the recurrences

$$U_n = PU_{n-1} - QU_{n-2}, \quad V_n = PV_{n-1} - QV_{n-2}, \tag{2.1}$$

with initial conditions $U_0 = 0$, $U_1 = 1$, $V_0 = 2$, $V_1 = P$. Then $r(t) = 1 - Pt + Qt^2$ is the characteristic polynomial of the recurrence for either $\{U_n\}$ or $\{V_n\}$, with discriminant $D = P^2 - 4Q$. If $r(t)$ factors as $r(t) = (1-\alpha t)(1-\beta t)$ then $\alpha = (P+\sqrt{D})/2$ and $\beta = (P-\sqrt{D})/2$, so that $\alpha - \beta = \sqrt{D}$, and for all n we have

$$V_n = \alpha^n + \beta^n, \qquad U_n = \frac{1}{\sqrt{D}}(\alpha^n - \beta^n), \tag{2.2}$$

unless $D = 0$, in which case $U_n = n\alpha^{n-1}$. These sequences may be generated by the differential forms

$$\frac{dt}{r(t)} = \sum_{n=1}^{\infty} U_n t^n \frac{dt}{t}, \qquad \frac{dr}{r} = -\sum_{n=1}^{\infty} V_n t^n \frac{dt}{t}. \tag{2.3}$$

We will make use of two well-known congruence properties of these numbers (cf. [7]): For any prime p we have

$$U_p \equiv (D|p) \pmod{p}, \qquad \text{and} \qquad V_p \equiv P \pmod{p}, \tag{2.4}$$

where $(D|p)$ is the Legendre symbol. See (5.6), (5.7) for more general versions of (2.4).

Throughout this paper p will denote a prime number, $\mathbb{Z}_p$ the ring of p-adic integers and $\mathbb{Z}_{(p)}$ the ring of rational numbers whose denominator is relatively prime to p, so that $\mathbb{Z}_p \bigcap \mathbb{Q} = \mathbb{Z}_{(p)}$. All our congruences involve rational numbers and are stated in $\mathbb{Z}_{(p)}$, but we often work in $\mathbb{Z}_p$ rather than $\mathbb{Z}_{(p)}$ because $\mathbb{Z}_p$ is complete. A congruence $x \equiv y \pmod{p^A\mathbb{Z}_{(p)}}$ means that $x-y$ is a rational number whose numerator is divisible by p^A. If R is a commutative ring with identity then $R^\times$ will denote its multiplicative group of units and $R[[X]]$ will denote the ring of formal power series in the indeterminate X over R. Recall that a formal power series f is a unit in $R[[X]]$ if and only if the constant term of f is a unit in R, and that f has a compositional inverse in $R[[X]]$ if and only if f has constant term zero and linear coefficient in $R^\times$. The binomial expansion

$$(1+y)^a = \sum_{k=0}^{\infty} \binom{a}{k} y^k \tag{2.5}$$

will be invoked in several contexts. First, if $a \in \mathbb{Z}_p$ and $y \in p\mathbb{Z}_p$ then the series (2.5) converges in $\mathbb{Z}_p$; therefore if $x \equiv 1 \pmod{p\mathbb{Z}_p}$ and $a \in \mathbb{Z}_p$ then $x^a \in \mathbb{Z}_p$ as well. Second, if $a \in R$ and $y \in XR[[X]]$ is a power series with constant term zero then (2.5) makes sense in $R[[X]]$; thus if $f \in R[[X]]$ has constant term 1, then $f^a \in R[[X]]$ for any $a \in R$.

If c is a nonnegative integer, the difference operator Δ_c with increment c operates on the sequence $\{a_m\}$ by

$$\Delta_c\, a_m = a_{m+c} - a_m. \tag{2.6}$$

The powers Δ_c^k of Δ_c are defined by $\Delta_c^0 =$ identity and $\Delta_c^k = \Delta_c \circ \Delta_c^{k-1}$ for positive integers k, so that

$$\Delta_c^k\, a_m = \sum_{j=0}^{k} \binom{k}{j} (-1)^{k-j} a_{m+jc} \tag{2.7}$$

for all nonnegative integers k. Thus for example the congruences (1.2) may be expressed as $\Delta_c^k\{B_m/m\} \equiv 0 \pmod{p^A\mathbb{Z}_{(p)}}$. The calculations in our proof of the congruences (1.7) are primarily based on two principles. One is the identity

$$\Delta_c^k\{X_mY_m\} = \sum_{i=0}^{k} \binom{k}{i} \Delta_c^i\{X_m\}\Delta_c^{k-i}\{Y_{m+ic}\}, \tag{2.8}$$

([8], eq. (5.38)). The other is Theorem 1.1 of [8], which states that if $h \in \mathbb{Z}_p[[T-1]]$ and $h(e^t) = \sum_{n=0}^{\infty} a_n t^n/n!$ then for $c \equiv 0 \pmod{(p-1)p^a}$ we have $\Delta_c^k a_m \equiv 0 \pmod{p^A\mathbb{Z}_p}$ for all $k \geq 0$, where $A = \min\{m, k(a+1)\}$.

3. LUCAS-BERNOULLI NUMBERS OF THE FIRST KIND

In this section we show that the numbers $\hat{B}_n$ obtained by specializing $c_i \mapsto U_{i+1}$ may be expressed in terms of the usual Bernoulli numbers B_n, and prove the congruences (1.7) for these numbers.

Theorem 3.1: *Let $\hat{B}_n$ denote the numbers obtained in (1.4) by specializing $c_i \mapsto U_{i+1}$ in (1.3). Then for all n,*

$$\hat{B}_n = \sqrt{D}^n B_n + \alpha\delta_{1,n}$$

where $\delta_{i,j}$ is the Kronecker delta. For even $n > 0$ the denominator of $\hat{B}_n$ is equal to the product of those primes p not dividing D such that $p-1$ divides n.

Proof: Following (2.3), let

$$\omega = \frac{dt}{r(t)} = \sum_{n=1}^{\infty} U_n t^{n-1}\,dt, \qquad \text{so} \qquad \lambda(t) = \int_0^t \omega = \sum_{n=1}^{\infty} U_n \frac{t^n}{n} \tag{3.1}$$

agrees with (1.3). If $D = 0$ then $\lambda(t) = t/(1-\alpha t)$, whereas if $D \neq 0$ then

$$\lambda(t) = \frac{1}{\sqrt{D}} \log\left(\frac{1-\beta t}{1-\alpha t}\right). \tag{3.2}$$

Therefore if $D = 0$, the compositional inverse ε of λ satisfies $\varepsilon(t) = t/(1+\alpha t)$, and if $D \neq 0$ then

$$\varepsilon(t) = \frac{1-e^{\sqrt{D}t}}{\beta - \alpha e^{\sqrt{D}t}}. \tag{3.3}$$

So if $D = 0$ then $t/\varepsilon(t) = 1 + \alpha t$, whence $\hat{B}_0 = 1$, $\hat{B}_1 = \alpha$, and $\hat{B}_n = 0$ for $n > 1$. The theorem is thus proven in this case. If $D \neq 0$ then

$$\frac{t}{\varepsilon(t)} = \alpha t + \frac{\sqrt{D}t}{e^{\sqrt{D}t} - 1}, \tag{3.4}$$

and comparison with (1.1) yields the stated identity.

The von Staudt-Clausen theorem (cf. [3]) states that the denominator of B_n is always squarefree, and for even $n > 0$ is in fact equal to the product of those primes p such that $p-1$ divides n. This formula implies that the denominator of the number $\hat{B}_n$ associated to $c_i \mapsto U_{i+1}$ is also squarefree, and for even $n > 0$ is equal to the product of those primes p not dividing D such that $p-1$ divides n. Therefore $\hat{B}_n \in \mathbb{Z}_{(p)}$ for all $n > 1$ when p is a prime dividing D.

Remarks: If we choose $r(t)$ so that its discriminant D is not a square, this formula provides another proof of the well-known facts that $B_1 = -1/2$ and $B_{2k+1} = 0$ for all $k > 0$, since it is clear that both B_n and $\hat{B}_n$ are rational numbers. When $k > 0$ the formula reads $\hat{B}_{2k+1} = \sqrt{D}^{2k+1} B_{2k+1}$, which cannot hold unless both sides are zero. With $n = 1$ we have $\hat{B}_1 = (P/2) + \sqrt{D}(B_1 + (1/2))$, implying $B_1 + (1/2) = 0$, and thus $\hat{B}_1 = P/2$.

The first few values of $\hat{B}_n$ for $c_i \mapsto U_{i+1}$ are $\hat{B}_0 = 1$, $\hat{B}_1 = P/2$, $\hat{B}_2 = D/6$, $\hat{B}_3 = 0$, $\hat{B}_4 = -D^2/30$, $\hat{B}_5 = 0$, $\hat{B}_6 = D^3/42$, $\hat{B}_7 = 0$, $\hat{B}_8 = -D^4/30$, $\hat{B}_9 = 0$, $\hat{B}_{10} = 5D^5/66$. The usual Bernoulli numbers B_n may be obtained in this way by choosing $P = -1$ and $Q = 0$; in this case $U_n = (-1)^{n+1}$ for $n > 0$.

Theorem 3.2: *Let $\hat{B}_n$ denote the numbers obtained in (1.4) by specializing the indeterminates $c_i \mapsto U_{i+1}$ in (1.3). Then if p is an odd prime, $p-1$ does not divide m, and the increment $c = l(p-1)$ where p^a divides l for some $a \geq 0$, then for all $k \geq 0$, the congruence*

$$\sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} c_{p-1}^{(k-j)l} \frac{\hat{B}_{m+jc}}{m+jc} \equiv 0 \qquad \pmod{p^A \mathbb{Z}_{(p)}}$$

given in (1.7) holds, where $A = \min\{m-1, k(a+1)\}$.

Proof: In the case $m = 1$ the left side of the congruence is just $(-1)^k U_p^{kl} P/2$, which lies in $\mathbb{Z}_{(p)}$; the theorem is therefore true in this case. If $m > 1$ is odd, the left side is zero and the theorem is also true in this case. Now assume $m > 1$ is even, which implies $\hat{B}_m = \sqrt{D}^m B_m$ with $\sqrt{D}^m \in \mathbb{Z}$, and therefore the left side of the congruence becomes

$$\sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} U_p^{(k-j)l} \sqrt{D}^{m+jc} \frac{B_{m+jc}}{m+jc}. \tag{3.5}$$

If p divides D then p divides U_p as well by (2.4); therefore the power of p dividing the j-th term in (3.5) is at least $(k-j)l + (m+jc)/2$, which may be written as $kl + (m/2) + jl(p-3)/2$ and is therefore greater than kl. Since p^a divides l, we have $l \geq a+1$ so this exponent is at least $k(a+1)$, proving the theorem in this case.

Finally suppose that p does not divide D, while $m > 1$ is even. In this case (2.4) tells us that $U_p \equiv D^{(p-1)/2} \equiv (D|p) \pmod{p}$. Since $D^{(p-1)/2}/U_p \equiv 1 \pmod{p\mathbb{Z}_p}$, we may expand $(D^{(p-1)/2}/U_p)^{e/(p-1)}$ in $\mathbb{Z}_p$ for any integer e by (2.5). If we take $e = 1$ this defines an element of $\mathbb{Z}_p$ we'll denote by $U_p^{-1/(p-1)}\sqrt{D}$. If $e = 2c$ is even this defines an element of $\mathbb{Z}_p$ we'll denote by $D^c/U_p^{e/(p-1)}$, which in turn defines an element $U_p^{e/(p-1)} \in \mathbb{Z}_p$ such that $(U_p^{e/(p-1)})^{(p-1)} = U_p^e$ and $U_p^{e/(p-1)} \equiv D^c \pmod{p\mathbb{Z}_p}$. The expression (3.5) may then be written as

$$\begin{aligned} U_p^{kl+m/(p-1)} &\sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} (U_p^{-1/(p-1)}\sqrt{D})^{m+jc} \frac{B_{m+jc}}{m+jc} \\ &= U_p^{kl+m/(p-1)} \Delta_c^k \left\{ (U_p^{-1/(p-1)}\sqrt{D})^m \frac{B_m}{m} \right\}. \end{aligned} \tag{3.6}$$

By the identity (2.8), this expression is equal to

$$U_p^{kl+m/(p-1)} \sum_{i=0}^{k} \binom{k}{i} \Delta_c^i \left\{ \frac{B_m}{m} \right\} \Delta_c^{k-i} \left\{ (U_p^{-1/(p-1)}\sqrt{D})^{m+ic} \right\}. \tag{3.7}$$

By (1.2) we have $\Delta_c^i\{B_m/m\} \equiv 0 \pmod{p^{A_i}\mathbb{Z}_{(p)}}$ for $A_i = \min\{m-1, i(a+1)\}$. By the binomial theorem the term $U_p^{kl+m/(p-1)}\Delta_c^{k-i}\{(U_p^{-1/(p-1)}\sqrt{D})^{m+ic}\}$ is equal to

$$\sqrt{D}^{m+ic}U_p^{(k-i)l}\left(\left(\frac{D^{(p-1)/2}}{U_p}\right)^l - 1\right)^{k-i}. \tag{3.8}$$

Since $D^{(p-1)/2} \equiv U_p \pmod p$ we have $(D^{(p-1)/2}/U_p)^l \equiv 1 \pmod{p^{(a+1)}\mathbb{Z}_{(p)}}$, and therefore (3.8) is zero modulo $p^{(k-i)(a+1)}\mathbb{Z}_{(p)}$. Therefore each term in the sum (3.7) is zero modulo $p^A\mathbb{Z}_{(p)}$, proving the theorem.

4. LUCAS-BERNOULLI NUMBERS OF THE SECOND KIND

In this section we express the numbers $\hat{B}_n$ obtained by specializing $c_i \mapsto V_{i+1}$ in terms of the Bernoulli numbers B_n and the Stirling numbers $S(n,k)$ of the second kind, which are defined by the generating function

$$\frac{(e^t-1)^k}{k!} = \sum_{n=k}^{\infty} S(n,k)\frac{t^n}{n!}, \tag{4.1}$$

and use this to prove the congruences (1.7) for these numbers.

Theorem 4.1: *Let $\hat{B}_n$ denote the numbers obtained in (1.4) by specializing $c_i \mapsto V_{i+1}$ in (1.3), where $P = 1$ and Q is an arbitrary integer. Then for all n,*

$$\hat{B}_n = (-1)^n B_n - n\sum_{k=1}^{n}\binom{1/2}{k}2^{2k-1}Q^k(k-1)!S(n-1,k-1).$$

The denominator of $\hat{B}_n$ is equal to the denominator of B_n for all n.

Proof: Following (2.3), let

$$\omega = -\frac{dr}{r} = \sum_{n=1}^{\infty} V_n t^{n-1}\,dt, \qquad \text{so} \qquad \lambda(t) = \int_0^t \omega = \sum_{n=1}^{\infty} V_n\frac{t^n}{n} \tag{4.2}$$

agrees with (1.3), since we assume $P = 1$. It follows that $\lambda(t) = -\log r(t)$, so that its compositional inverse ε satisfies

$$e^{-t} = 1 - \varepsilon(t) + Q\varepsilon(t)^2. \tag{4.3}$$

By the quadratic formula we have

$$\varepsilon(t) = \frac{1-\sqrt{1+4Q(e^{-t}-1)}}{2Q} \tag{4.4}$$

if $Q \neq 0$, whereas $\varepsilon(t) = 1 - e^{-t}$ if $Q = 0$. Observe that the power series $f = 1 + 4Q(e^{-t}-1) \in \mathbb{Q}[[t]]$ has constant term 1, so that $\sqrt{f} = f^{1/2}$ may be expanded by (2.5) as a power series in $\mathbb{Q}[[t]]$, which also has constant term 1; this is the meaning of the square root symbol in (4.4).

The negative sign is chosen for the square root in order that the power series $\varepsilon \in \mathbb{Q}[[t]]$ has constant term zero, so (4.3) makes sense. Therefore for $Q \neq 0$,

$$\frac{t}{\varepsilon(t)} = \frac{2Qt}{1-\sqrt{1+4Q(e^{-t}-1)}} = \frac{-t(1+\sqrt{1+4Q(e^{-t}-1)})}{2(e^{-t}-1)}, \tag{4.5}$$

and the right side of (4.5) is correct even for $Q = 0$.

The identity of the theorem follows by applying the binomial expansion (2.5) to the generating function (4.5), yielding

$$\begin{aligned}\sum_{n=0}^{\infty} \hat{B}_n \frac{t^n}{n!} &= \frac{-t(1+\sqrt{1+4Q(e^{-t}-1)})}{2(e^{-t}-1)} \\ &= \frac{-t}{e^{-t}-1} - \frac{t}{2}\sum_{k=1}^{\infty}\binom{1/2}{k}4^k Q^k (e^{-t}-1)^{k-1} \qquad (4.6)\\ &= \frac{-t}{e^{-t}-1} - \sum_{n=1}^{\infty} n\frac{t^n}{n!}\sum_{k=1}^{n}\binom{1/2}{k}2^{2k-1}Q^k(k-1)!S(n-1,k-1).\end{aligned}$$

Expanding the right side using (1.1) and (4.1) gives the stated identity. Since $k!S(n,k) \in \mathbb{Z}$ we see that $\hat{B}_n - (-1)^n B_n \in n\mathbb{Z}$ for all n; therefore the denominator of $\hat{B}_n$ is always equal to the denominator of B_n.

Remarks: The first few values of $\hat{B}_n$ in this case are $\hat{B}_0 = 1$, $\hat{B}_1 = \frac{1}{2} - Q$, $\hat{B}_2 = \frac{1}{6} - 2Q^2$, $\hat{B}_3 = 3Q^2 - 12Q^3$, $\hat{B}_4 = -\frac{1}{30} - 4Q^2 + 48Q^3 - 120Q^4$, $\hat{B}_5 = 5Q^2 - 140Q^3 + 900Q^4 - 1680Q^5$, $\hat{B}_6 = \frac{1}{42} - 6Q^2 + 360Q^3 - 4500Q^4 + 20160Q^5 - 30240Q^6$. Clearly, if we choose $Q = 0$ then we obtain $\hat{B}_n = (-1)^n B_n$. Although it is not an integer, the choice $Q = 1/4$ gives us $\hat{B}_n = (-2)^{-n} B_n$ for all n.

Theorem 4.2: *Let $\hat{B}_n$ denote the numbers obtained in (1.4) by specializing the indeterminates $c_i \mapsto V_{i+1}$ in (1.3), where $P = 1$ and Q is an arbitrary integer. If p is an odd prime, $p-1$ does not divide m, and the increment $c = l(p-1)$ where p^a divides l for some $a \geq 0$, then for all $k \geq 0$,*

$$\sum_{j=0}^{k}(-1)^{k-j}\binom{k}{j}\frac{\hat{B}_{m+jc}}{m+jc} \equiv 0 \qquad (\mathrm{mod}\ p^A\mathbb{Z}_{(p)}),$$

where $A = \min\{m-1, k(a+1)\}$.

Proof: We define

$$g(T) = \frac{1+\sqrt{1+4Q(T-1)}}{2(T-1)}, \tag{4.7}$$

so that $g(e^t) = -1/\varepsilon(-t)$. Choose a positive integer b such that $(b, p) = 1$, and consider $h(T) = bg(T^b) - g(T)$. We compute

$$h(T) = \frac{1}{2(T-1)}\left[\frac{b(1+\sqrt{1+4Q(T^b-1)})}{\Phi_b(T)} - 1 - \sqrt{1+4Q(T-1)}\right], \tag{4.8}$$

where

$$\begin{aligned} T^b - 1 &= ((T-1)+1)^b - 1 \\ &= b(T-1) + \binom{b}{2}(T-1)^2 + \cdots + (T-1)^b \in \mathbb{Z}_p[[T-1]], \end{aligned} \tag{4.9}$$

and therefore

$$\Phi_b(T) = \frac{T^b-1}{T-1} = b + \binom{b}{2}(T-1) + \cdots + (T-1)^{b-1} \in \mathbb{Z}_p[[T-1]]^\times. \tag{4.10}$$

By (4.9), $T^b - 1$ has no constant term when considered as an element of $\mathbb{Z}_p[[T-1]]$, so both square root terms in (4.8) lie in $\mathbb{Z}_p[[T-1]]$. Furthermore since its constant term b is invertible in $\mathbb{Z}_p$, the polynomial $\Phi_b(T)$ is invertible as an element of $\mathbb{Z}_p[[T-1]]$, and therefore the expression in brackets in (4.8) lies in $\mathbb{Z}_p[[T-1]]$. The constant term of this expression in brackets is clearly $(b \cdot 2/b) - 1 - 1 = 0$, so this expression in brackets in (4.8) is divisible by $T-1$ and therefore $h(T) \in \mathbb{Z}_p[[T-1]]$.

In ([7], Theorem 1.1) we showed that if $h \in \mathbb{Z}_p[[T-1]]$ and $h(e^t) = \sum_{n=0}^{\infty} a_n t^n/n!$ then for $c \equiv 0 \pmod{(p-1)p^a}$ we have $\Delta_c^k a_m \equiv 0 \pmod{p^A\mathbb{Z}_p}$ for all $k \geq 0$, where $A = \min\{m, k(a+1)\}$. Since $g(e^t) = -1/\varepsilon(-t)$ and $h(T) = bg(T^b) - g(T)$ we have

$$h(e^t) = \sum_{n=0}^{\infty}(b^{n+1}-1)\frac{\hat{B}_{n+1}}{n+1}(-1)^{n+1}\frac{t^n}{n!} \tag{4.11}$$

so that $a_n = (b^{n+1}-1)(-1)^{n+1}\hat{B}_{n+1}/(n+1)$. Therefore for any m,

$$\Delta_c^k\left\{(b^m-1)\frac{\hat{B}_m}{m}(-1)^m\right\} \equiv 0 \qquad \pmod{p^A\mathbb{Z}_{(p)}} \tag{4.12}$$

where $A = \min\{m-1, k(a+1)\}$. Since the increment c is even the factor $(-1)^{m+jc} = (-1)^m$ independent of j and therefore may be factored out of the congruences. Now suppose that k and m are given such that $p-1$ does not divide m. Since the mutiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $p-1$, we may choose a positive integer x such that $(x,p) = 1$ and $x^m \not\equiv 1$

(mod p). Now let $N > k(a+1)$ and put $b = x^{p^N}$. Since $y^{p^s(p-1)} \equiv 1 \pmod{p^{s+1}}$ for any nonnegative integers y, s, it follows that this choice of b satisfies $(b,p)=1$, $b^m \equiv x^m \not\equiv 1$ (mod p), and $b^{m+jc} \equiv b^m \pmod{p^{N+1}}$ for all j. Therefore from (4.12),

$$\begin{aligned}0 &\equiv \sum_{j=0}^{k}(-1)^{k-j}\binom{k}{j}(b^{m+jc}-1)\frac{\hat{B}_{m+jc}}{m+jc}(-1)^{m+jc} \\ &\equiv (b^m-1)(-1)^m\sum_{j=0}^{k}(-1)^{k-j}\binom{k}{j}\frac{\hat{B}_{m+jc}}{m+jc} \qquad (\text{mod } p^A\mathbb{Z}_{(p)}),\end{aligned} \tag{4.13}$$

but since the factor $(b^m-1)(-1)^m$ is a unit in $\mathbb{Z}_{(p)}$ the result follows.

Theorem 4.3: *Let $\hat{B}_n$ denote the numbers obtained in (1.4) by specializing the indeterminates $c_i \mapsto V_{i+1}$ in (1.3), where $P=1$ and Q is an arbitrary integer. If p is an odd prime, $p-1$ does not divide m, and the increment $c = l(p-1)$ where p^a divides l for some $a \geq 0$, then for all $k \geq 0$, the congruence*

$$\sum_{j=0}^{k}(-1)^{k-j}\binom{k}{j}c_{p-1}^{(k-j)l}\frac{\hat{B}_{m+jc}}{m+jc} \equiv 0 \qquad (\text{mod } p^A\mathbb{Z}_{(p)})$$

given in (1.7) holds, where $A = \min\{m-1, k(a+1)\}$.

Proof: We have $V_p \equiv 1 \pmod p$, so by (2.5) there exists $V_p^{1/(p-1)} \in \mathbb{Z}_p$ such that $(V_p^{1/(p-1)})^{p-1} = V_p$ and $V_p^{1/(p-1)} \equiv 1$ (mod $p\mathbb{Z}_p$). The left side of the congruence of the theorem may be written as

$$\begin{aligned}&\sum_{j=0}^{k}(-1)^{k-j}\binom{k}{j}V_p^{(k-j)l}\frac{\hat{B}_{m+jc}}{m+jc} \\ &= V_p^{kl+m/(p-1)}\sum_{j=0}^{k}(-1)^{k-j}\binom{k}{j}(V_p^{-1/(p-1)})^{m+jc}\frac{\hat{B}_{m+jc}}{m+jc} \\ &= V_p^{kl+m/(p-1)}\Delta_c^k\left\{(V_p^{-1/(p-1)})^m\frac{\hat{B}_m}{m}\right\}.\end{aligned} \tag{4.14}$$

By the identity (2.8), this expression is equal to

$$V_p^{kl+m/(p-1)}\sum_{i=0}^{k}\binom{k}{i}\Delta_c^i\left\{\frac{\hat{B}_m}{m}\right\}\Delta_c^{k-i}\left\{(V_p^{-1/(p-1)})^{m+ic}\right\}. \tag{4.15}$$

By Theorem 4.2 we have $\Delta_c^i\{\hat{B}_m/m\} \equiv 0$ (mod $p^{A_i}\mathbb{Z}_{(p)}$) for $A_i = \min\{m-1, i(a+1)\}$. By the binomial theorem the term $V_p^{kl+m/(p-1)}\Delta_c^{k-i}\{(V_p^{-1/(p-1)})^{m+ic}\}$ is equal to

$$V_p^{(k-i)l}\left(V_p^{-l}-1\right)^{k-i}. \tag{4.16}$$

Since $V_p \equiv 1 \pmod{p}$ we have $V_p^{-l} \equiv 1 \pmod{p^{(a+1)}\mathbb{Z}_{(p)}}$, and therefore (4.16) is zero modulo $p^{(k-i)(a+1)}\mathbb{Z}_{(p)}$. Therefore each term in the sum (4.15) is zero modulo $p^A\mathbb{Z}_{(p)}$, proving the theorem.

5. CONNECTIONS TO FORMAL GROUP LAWS

In this section we summarize some basic facts concerning formal group laws which relate to the results of this paper. Let $c_1, c_2, \ldots \in \mathbb{Z}$, define $\lambda \in \mathbb{Q}[[t]]$ by (1.3), and let ε be the compositional inverse of λ in $\mathbb{Q}[[t]]$. Then the two-variable formal power series $F \in \mathbb{Q}[[X,Y]]$ defined by $F(X,Y) = \varepsilon(\lambda(X) + \lambda(Y))$ is a commutative formal group law over $\mathbb{Q}$; that is,

$$F(X,Y) = F(Y,X), \tag{5.1}$$

$$F(X,0) = X \qquad \text{and} \qquad F(0,Y) = Y \tag{5.2}$$

and

$$F(F(X,Y),Z) = F(X,F(Y,Z)) \tag{5.3}$$

hold as identities in $\mathbb{Q}[[X,Y]]$. If

$$v(T) = \frac{\partial}{\partial X}(F(X,Y))\bigg|_{X=0,Y=T} \tag{5.4}$$

then $\omega = dT/v(T)$ is the canonical invariant differential on F, $\lambda(t) = \int_0^t \omega$ is the formal logarithm of F, and the compositional inverse ε of λ is the formal exponential of F, which satisfies the autonomous differential equation $\varepsilon' = v(\varepsilon)$. Any choice of integers c_i in (1.3) will make λ into the logarithm of a formal group law over $\mathbb{Q}$, but only certain choices of $c_i \in \mathbb{Z}$ will yield a formal group law over $\mathbb{Z}$.

By the functional equation lemma of Hazewinkel [5], the formal group law F thus constructed will be defined over $\mathbb{Z}$ (i.e., $F \in \mathbb{Z}[[X,Y]]$) if and only if for each prime p there exists an element $\eta_p \in \mathbb{Z}_p$ such that for all positive integers m, s we have

$$c_{mp^s-1} \equiv \eta_p c_{mp^{s-1}-1} \qquad \pmod{p^s\mathbb{Z}_p}, \tag{5.5}$$

with the convention $c_0 = 1$. For $c_i \mapsto U_{i+1}$ we have

$$U_{mp^s} \equiv (D|p) U_{mp^{s-1}} \qquad \pmod{p^s\mathbb{Z}_p}, \tag{5.6}$$

whereas for $c_i \mapsto V_{i+1}$ we have

$$V_{mp^s} \equiv V_{mp^{s-1}} \qquad \pmod{p^s\mathbb{Z}_p}, \tag{5.7}$$

(cf. [7]). Therefore the differential forms in (2.3), (3.1), (4.2) are invariant differentials on integral formal group laws. (For $c_i \mapsto V_{i+1}$ we required $P = 1$ only so that the first coefficient c_0 of λ will be 1.) For both of these specializations of the c_i we have seen that for even $n > 0$ the denominator of $\hat{B}_n$ is equal to the product of those primes p not dividing c_{p-1} such that $p-1$ divides n (see Theorems 3.1 and 4.1 and also [3]).

If we map $c_i \mapsto U_{i+1}$ so that ω and λ are as in (3.1), we may calculate that the rational function

$$F(X,Y) = \frac{X+Y-PXY}{1-QXY} \tag{5.8}$$

is the corresponding formal group law. From [4] we know that every rational formal group law over $\mathbb{Q}$ is of the form (5.8). Therefore we may interpret Theorem 3.2 as saying that the numbers $\hat{B}_n$ satisfy the congruences (1.7) whenever the c_i in (1.3) are specialized to integers which make λ into the logarithm of a *rational* formal group law.

A more general connection between integrality of formal group laws and Kummer congruences may be seen in Adelberg's result ([1], Theorem 4.5). There he showed that if $c = l(p-1)$ where p^a divides l, $m \geq a+2$, and $m \not\equiv 0, 1 \pmod{p-1}$ then the congruence (1.5) holds, whereas if $m \equiv 1 \pmod{p-1}$ and $m \geq a+2$ then the congruence (1.6) holds for the universal Bernoulli numbers $\hat{B}_n$. Now if the c_i are specialized to integers in (1.3) so that λ is the logarithm of an *integral* formal group law, then by (5.5) with $s = 1$ we have $c_{p-1} \equiv \eta_p \pmod{p}$ and $c_{2p-1} \equiv \eta_p c_1 \pmod{p}$. It follows that $c_{p-1}c_1^p - c_{2p-1} \equiv 0 \pmod{p}$, and therefore the expression on the right in (1.6) vanishes modulo $p^{a+1}\mathbb{Z}_p$. That is, the right side of (1.6) is trivial for the $\hat{B}_n$ associated to any formal group law over $\mathbb{Z}$, but not for an arbitrary formal group law over $\mathbb{Q}$. In [6] Snyder showed that the numbers $\hat{B}_n$ associated to any formal group law over $\mathbb{Z}$ satisfy the congruences (1.7) in the case where $l = 1$. In this paper we have looked at the examples of integral formal group laws obtained by $c_i \mapsto U_{i+1}$ or $c_i \mapsto V_{i+1}$ and shown that their associated numbers $\hat{B}_n$ satisfy not only (1.5), but the more general version (1.7).

REFERENCES

[1] A. Adelberg. "Universal Kummer Congruences Mod Prime Powers." *J. Number Theory* **109** (2004): 362-378.

[2] L. Carlitz. "Some Congruences for the Bernoulli Numbers." *Amer. J. Math.* **75** (1953): 163-172.

[3] F. Clarke. "The Universal von Staudt Theorems." *Trans. Amer. Math. Soc.* **315** (1989): 591-603.

[4] R. Coleman and F. McGuinness. "Rational Formal Group Laws." *Pacific J. Math.* **147** (1991): 25-27.

[5] M. Hazewinkel. *Formal Groups and Applications*, Academic Press, New York, 1978.

[6] C. Snyder. "A Concept of Bernoulli Numbers in Algebraic Function Fields (II)." *Manuscripta Math.* **35** (1981): 69-89.

[7] P. T. Young. "p-adic Congruences for Generalized Fibonacci Sequences." *The Fibonacci Quarterly* **32.1** (1994): 2-10.

[8] P. T. Young. "Congruences for Bernoulli, Euler, and Stirling Numbers." *J. Number Theory* **78** (1999): 204-227.

AMS Classification Numbers: 11B68, 11B39

✠ ✠ ✠