A NOTE ON NUMERATORS OF BERNOULLI NUMBERS

DINESH S. THAKUR

(Communicated by Matthew A. Papanikolas)

ABSTRACT. The object of this short note is to give some observations on Bernoulli numbers and their function field analogs and to point out 'known' counterexamples to a conjecture of Chowla.

Bernoulli numbers B_n defined (for integer $n > 1$) by $z/(e^z - 1) = \sum B_n z^n/n!$, and their important cousins B_n/n, play interesting roles in many areas of mathematics. (Below we only restrict to these for n even, precisely the case when they are non-zero.) We mention some key words by which the reader can search: power sums, Zeta special values, Eisenstein series, measures, p-adic L-functions, finite differences, combinatorics, Euler-Maclaurin formula, Todd classes in topology, Grothendieck-Hirzebruch-Riemann-Roch formula, K-theory of integers, stable homotopy, Bhargava factorial associated to the set of primes, Kummer-Herbrand-Ribet theorems in cyclotomic theory, Kervaire-Milnor formula for diffeomorphism classes of exotic spheres. Their factorization is of interest; the denominators (which show up explicitly in the third and fourth items from the end) are well understood via theorems of von Staudt, but the numerators (which show up explicitly in the last two items above) are mysterious and connected to many interesting phenomena.

In one of the rare lapses, Ramanujan, in his very first paper [R1911, (14), (18) and Sec. 12], claimed to have proved (editors downgrade it to a conjecture) that the numerator N_n of B_n/n is always a prime, when it was already known since Kummer (in Fermat's last theorem connection) that the 'irregular' prime 37 is a proper divisor of N_{32}, and even N_{20} is composite. In [C1930], Chowla showed that Ramanujan's claim had an infinity of counterexamples. Note that this also follows from one counter-example and the Kummer congruences (recalled below) for that prime!

Interestingly, in his last paper [CC1986], Chowla (jointly with his daughter) asks as an unsolved problem whether the numerator is always square-free. (This is also mentioned in the nice survey article by Murtys and Williams on Chowla's work in Vol. 1 of [C1999], where the author learned about it.)

Theorem 1. *Chowla's conjecture stated above has an infinity of counterexamples. In fact, for any given irregular prime p less than 163 million, and given arbitrarily large k, there is an n such that p^k divides N_n.*

Proof. Using the tables (or the reader can try to check directly!) giving factorizations of B_n/n, for example the table by Wagstaff at the Bernoulli webpage

©2012 Dinesh S. Thakur

www.bernoulli.org, we see that 37^2 divides N_{284}. Now recall the well-known Kummer congruences that the value of $(1 - p^{n-1})B_n/n$ modulo p^k depends only on (even) n modulo $p^{k-1}(p-1)$, for n not divisible by $p-1$. The first claim follows by taking $p^k = 37^2$.

By the Kummer congruences and the von Staudt theorem [W1982, Ch. 5], the prime divisors of N_n are exactly the irregular primes p defined [W1982, p. 62] as those dividing B_k for some even positive k less than $p-1$.

Now, Kubota-Leopaldt p-adic L-functions [W1982, Chs. 5, 7] are p-adically continuous functions of n interpolating the values at $(1 - p^{n-1})B_n/n$ at n in a fixed congruence class k modulo $p-1$. Thus having a zero in $\mathbb{Z}_p$ for these functions implies that arbitrarily high powers of p divide N_n as n approaches such a zero p-adically through the positive integers.

Computations by Iwasawa, Sims, Johnson, Wagstaff, Buhler et al. (see for example [EM1991, p. 852] and [BCEMS, BH]) show that for irregular primes p less than 163 million, the Iwasawa lambda invariant for the Kubota-Leopaldt L-functions is always one for all irregular pairs (p, k) for this range, and thus the corresponding Weierstrass polynomials, being linear, have a zero in $\mathbb{Z}_p$. This proves the second claim. $\qquad\square$

Remarks 2. (i) The awkward reference at the start of the proof is because we do not know exactly when the relevant computations in the range we want were first made and by whom. The website has many examples; we have chosen one with the smallest n.

(ii) The proof shows that, in some sense, infinitely many counterexamples were already 'known', but probably Chowla's conjecture was not known to the people who knew counterexamples, as there are no citations to [CC1986].

It may be of interest to the reader that before thinking of these things and looking at the data, the author had noticed the evidence in the function field case. There is a well-developed number fields (function fields) analogy [G1996, T2004]. The analogy is even stronger in the simplest case: it is between $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, the exponential '$e^z$', the Euler-Riemann zeta '$\zeta(s)$', the factorial '!' on the one hand, and $\mathbb{F}_q[t], \mathbb{F}_q(t), \mathbb{F}_q((1/t))$, the Carlitz exponential '$e(z)$', the Carlitz-Goss zeta '$\zeta_c(s)$' and the Carlitz factorial '$!_c$', respectively.

Let us define our terms: Here q is a prime power, and $\mathbb{F}_q$ a finite field of q elements. If a positive integer n has the base q expansion, $n = \sum n_i q^i$, $0 \le n_i < q$, then $n!_c := \prod D_i^{n_i} \in \mathbb{F}_q[t]$, where $D_m := \prod_{i=0}^{m-1}(t^{q^m} - t^{q^i})$. We have $e_c(z) = \sum z^{q^i}/q^i!_c$ parallel to $e^z = \sum z^n/n!$. Finally, for $s \in \mathbb{Z}$, $\zeta_c(s) := \sum_{d=0}^{\infty} \sum 1/a^s \in \mathbb{F}_q((1/t))$, where the second sum is over monic polynomials $a \in \mathbb{F}_q[t]$ of degree d. Counting cardinalities of analogous objects $\mathbb{Z}^*$ and $\mathbb{F}_q[t]^*$, we see that the analog of even integers is played often by multiples of $q-1$, which we call 'even'. Other integers (if any!) are called 'odd'.

The Bernoulli-Carlitz numbers $\mathcal{B}_n \in \mathbb{F}_q(t)$ are defined analogously by $z/e(z) = \sum \mathcal{B}_n z^n/n!_c$. They are non-zero, precisely when n is 'even'. See, e.g., [T2004, 4.16, 5.2, 5.3, 8.9] or [G1996] for properties, various analogies, such as an analog of Euler's theorem connecting to values of zeta at positive 'even' integers n, von Staudt, Herbrand-Ribet theorem analogs, and references to the original works.

Note that since n is in characteristic zero, while $\mathcal{B}_n$ is in characteristic p, $\mathcal{B}_n/n$ does not make sense and is thus replaced by $\mathcal{B}_n(n-1)!_c/n!_c$, and its numerator is denoted by $\mathcal{N}_n$.

Here are counterexamples to a naive analog of the Chowla conjecture.

Theorem 3. *For any given prime $\wp$ of $\mathbb{F}_q[t]$ and any positive integer k, there are infinitely many n (in fact, even of the form $q^r - 1$) such that $\wp^k$ divides $\mathcal{N}_n$.*

Proof. Carlitz [T2004, Thm. 4.16.1] proved that for $n = q^k - 1$, we have

$$\mathcal{B}_n = \mathcal{B}_n(n-1)!_c/n!_c = (-1)^k \prod_{i=1}^{k-1} [k-i]^{q^i-2}/[k],$$

where $[j] := t^{q^j} - t$ is the product of all monic irreducible polynomials of degree dividing j. Hence for large k, the numerators are divisible by large (tending to infinity with k) powers of *all* primes of small (tending to infinity with k) degree. $\square$

In spite of various nice analogies mentioned above, the Bernoulli-Carlitz numbers do not satisfy Kummer type congruences, and thus the prime divisors of $\mathcal{N}_n$ are not necessarily 'irregular' primes $\wp$, defined again by analogy as those dividing some $\mathcal{B}_k$ for positive 'even' k less than the norm$(\wp) - 1$. Here, as usual, the norm of a polynomial in $\mathbb{F}_q[t]$ is q raised to its degree.

Analogs of Kummer congruences, as well as Herbrand-Ribet theorems, are satisfied by another analog $\beta(n) \in \mathbb{F}_q[t]$ due to Goss, the Bernoulli-Goss numbers [G1996], [T2004, 5.3] defined by $\beta(n) = \zeta_c(-n)$ for 'odd' positive n. (For general n, they are defined by some kind of 'derivative', but we will not need it.) Recall that $\zeta(1-n) = -B_n/n$, for even n, but also note that $1-n$ is 'odd' does not mean n is 'even'! We do not know any 'functional equation' for ζ_c connecting $\mathcal{B}_n$ and $\beta(n)$. We can have a new notion of 'irregular' primes in this connection, defined as prime divisors of these $\beta(n)$.

Theorem 4. *Given any 'irregular' prime $\wp$ defined as in the last paragraph, and any positive integer k, there are infinitely many n such that $\beta(n)$ is divisible by $\wp^k$.*

Proof. Let q be a power of a prime p. We have that $\beta(p^r m) = \beta(m)^{p^r}$ just from the definitions since p-th powers are additive in characteristic p. $\square$

Remarks 5. (i) Hence, both of the function field Bernoulli analogs prove an analog of the 'conjecture' in the classical case that primes which divide the numerators of B_n/n divide some B_m/m to an arbitrarily large given power, with a second analog fitting even more strongly by working exactly for 'irregular' primes. It is also interesting that these Iwasawa theory calculations which started with analogies with cyclotomic extensions of constant field type also fit well in this case with cyclotomic extensions of Carlitz-Drinfeld type [G1996, T2004].

(ii) Regarding the 'conjecture' mentioned in (i), it has a status similar to the Vandiver conjecture: some have expressed the possibility (see e.g. [BCEMS, p. 94]) of this being true, whereas many experts tend to go with probabilistic models initiated by Siegel [W1982] which predict counterexamples. In fact, Ralph Greenberg has mentioned to the author that he believes that for some irregular primes, the power they divide N_n can stay bounded, so that the Iwasawa lambda invariants can be more than one and no zeros in $\mathbb{Z}_p$ for the p-adic L-functions in the corresponding case. Hopefully, we will know soon!

Acknowledgments

The author thanks Kirti Joshi for making him aware of [R1911, C1930] a few years ago; Sheldon Joyner for making him think of these questions again by asking him a question and then referring him to www.bernoulli.org for higher irregular pairs; Romyar Sharifi for referring him to the computation of Iwasawa invariants leading to p-adic zeros; and Ralph Greenberg for his comments mentioned above.

References

[BCEMS] J. Buhler, R. Crandall, R. Ernvall, T. Metsänkylä, and M. Shokrollahi, *Irregular primes and cyclotomic invariants to* 12 *million*, J. Symb. Comp. 31 (2001), 89-96. MR1806208 (2001m:11220)

[BH] J. Buhler and D. Harvey, *Irregular primes to* 163 *million*, on arXiv 12 Dec 2009. To appear in Math. Comp.

[C1930] S. Chowla, *On a conjecture of Ramanujan*, Tohoku Math. J. 33 (1930), 1-2. (Paper [34] in [C1999]). MR1829817 (2002m:01034a)

[CC1986] S. Chowla and P. Chowla, *Some unsolved problems*, Norske Vid. Selsk. Skr. (Trondheim) 1986, no. 2, 7 (last paper [351] in [C1999]). MR1829819 (2002m:01034c)

[C1999] S. Chowla, *Collected papers of Sarvadaman Chowla, Vols. 1-3*, ed. by J. Huard, K. Williams, Centre de Recherches Mathematiques, 1999. MR1829817 (2002m:01034a); MR1829818 (2002m:010346); MR1829819 (2002m:01034c)

[EM1991] R. Ernvall and T. Metsänkylä, *Cyclotomic invariants for primes between* 125000 *and* 150000, Math. Comp. 56, no. 194 (1991), 851-858. MR1068819 (91h:11157)

[G1996] D. Goss, *Basic Structures of Function Field Arithmetic*, Springer-Verlag, NY, 1996. MR1423131 (97i:11062)

[R1911] S. Ramanujan, *Some properties of Bernoulli's numbers*, J. Indian Math. Soc. 3 (1911), 219-234. Also the first paper in [R1927]. MR2280844

[R1927] S. Ramanujan, *Collected papers of Srinivasa Ramanujan*, ed. by G. H. Hardy et al., Cambridge Univ. Press, 1927. MR2280843 (2008b:11002)

[T2004] D. Thakur, *Function Field Arithmetic*, World Sci., NJ, 2004. MR2091265 (2005h:11115)

[W1982] L. Washington, *Introduction to Cyclotomic Fields*, Springer, NY, 1982. MR718674 (85g:11001)

Department of Mathematics, University of Arizona, Tucson, Arizona 85721
E-mail address: thakur@math.arizona.edu