ON THE ZETA FUNCTION FOR FUNCTION FIELDS OVER $F_p$

Emery Thomas
ON THE ZETA FUNCTION
FOR FUNCTION FIELDS OVER $F_p$

EMERY THOMAS

We consider here the zeta function for a function field defined over a finite field $F_p$. For each integer $j$, $\zeta(j)$ is a polynomial over $F_p$, as is $\zeta'(j)$, the "derivative" of zeta. In this note we compute the degree of these polynomials, determine when they are the constant polynomial and relate them to the polynomial gamma function.

In a recent series of papers D. Goss has introduced the notion of a zeta function $\zeta(j)$ for rational function fields over $F_r$, where $r = p^k$, with $p$ a rational prime. In particular, for each positive integer $i$, with $i \equiv 0 (r - 1)$, $\zeta(-i) \in F_r[t]$. Goss also defines the "derivative" of $\zeta$, $\zeta'$, with $\zeta'(-i) \in F_r[t]$ if $i \equiv 0 (r - 1)$. We combine these special values of $\zeta$ and $\zeta'$ into a single function $\beta(n)$ (with $n = -i$) defined by:

$$
\beta(0) = 0, \quad \beta(1) = 1,
$$

$$
\beta(n) = 1 - \sum_{i=1}^{n-1} \binom{n}{i} t^i \beta(i), \quad n \geq 2,
$$

where $s = r - 1$. Thus, by (3.9) and (3.10) of [2],

$$
\beta(n) = \begin{cases} 
\zeta(-n), & n \equiv 0 (s) \\
\zeta'(-n), & n \equiv 0 (s).
\end{cases}
$$

An important situation where these functions arise is in determining the class numbers of certain extension fields over $F_r[t]$ (modeled on cyclotomic fields). If $P$ is a prime polynomial in $F_r[t]$, Goss defines class numbers $h^+(P)$ and $h^-(P)$ associated to $P$, in the classical fashion, and shows that their study (à la Kummer) involves the polynomials $\zeta(-i)$ and $\zeta'(-i)$. Thus it is important that we know certain facts about these functions, and hence about $\beta(n)$. Specifically, when is $\beta(n) = 1$? What is the degree of $\beta(n)$? When does $\beta(n)$ factor? In this note we give some answers to these questions, for the case $r = p$.

Remark. I am indebted to Goss for bringing this material to my attention.
The function $\beta(n)$. Let $p$ be a rational prime, and for each integer $n \geq 0$, let $\beta(n) \in F_p[t]$ be the polynomial defined above. Note that if $0 < n \leq s$ ($= p - 1$), then $\beta(n) = 1$. For $n > s$ we rewrite (1) as follows: set $k = [(n - 1)/s]$. Then (1) becomes:

$$
\beta(n) = 1 - \sum_{i=1}^{k} \binom{n}{is} t^{n-is} \beta(n-is).
$$

Let $n = \sum_i a_i p^i$ be the $p$-adic representation of $n$; thus, $0 \leq a_i \leq s$, and almost all $a_i$ are zero. Define

$$
l(n) = \sum_i a_i.
$$

Our first result is:

**Theorem 1.** Let $n$ be a positive integer with $l(n) \leq s$. Then,

$$
\beta(n) = 1.
$$

The proof depends upon several simple facts about binomial coefficients mod $p$. Recall the result of Lucas:

$$
\left( \begin{array}{c} n \\ m \end{array} \right) \equiv \prod_i \left( \begin{array}{c} a_i \\ b_i \end{array} \right) \mod p.
$$

In particular,

$$
\left( \begin{array}{c} n \\ m \end{array} \right) \equiv 0 \mod p \iff 0 \leq b_i \leq a_i, \text{ all } i.
$$

As an immediate consequence, we have:

$$
\left( \begin{array}{c} n \\ m \end{array} \right) \equiv 0 \mod p, \text{then } l(n) = l(m) + l(n-m). \text{ In particular, if } 1 \leq m < n, \text{then } l(n) > l(m).
$$

Finally, note that since $p \equiv 1 \mod s$, we have:

$$
n \equiv l(n) \mod s.
$$

**Proof of Theorem 1.** Let $j$ be any positive integer. By (6), since $js \equiv 0 \mod s$, $l(js) \geq s$. Thus, if $n$ is an integer with $js < n$ and $\left( \begin{array}{c} n \\ js \end{array} \right) \equiv 0 \mod p$, then by (5), $l(n) > l(js) \geq s$. Therefore, if $l(n) \leq s$, then $\left( \begin{array}{c} n \\ js \end{array} \right) \equiv 0 \mod p$. Thus, by (3), $\beta(n) = 1$, as claimed.
We suppose now that \( n \) is an integer with \( l(n) > s \); our goal is to calculate the degree of \( \beta(n) \) — call this simply \( D(n) \).

Define an integer valued function \( \rho(n) \) by:

\[
\text{If } l(n) \geq s, \text{ set } \rho(n) = n - m, \text{ where } m \text{ is the least positive integer such that } l(m) = s \text{ and } \left( \frac{n}{m} \right) \equiv 0 \pmod{p}.
\]

Thus, if \( n \) is written \( p \)-adically in the form

\[
n = \sum_{i=0}^{N} p^{e_i}, \text{ with } e_0 \leq \cdots \leq e_N,
\]

and with no more than \( s \) \( e_i \)'s with the same value, then

\[
m = \sum_{i=0}^{s-1} p^{e_i}.
\]

If \( q \) is an integer (\( \geq 0 \)) with \( l(q) < s \), set \( \rho(q) = 0 \).

Set \( \rho^{i+1}(n) = \rho(\rho^i(n)) \), with \( \rho^0(n) = n \). Thus, for large \( i \), \( \rho^i(n) = 0 \).

**Example.** \( p = 5, \ n = 3 \cdot 1 + 4 \cdot 5 + 2 \cdot 5^3 \). Then,

\[
\begin{align*}
\rho^1(n) &= 3 \cdot 5 + 2 \cdot 5^3, \\
\rho^2(n) &= 5^3, \\
\rho^3(n) &= 0.
\end{align*}
\]

Our result is:

**Theorem 2.** Let \( n \) be an integer with \( l(n) > s \). Then

\[
D(n) = \text{degree } \beta(n) = \sum_{i \geq 1} \rho^i(n).
\]

The proof will be by induction on \( l(n) \). Suppose first that \( l(n) = s + 1 \).

If \( j \) is any positive integer with \( js < n \) and \( \left( \frac{n}{js} \right) \equiv 0 \pmod{p} \), then by (5) and (6), \( l(n - js) = 1 \), and so by Theorem 1, \( \beta(n - js) = 1 \). Therefore, by (2), \( D(n) = n - js \), where \( j \) is the least positive integer such that \( \left( \frac{n}{js} \right) \equiv 0 \pmod{p} \); i.e., \( D(n) = \rho(n) \), as stated in Theorem 2.

We now make the following pair of inductive hypotheses: let \( k \) be an integer \( \geq s + 1 \), and suppose that \( n \) is any integer such that

\[
s + 1 \leq l(n) \leq k.
\]
For any such integer \( n \), \( D(n) \) is given by Theorem 2.

Let \( n \) be any integer as above. If \( c \) is the least positive integer such that \( \binom{n}{cs} \equiv 0 \pmod{p} \) and \( d \) is any integer with \( cs \leq ds \leq n \) and \( \binom{n}{ds} \equiv 0 \pmod{p} \); then \( D(n - cs) \geq D(n - ds) \).

**Claim 1.** \( A_k \) implies \( B_{k+1} \).

**Proof.** Write \( n \) as in (8) so that \( cs = \sum_{i=0}^{s-1} p^i \). Thus, \( n - cs = \sum_{i=0}^{N-s} p^i \), where \( f_i = e_{i+s} \). Similarly, write \( n - ds = \sum_{i=0}^{M} p^i \), where \( M \leq N - s \).

Then, for \( i \leq M \), \( p^i \geq p^s \), and so \( D(n - cs) \geq D(n - ds) \), either by Theorem 1 or by \( A_k \) and Theorem 2, since \( l(n - cs) \) and \( l(n - ds) \) are less than \( l(n) \).

**Claim 2.** \( A_k \) and \( B_{k+1} \) imply \( A_{k+1} \).

**Proof.** Let \( n \) be an integer with \( l(n) = k + 1 \). Write \( n \) as in (8) and define \( cs \) as above, so that \( \rho(n) = n - cs \). By (3) and \( B_{k+1} \),

\[
D(n) = n - cs + D(n - cs) = \rho(n) + D(\rho(n)).
\]

Since \( l(\rho(n)) < l(n) = k + 1 \), by \( A_k \)

\[
D(\rho(n)) = \sum_{i \geq 1} \rho'(\rho(n)) = \sum_{i \geq 1} \rho'^{i+1}(n).
\]

Therefore, \( D(n) = \sum_{i \geq 1} \rho'(n) \), which proves \( A_{k+1} \).

**Proof of Theorem 2.** We showed above that \( A_{s+1} \) holds, and so by Claims 1 and 2, \( A_k \) holds for all \( k > s \). This proves the theorem.

Note that (trivially) if \( n \) is positive, then \( \beta(n) \neq 0 \). Combining Theorems 1 and 2 we have:

**Corollary 1.** If \( n \) is a positive integer, then \( \beta(n) = 1 \) if, and only if, \( l(n) \leq s \).

For certain values of \( n \), \( D(n) \) can be written out explicitly.

**Corollary 2.** Let \( k \) and \( m \) be positive integers, with \( m \leq s \). Then

\[
D((m + 1)p^k - 1) = s \sum_{i=1}^{k-1} ip' + kmp^k.
\]
Relation to the gamma function. We are interested in comparing the function \( \beta(n) \) with the Gamma function \( \Gamma_n \) (see [1]). Combining Corollary 2 with (3.1.1) of [1], we find:

**Corollary 3.** Let \( n = (m + 1)p^k - 1 \), where \( k \) and \( m \) are positive integers with \( m \leq s \). Then,

\[
\deg \beta(n) = \deg \Gamma_n.
\]

For certain values of \( n \) we have a stronger result.

**Theorem 3.** Suppose that \( n = (m + 1)p - 1 \), with \( 1 \leq m \leq s \). Then,

\[
\beta(n) = 1 - \Gamma_n.
\]

We are especially interested in divisibility properties of \( \beta(n) \). Thus, we have:

**Corollary 4.** For \( 1 \leq k \leq s/2 \) and \( p \) an odd prime,

\[
\beta((2k + 1)p - 1) = (1 - \Gamma_{kp})(1 + \Gamma_{kp}).
\]

In particular,

\[
\beta(p^2 - 1) = (1 - \Gamma_{sp/2})(1 + \Gamma_{sp/2}).
\]

**Proof of Theorem 3.** We will need the following (easily proved) fact:

If \( 0 \leq i \leq s \), then \( \left( \begin{array}{c} s \\ i \end{array} \right) \equiv (-1)^i \mod p \).

Suppose that \( n = (m + 1)p - 1 \), as above. Thus, \( n = s \cdot 1 + mp \), and so by (3) and Theorem 1,

\[
\beta(n) = 1 - \sum_{i=0}^{m} \left( \begin{array}{c} s \\ i \end{array} \right) \left( \begin{array}{c} m \\ i \end{array} \right) t^i \cdot t^{(m-i)p}
\]

by (3.1.1) of [1].
REFERENCES


Received May 22, 1981. Research supported by a grant from the National Science Foundation.

UNIVERSITY OF CALIFORNIA
BERKELEY, CA 94720
John Kelly Beem and Phillip E. Parker, Klein-Gordon solvability and the geometry of geodesics .................................................. 1
David Borwein and Amnon Jakimovski, Transformations of certain sequences of random variables by generalized Hausdorff matrices ... 15
Willy Brandal and Erol Barbut, Localizations of torsion theories ........... 27
John David Brillhart, Paul Erdős and Richard Patrick Morton, On sums of Rudin-Shapiro coefficients. II ............................................ 39
Martin Lloyd Brown, A note on tamely ramified extensions of rings ....... 71
Chang P’ao Ch’ên, A generalization of the Gleason-Kahane-Żelazko theorem ............................................................................. 81
I. P. de Guzman, Annihilator alternative algebras ................................... 89
Ralph Jay De Laubenfels, Extensions of $d/dx$ that generate uniformly bounded semigroups .................................................... 95
Patrick Ronald Halpin, Some Poincaré series related to identities of $2 \times 2$ matrices ........................................................................ 107
Fumio Hiai, Masanori Ohya and Makoto Tsukada, Sufficiency and relative entropy in $\ast$-algebras with applications in quantum systems ........ 117
Dean Robert Hickerson, Splittings of finite groups .................................... 141
Jon Lee Johnson, Integral closure and generalized transforms in graded domains ........................................................................... 173
Maria Grazia Marinari, Francesco Odetti and Mario Raimondo, Affine curves over an algebraically nonclosed field ................................. 179
Douglas Shelby Meadows, Explicit PL self-knottings and the structure of PL homotopy complex projective spaces ............................ 189
Charles Kimbrough Megibben, III, Crawley’s problem on the unique $\omega$-elongation of $p$-groups is undecidable ................................ 205
Mary Elizabeth Schaps, Versal determinantal deformations ..................... 213
Stephen Scheinberg, Gauthier’s localization theorem on meromorphic uniform approximation ....................................................... 223
Peter Frederick Stiller, On the uniformization of certain curves ............ 229
Ernest Lester Stitzinger, Engel’s theorem for a class of algebras ............ 245
Emery Thomas, On the zeta function for function fields over $F_p$ ............ 251