ON POWER SUMS OF POLYNOMIALS OVER FINITE FIELDS

ERNST-ULRICH GEKELER

Max-Planck-Institut
für Mathematik
Gottfried-Claren-Str. 26

5300 Bonn 3

MPI/87-26

On power sums of polynomials over finite fields

Ernst-Ulrich Gekeler

0. Introduction

Let $A = \mathbb{F}_q[T]$ be the polynomial ring over a finite field $\mathbb{F}_q$ with q elements, K its quotient field, and K_∞ the completion of K at its prime at infinity. Non-zero elements of A are <u>monic</u> if their leading coefficient equals one. In a series of papers (e.g. [5], [6], [7]), D. Goss has introduced and investigated the K_∞-valued zeta function of K which interpolates the sums $\sum a^{-k}$ ($a \in A$ monic, $k \in \mathbb{N}$). Let $s_i(k) = \sum a^k$ ($a \in A$ monic of degree i). Then $s_i(k) = 0$ for i large, and $\sum s_i(k)$ $(i \geq 0)$ appears as the value of zeta at $-k$ [6]. Another source of interest in these "numbers" is the link between their congruence properties and class number formulas, which leads to a Kummer-type criterion for abelian extensions of K [5].

In this article, we study the $s_i(k)$. Among other things, we prove certain relations between $s_i(k)$ and the polynomial gamma function Γ_k, for special values of k. These relations (i.e. (6.3)), had been empirically observed by Goss [6]. For k of the form $q^h - 1$, we obtain a simple expression for $s_i(k)$ by means of elementary arithmetic functions (see (4.1)). Further, we have some results on the size of $s_i(k)$ and on congruences modulo small primes. Questions of this type have been studied for the first time by L. Carlitz in the thirties. In particular, (1.13) and a part of (3.4) are due to him [2], but given there with different proofs.

1. Some arithmetic functions

For natural numbers i, define the following elements of A:

(1.1) $$[i] = T^{q^i} - T,$$

$$L_i = [i][i-1] \ldots [1], \qquad \text{and}$$

$$D_i = [i][i-1]^q \ldots [1]^{q^{i-1}}.$$

Put further $L_0 = D_0 = 1$. Obviously, $L_i = [i]L_{i-1}$ and $D_i = [i]\, D_{i-1}^q$.

Let $f \in A$ be monic, prime, of degree d dividing i. Mod f, $T^{q^d} \equiv T$, thus f divides $[i]$. Counting the number of such f, we obtain

(1.2) $$[i] = \prod f \ (\ f \text{ monic, prime, deg } f|i\ )\ ,$$

(1.3) $$D_i = \prod f \ (\ f \text{ monic, deg } f = i\ )\ , \text{ and}$$

(1.4) $$L_i = \ell.\text{c.m.}\ \{\ f|f \text{ monic, deg } f = i\ \}\ ,$$

where (1.3) and (1.4) are easy consequences of (1.2). Next, let

(1.5) $$\begin{bmatrix} k \\ i \end{bmatrix} = D_k/(D_i L_{k-i}^{q^i}) \qquad (= 0 \text{ for } i > k)$$

and

(1.6) $$e_k(z) = \sum_{i \geq 0} (-1)^{k-i} \begin{bmatrix} k \\ i \end{bmatrix} z^{q^i}\ .$$

Then $e_k(z)$ is a monic separable q-additive polynomial with coefficients in A. (q-additive: $\mathbb{F}_q$-linear; separable: coefficient of z is non-zero). Equating coefficients, we have

(1.7) $$e_k(Tz) = Te_k(z) + [k]e_{k-1}^q(z)$$

and

(1.8) $$e_k(z) = e_{k-1}^q(z) - D_{k-1}^{q-1}\, e_{k-1}(z)\ .$$

Since $\mathbb{F}_q^* \hookrightarrow K^*$ consists of the $(q-1)$-st roots of unity,

(1.9) $$\prod_{c \in \mathbb{F}_q} (X - c) = X^q - X \ .$$

By logarithmic derivation, the following frequently used formulas result:

(1.10) $$\sum 1 / (X - c) = -1 / (X^q - X)$$

(1.11) $$\sum c / (X - c) = 1 / (X^{q-1} - 1) \ .$$

Let H be a finite-dimensional $\mathbb{F}_q$-subspace of K_∞, and let

$$e_H(z) = \prod_{h \in H} (z - h) \ ,$$

which is a monic separable q-additive polynomial. Let H be a direct sum $H = U \oplus V$, and let the $\mathbb{F}_q$-spaces U', V' be defined by $U' = e_V(U)$ and $V' = e_U(V)$. Comparing zeroes, we get

(1.12) $$e_H(z) = e_{U'}(e_V(z)) = e_{V'}(e_U(z)) \ .$$

Note that composition of two q-additive polynomials results in another q-additive polynomial.

Now let $A_k = \{a \in A \mid \deg a < k\}$. (As usual, we assume the degree of $0 \in A$ to be $-\infty$.)

1.13. Proposition [2] :

(i) $e_k(z) = e_{A_k}(z) = \prod_{a \in A_k} (z - a)$;

(ii) $e_k(T^k) = D_k$.

Proof: In view of (1.3), (ii) follows from (i). Let f_k be the right hand side of (i). We use induction on k , the case $k = 1$ being given by (1.9). Thus let $k > 1$. We have $A_k = \mathbb{F}_q T^{k-1} \oplus A_{k-1}$. By induction hypothesis, $f_{k-1} = e_{k-1}$ and $e_{k-1}(T^{k-1}) = D_{k-1}$. Therefore, putting $U = e_{k-1}(\mathbb{F}_q T^{k-1})$, we have

$$e_U(z) = z^q - D_{k-1}^{q-1} z \quad .$$

Using (1.12) and (1.8),

$$f_k(z) = e_U(e_{k-1}(z)) = e_{k-1}^q(z) - D_{k-1}^{q-1} e_{k-1}(z) = e_k(z) \quad .$$

1.14. Corollary: $\sum_{a \in A_k} 1/(z - a) = \begin{bmatrix} k \\ 0 \end{bmatrix} / e_k(z)$.

Proof: Logarithmic derivation of (1.13i).

2. Power sums

For $i, k \geq 0$, define

(2.1) $s_i(k) = \sum a^k$ (a monic, deg a = i) .

In particular, $s_0(k) = 1$ and $s_i(0) = 0$ if $i > 0$. Obviously, the $s_i(k)$ satisfy congruences of Kummer type, i.e. if p is a prime ideal of A of degree d, and $k \equiv k' \bmod (q^d - 1)$, then

$$(2.2) \qquad s_i(k) \equiv s_i(k') \bmod p .$$

For these numbers, there are two recursions. Let us first consider the one concerning i. We write $a = Tb + c$ with b monic of degree $i-1$ and $c \in \mathbb{F}_q$ and get

$$s_i(k) = \sum_{b,c} (Tb+c)^k$$

$$= \sum_{j \leq k} \binom{k}{j} T^j \sum_{b,c} b^j c^{k-j} .$$

Now $\sum_{c \in \mathbb{F}_q} c^s = -1$ if $0 < s \equiv 0 \bmod (q-1)$, and zero otherwise.

Hence

$$(2.3) \qquad s_i(k) = - \sum_{\substack{j<k \\ j \equiv k \bmod (q-1)}} \binom{k}{j} T^j s_{i-1}(j) .$$

Let p be the characteristic of $\mathbb{F}_q$ and $k = \sum k_{s,p} p^s$, $j = \sum j_{s,p} p^s$ the p-adic expansions, i.e. $0 \leq k_{s,p}, j_{s,p} < p$.

Then by Lucas

(2.4) $$\binom{k}{j} \equiv \prod_{s\geq 0} \binom{k_{s,p}}{j_{s,p}} \mod p ,$$

where $\binom{k_{s,p}}{j_{s,p}} = 0$ if $k_{s,p} < j_{s,p}$. In the sequel, we often write " = " for the congruence of integers in $\mathbb{F}_p$. In particular

(2.5) $$\binom{k}{j} \neq 0 \Longleftrightarrow (j_{s,p} \leq k_{s,p}, \text{ all } s) \Longleftrightarrow \ell_p(k) = \ell_p(j) + \ell_p(k-j) .$$

Here $\ell_p(k)$ denotes the sum $\sum k_{s,p}$ of p-adic digits.

Now consider the expansions of k and j with respect to q : $k = \sum k_s q^s$, $j = \sum j_s q^s$, but now $0 \leq k_s, j_s < q$. Since these are derived in the obvious way from the p-adic expansions, (2.4) still holds, i.e.

$$\binom{k}{j} = \prod \binom{k_s}{j_s} ,$$

but (2.5) has to be replaced by

(2.6) $$\binom{k}{j} \neq 0 \Rightarrow (j_s \leq k_s, \text{ all } s) \Rightarrow \ell(j) \leq \ell(k) ,$$

$\ell(k) = \sum k_s$ = sum of q-adic digits.

(2.7) In order to control the binomial coefficients, we define the relation " $\prec$ " on non-negative integers by

$$j \prec k \Longleftrightarrow \text{(i) } j < k \text{ ; (ii) } j \equiv k \bmod (q-1) \text{ ; (iii) } \binom{k}{j} \not\equiv 0 \bmod p .$$

Since $\ell(j) \equiv j \bmod (q-1)$, $j < k$ implies $\ell(j) \leq \ell(k) - q + 1$. Further, " $<$ " is transitive, as one sees from $\binom{r}{s}\binom{s}{t} = \binom{r}{t}\binom{r-t}{r-s}$.

(2.8) Let ρ be the following operator on non-negative integers: If k is written in the form

$$k = \sum_{1 \leqq s \leqq \ell(k)} q^{e_s} ,$$

where always (i) $e_s \leqq e_{s+1}$ and (ii) $e_s < e_{s+q}$, then

$$\rho(k) = -\infty, \quad \text{if} \quad \ell(k) < q-1 , \quad \text{and}$$

$$\rho(k) = k - \sum_{1 \leqq s \leqq q-1} q^{e_s} \quad \text{otherwise} .$$

Put further $\rho(-\infty) = -\infty$, $\rho^0(k) = k$, and $\rho^i = \rho \circ \rho^{i-1}$. Example: $q = 3$, $k = 71 = 2 + 2 \cdot 3 + 3^2 + 2 \cdot 3^3$. Then $\rho(k) = 69$, $\rho^2(k) = 63$, $\rho^3(k) = 27$, $\rho^4(k) = -\infty$.

<u>2.9. Lemma:</u> If $j \leq k$ and $\ell(j) \leq \ell(k)$ then $\rho(j) \leq \rho(k)$.

<u>Proof:</u> Let e_s (resp. e'_s) be the exponents occurring in the representation (2.8) of k (resp. of j). Since $\ell(j) \leq \ell(k)$, there are less e'_s than e_s, and since $j \leq k$, the tail of j (leaving off the contribution of the first $q-1$ e'_s) is less than the tail of k.

<u>2.10. Corollary:</u> $j < k$ implies $\rho^s(j) \leq \rho^{s+1}(k)$ for all $s \geq 0$.

<u>Proof:</u> For $s = 0$, the assertion is $j \leq \rho(k)$ which follows from (2.7) and the construction of $\rho(k)$. Assume $s > 0$. From (2.7), $\ell(\rho^{s-1}(j)) \leq \ell(\rho^s(k))$ and, by induction hypothesis, $\rho^{s-1}(j) \leq \rho^s(k)$. Thus by the lemma, $\rho^s(j) \leq \rho^{s+1}(k)$.

The next proposition is a refinement of Thm. 1 in [11].

<u>2.11. Proposition:</u>

(i) For $i > 0$, $\deg s_i(k) \leq \rho(k) + \ldots + \rho^i(k)$.

(ii) If the following condition is satisfied:

(*) For $0 < s \leq i$, $\binom{k}{\rho^s(k)} \not\equiv 0 \bmod p$,

equality holds in (i).

<u>Proof:</u> (2.3) combined with (2.10) gives $\deg s_1(k) \leq \rho(k)$, i.e. (i) for $i = 1$. Now use induction on i: $\deg s_i(k) \leq \sup\{j + \deg s_{i-1}(j) \mid j < k\} \leq \sup\{j + \rho(j) + \ldots \rho^{i-1}(j)\}$ (by ind. hyp.) $\leq \rho(k) + \rho^2(k) + \ldots \rho^i(k)$, i.e. (i). Condition (*) says that $\rho^s(k)$ is the unique maximal j such that there exists a chain $j = j_s < j_{s-1} < \ldots < j_1 < k$. Now (ii) follows from (2.3).

2.12. Corollary: $s_i(k) = 0$ for $i > \ell(k)/(q-1)$. In particular, $s_i(k) = 0$ if $k < q^i - 1$.

2.13. Remark: By (2.5), (*) is automatically fulfilled for $q = p$ prime. Another example where (*) holds is given by $k = (q^i - 1) + k'$, $k' \equiv 0 \bmod q^i$, and $\ell(k') < q$, as comes from the expansion $k = (q-1)(1 + q + \ldots q^{i-1}) + k'$.

3. The generating function

Let X and z be two indeterminates over K . Then $e_i(X-z)$, considered as a polynomial in X over $K(z)$, has $\{z - a \mid a \in A_i\}$ as its set of zeroes. Thus

$$(3.1) \qquad P_{i,k}(z) = \sum_{a \in A_i} (z-a)^k$$

is the k-th power sum which may be computed by Newton's formulas [1, Ch. IV]. In view of $e_i(X-z) = e_i(X) - e_i(z)$ and (1.13), we obtain

$$(3.2) \qquad P_{i,k}(z) = 0 \qquad\qquad (k < q^i - 1) ,$$

$$P_{i,k}(z) = (-1)^i D_i/L_i = \begin{bmatrix} i \\ 0 \end{bmatrix} \qquad\qquad (k = q^i - 1) ,$$

and for $k \geq q^i$

$$P_{i,k} - \begin{bmatrix} i \\ i-1 \end{bmatrix} P_{i,k-q^i+q^{i-1}} + \ldots + (-1)^i \begin{bmatrix} i \\ 0 \end{bmatrix} P_{i,k-q^i+1} - e_i(z) P_{i,k-q^i} = 0 \; .$$

(The first two equations result from the specific form of e_i , combined with Newton.)

If we put

$$(3.3) \qquad P_i(U,z) = \sum_{k \geq 0} P_{i,k}(z) U^k \; ,$$

we arrive at

$$P_i(U,z) = \frac{(-1)^i D_i/L_i \cdot U^{q^i-1}}{1 - \begin{bmatrix} i \\ i-1 \end{bmatrix} U^{q^i-q^{i-1}} + \ldots (-1)^i \begin{bmatrix} i \\ 0 \end{bmatrix} U^{q^i-1} - e_i(z) U^{q^i}}$$

$$= \frac{(-1)^i D_i/L_i \cdot U^{q^i-1}}{e_i(U^{-1}) U^{q^i} - e_i(z) U^{q^i}} \; ,$$

and, noting $e_i(T^i) = D_i$, $P_{i,k}(T^i) = s_i(k)$,

$$(3.4) \qquad \sum_{k \geq 0} s_i(k) U^k = (-1)^i D_i/L_i \; \frac{U^{q^i-1}}{e_i(U^{-1}) U^{q^i} - D_i U^{q^i}} \; .$$

A result essentially equivalent with (3.4) has been obtained by Carlitz [2, Thm. 9.5]. Let us now derive some consequences of (3.4). Let $k < q^{i+1} - 1$. By (2.12), the highest possible non-zero s_j is $s_i = s_i(k)$ that will now be computed. Let

$k' = k - (q^i - 1)$. We may assume $k' > 0$; otherwise, $s_i(k)$ would vanish $(k' < 0)$ or equal $(-1)^i D_i/L_i (k' = 0)$. Let

(3.5) $$k' = a_N q^N + \ldots + a_i q^i \qquad (a_N \neq 0)$$

be the q-adic expansion. Since

$$e_i(U^{-1})U^{q^i} = \sum_{j\leq i} (-1)^{i-j} \begin{bmatrix} i \\ j \end{bmatrix} U^{q^i - q^j} ,$$

$s_i(k)$ is contributed by each representation of k' as a sum

(3.6) $$\sum_{j<i} \alpha_j (q^i - q^j) + \beta q^i = k' ,$$

where β and α_j are non-negative integers, as results from expanding (3.4). Now, since $k' < q^{i+1} - q^i$, the numbers $\alpha_j (j < i)$ and β are $< q$. Comparing (3.5) and (3.6), we read off:

(3.7) $$\alpha_j = 0 \qquad (j < N) ,$$

$$= q - a_N \qquad (j = N) ,$$

$$= q - 1 - a_j \qquad (N < j < i) ,$$

$$\beta = a_i + 1 - \sum_{j<i} \alpha_j ,$$

in case $N < i$, and $\alpha_j = 0$, $\beta = a_i$ if $N = i$. In particular, any solution of (3.6) is uniquely determined. If β happens to be negative, there will be no solution of the type required, and $s_i(k) = 0$. In what follows, we assume the solution (α_j, β) of (3.6) to exist. Then by (3.4),

$$(3.8) \qquad s_i(k) = (-1)^i D_i/L_i \cdot M\, D_i^{\beta} \prod_{j<i} \left((-1)^{i-j+1}\begin{bmatrix} i \\ j \end{bmatrix}\right)^{\alpha_j},$$

where M denotes the multinomial coefficient

$$M = (\alpha_0 + \ldots + \alpha_{i-1} + \beta)!/(\alpha_0! \ldots \alpha_{i-1}!\beta!)$$

(which may vanish). In order to evaluate the product, we need the easily proved formulas

$$(3.9) \qquad \prod_{t\leq s} D_t^{q-1} = D_{s+1}/L_{s+1} \qquad \text{and}$$

$$(3.10) \qquad \prod_{t\leq s} L_{s-t}^{q^t(q-1)} = D_s^q/L_s .$$

Up to the constant factor $(-1)^r M$, $s_i(k)$ equals $D_i^{1+\beta}/L_i \cdot \prod_{j<i} (D_i/D_j L_{i-j}^{q^j})^{\alpha_j}$. Let us first assume $N < i$. Then from (3.5)

$$(3.11) \qquad k = (q-1) + \ldots + (q-1)q^{N-1} + (a_N-1)q^N + a_{N+1}q^{N+1} + \ldots + a_{i-1}q^{i-1} + (a_i+1)q^i$$

$$= \sum b_j q^j$$

is the q-adic expansion of k. We may now use the relationship between (α_j,β) and b_j to express $s_i(k)$ through these coefficients. After some calculations, repeatedly applying (3.9) and (3.10), we arrive at

$$(3.12)\qquad s_i(k) = (-1)^r M \cdot \prod_{j\le i} L_{i-j}^{q^j(b_j-q+1)} \prod_{j\le i} D_j^{b_j} .$$

Note that the last factor $\prod D_j^{b_j}$ equals the value Γ_k of the Carlitz-Goss factorial at k [4], [12]. These factorials have been interpolated by Thakur [10] to a continous K_∞-valued gamma function with nice arithmetic properties. Let now $N = i$, i.e. $k = q^i - 1 + bq^i$, $0 < b < q$. In that case, by (3.7) and (3.8), $s_i(k) = (-1)^i D_i^{b+1}/L_i$, i.e. $s_i(k) = (-1)^i \Gamma_k$, as follows from the definition of Γ_k. Note this agrees with (3.12) since $b_j = q-1$ if $j < i$. It is easy to evaluate the terms M and r in (3.12). The final result (which does not distinguish between the cases $N < i$ and $N = i$) is summarized in

<u>3.13. Theorem:</u> Let $k < q^{i+1} - 1$ have the q-adic expansion $k = \sum b_j q^j$. Then

$$s_i(k) = (-1)^r \cdot M \cdot \prod_{j\le i} L_{i-j}^{q^j(b_j-q+1)} \cdot \Gamma_k ,$$

where $r = i + \sum_{j<i} (i-j+1) b_j$, and M is the multinomial coefficient $\binom{b_i}{b_0', \ldots, b_i'}$, $b_j' = q-1-b_j$ $(j < i)$, and

$b_i' = \ell(k) - i(q-1)$.

<u>3.14. Corollary:</u> In the above situation, let $i = 1$, $k = b_0 + b_1 q$, $\ell = b_0 + b_1 \geq q-1$. Then

$$s_1(k) = -\binom{b_1}{q-1-b_0} [1]^{\ell-q+1} .$$

In the special case $q = p$ prime, this result has also been obtained by Ireland-Small [8].

From (3.4), we can also derive some congruences for the $s_i(k)$. Let p be a prime of A of degree $d \leq i$. We may easily determine the order ord x of p in $x = L_i$, D_i , and $\left[\begin{matrix} i \\ j \end{matrix}\right]$, where $j < i$. Let gif(r) be the greatest integer function of $r \in \mathbb{Q}$ (which is usually denoted by $[r]$). Let further $i = i_0 + i_1 d$, $j = j_0 + j_1 d$, $0 \leq i_0, j_0 < d$.

<u>3.15. Lemma:</u>

(i) $\operatorname{ord} L_i = \operatorname{gif}(i/d)$;

(ii) $\operatorname{ord} D_i = q^{i_0} (q^{i_1 d} - 1)/(q^d - 1)$;

(iii) $\operatorname{ord} \left[\begin{matrix} i \\ j \end{matrix}\right] = (q^i - q^{i_0} - q^j + q^{j_0})/(q^d - 1) - cq^j$, where $c = i_1 - j_1$ if $i_0 \geq j_0$, and $c = i_1 - j_1 - 1$ otherwise.

Here, (iii) follows from (i) and (ii) which are direct consequences of the definitions of L_i and D_i , respectively.

Considering the cases in (ii) separately, we obtain

3.16. Lemma: $\begin{bmatrix} i \\ j \end{bmatrix} \not\equiv 0 \bmod p \Leftrightarrow j = i - d$.

3.17. Corollary: Let p be a prime of degree $d \leq i$ and $k \in \mathbb{N}$ arbitrary. The following assertions are equivalent:

(i) $d = i$ and $k \equiv 0 \mod (q^i - 1)$;

(ii) $s_i(k) \equiv -1 \mod p$;

(iii) $s_i(k) \not\equiv 0 \mod p$.

Proof: Clearly, (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) . Let us show (iii) $\Rightarrow$ (i) . Consider (3.4) reduced mod p . From $s_i(k) \not\equiv 0$, we derive $(-1)^i D_i/L_i = \begin{bmatrix} i \\ 0 \end{bmatrix} \not\equiv 0$, i.e. $d = i$. Further, $D_i/L_i \equiv (-1)^{i-1} \bmod p$, which follows for instance from (3.9). Hence the generating function mod p becomes congruent to $-U^{q^i-1}/(1 - U^{q^i-1})$, so (i) follows.

4. Computation of $s_i(q^h - 1)$

In this section, we show

4.1. Theorem:

$$s_i(q^h - 1) = \begin{cases} 0 & (h < i) \\ (-1)^i D_h/(D_{h-i}^{q^i} L_i) & (h \geq i) \, . \end{cases}$$

In contrast with the simple formula, no simple induction argument seems to apply, since in (2.3) and (3.4), arguments k which are not of the form $q^h - 1$ occur.

Our first step towards the theorem is to write

$$(4.2)\qquad s_i(q^h - 1) = \sum_{a_{i-1},\dots,a_0} (T^i + a_{i-1}T^{i-1} + \dots a_0)^{q^h-1}$$

$$= \sum_{j\leq i} T^{jq^h} K_{i,j} \qquad \text{with}$$

$$K_{i,j} = \sum_{a_{i-1},\dots,a_0} a_j/(T^i + a_{i-1}T^{i-1} + \dots a_0)\ ,$$

the $a_0, \dots, a_{i-1}$ running over $\mathbb{F}_q$, and $a_i = 1$. Thus we are reduced to determine $K_{i,j}$. We have to introduce some notation. For a k-tuple $\underline{r} = r_1, \dots, r_k$ of non-negative integers, put

$$(4.3)\qquad q(\underline{r}) = q^{r_1} + \dots + q^{r_k}\ .$$

In particular, $q(\underline{r}) = 0$ if $\underline{r}$ is the empty tuple of length 0 . Next, we define

$$(4.4)\qquad A_{i,k} = \sum T^{q(\underline{r})}\ ,$$

where $\underline{r}$ runs through those $\underline{r}$ of length k that satisfy $0 \leq r_1 \leq \dots \leq r_k < i$. Similarly, (4.5) $$B_{i,k} = \sum T^{q(\underline{r})} \ ,$$

but now with $\underline{r}$ satisfying $0 \leq r_1 < \ldots < r_k < i$. Thus, if we let

(4.6) $$g_i(X) = \prod_{0 \leq k < i} (X - T^{q^k}) \ ,$$

then $g_i(X) = \sum_{s \leq i} (-1)^s B_{i,s} X^{i-s}$. Obviously,

(4.7) $$A_{0,k} = B_{0,k} = 0 \ , \quad A_{i,0} = B_{i,0} = 1 \quad (i > 0) \ ,$$

$$B_{i,k} = 0 \quad (k > i) \ , \text{ and}$$

$$A_{i+1,k+1} = TA_{i+1,k} + A_{i,k+1}^q \ .$$

<u>4.8. Lemma:</u> Let $j > 0$, $k \geq 0$. Then $e_j(T^{j+k}) = D_j A_{j+1,k}$.

<u>Proof</u> by induction on $j + k$: The case $k = 0$ is given by (1.13). Now

$$e_j(T^{j+k+1}) = Te_j(T^{j+k}) + [j] \ e_{j-1}^q \ (T^{j+k}) \qquad \text{(by (1.7))}$$

$$= TD_j A_{j+1,k} + [j] \ D_{j-1}^q A_{j,k+1}^q \qquad \text{(ind. hyp.)}.$$

But $[j] \ D_{j-1}^q = D_j$, so $e_j(T^{j+k+1}) = D_j(TA_{j+1,k} + A_{j,k+1}^q)$ $= D_j A_{j+1,k+1}$.

We know a priori

$$(4.9) \qquad K_{i,i} = \sum_{a \text{ monic of degree } i} 1/a = (-1)^i/L_i$$

which follows from (1.14). Let us now compute $K_{i,j}(j < i)$, using (1.10) and (1.11).

$$K_{i,j} = \sum_{a_{i-1},\dots,a_0} a_j/(T^i + \dots a_0) = \sum_{a_{i-1},\dots,a_{j+1}} \sum_{a_j} a_j \sum_{a_{j-1},\dots,a_0} 1/(T^i + \dots a_0) .$$

Again by (1.14), the innermost sum equals $(-1)^j D_j/(L_j e_j(T^i + a_{i-1}T^{i-1} + \dots a_j T^j))$. Let $Q = Q(a_{i-1}, \dots ,a_{j+1}) = e_j(T^i) + \dots + a_{j+1}e_j(T^{j+1})$. Thus

$$K_{i,j} = (-1)^j D_j/L_j \cdot \sum_{a_{i-1},\dots,a_{j+1}} \sum_{a_j} a_j/(Q + a_j D_j)$$

$$= (-1)^j D_j/L_j \cdot \sum_{a_{i-1},\dots,a_{j+1}} QD_j^{q-2}/(Q^q - QD_j^{q-1}) ,$$

using (1.11). Comparing (1.11) with (1.10), we see: If we replace the factor Q in the numerator by $-D_j$, the modified sum evaluates to $K_{i,i}$. Correspondingly, replacing Q by $-a_s D_j$, where $j < s < i$, yields $K_{i,s}$. Therefore,

$$-D_j K_{i,j} = (-1)^j D_j/L_j \cdot \sum_{a_{i-1},\dots,a_{j+1}} -(e_j(T^i)+a_{i-1}e_j(T^{i-1}) + \dots + a_{j+1}e_j(T^{j+1}))D_j^{q-1}/(Q^q - QD_j^{q-1})$$

$$= e_j(T^i)K_{i,i} + e_j(T^{i-1})K_{i,i-1} + \dots + e_j(T^{j+1})K_{i,j+1} .$$

Taking (4.8) into account, this gives

$$-K_{i,j} = A_{j+1,i-j}K_{i,i} + A_{j+1,i-j-1}K_{i,i-1} + \dots + A_{j+1,1}K_{i,j+1} ,$$

i.e.

$$(4.10) \qquad \sum_{s\geq 0} A_{j+1,i-j-s}\, K_{i,i-s} = 0 \qquad (j < i) .$$

In the next section, we will prove

$$(4.11) \qquad \sum_{s\geq 0} (-1)^{i-j-s}\, A_{j+1,i-j-s}\, B_{i,s} = 0 \qquad (j < i) .$$

In view of $K_{i,i} = (-1)^i/L_i$, (4.10) and (4.11) then show by descending induction on j :

<u>4.12. Proposition:</u> $K_{i,j} = (-1)^j B_{i,i-j}/L_i$.

This in fact finishes the proof of Theorem 4.1 (modulo (4.11)): Of course, if $h < i$ then $s_i(q^h - 1) = 0$; otherwise,

$$\begin{aligned} (-1)^i L_i s_i(q^h - 1) &= (-1)^i L_i \sum_{j\leq i} T^{jq^h} K_{i,j} \\ &= \sum (-1)^{i-j} T^{jq^h} B_{i,i-j} \\ &= g_i(T^{q^h}) \qquad\qquad \text{(see (4.6))} \\ &= \prod_{0\leq j<i} (T^{q^h} - T^{q^j}) \end{aligned}$$

$$= [h][h-1]^q \ldots [h-i+1]^{q^{i-1}}$$

$$= D_h / D_{h-i}^{q^i} .$$

4.13. Remark: Possibly, using the method of Goss polynomials described in [3], one may compute sums of type $K_{i,j}$, but with powers $r > 1$ in the denominator. This would give an approach to $s_i(q^h - r)$ and (optimistically) to something like a functional equation for the Goss zeta function.

5. Some algebra

The reason for (4.11) to hold is of a general algebraic nature (an identity of Newton type between certain symmetric functions, i.e. Thm. 5.7), and does not depend on our special situation. As I could not find an equivalent result in the literature, and the induction used is tricky, I will present the complete proof.

In this section, F is an arbitrary field and $X, T_1, T_2 \ldots$ are indeterminates over F . For $i > 0$, we put

(5.1) $$A_{i,k} = \sum_{\underline{r}} T_{\underline{r}} ,$$

$\underline{r}$ running through the set of k-tuples satisfying $0 < r_1 \leq \ldots \leq r_k \leq i$, $T_{\underline{r}} = T_{r_1} \ldots T_{r_k}$. Further, let

(5.2) $$g_i(X) = \prod_{0<s\leq i} (X - T_s) = \sum_k (-1)^k B_{i,k} X^{i-k} ,$$

considered as a polynomial over $F[T_1, \ldots ,T_i]$. Spezialization $F \longrightarrow \mathbb{F}_q$, $T_r \longrightarrow T^{q^{r-1}}$ yields the numbers $A_{*,*}, B_{*,*}$ and the polynomials g_i of the last section. With the conventions $A_{i,k} = B_{i,k} = 0$ if $k < 0$, $A_{i,0} = B_{i,0} = 1$, we have

(5.3) $$A_{i+1,k} = A_{i,k} + T_{i+1}A_{i+1,k-1}$$ and

(5.4) $$B_{i+1,k} = B_{i,k} + T_{i+1}B_{i,k-1} .$$

Iterating (5.3), we arrive at

(5.5) $$A_{i+1,k} = \sum_{s\geq 0} T_{i+1}^s A_{i,k-s} .$$

<u>5.6. Lemma:</u> Let $i,k > 0$. Then $\sum_{s\geq 0} (-1)^s B_{i,s} A_{i,k-s} = 0$.

<u>Proof:</u> We use induction on i , where the case $i = 1$ reduces to $B_{1,0}A_{1,k} = B_{1,1}A_{1,k-1}$. This results from $B_{1,0} = 1$, $A_{1,k} = T_1^k$, $A_{1,k-1} = T_1^{k-1}$, $B_{1,1} = T_1$. Let $U_{i,k}$ be the sum in question. Then

$$U_{i+1,k} = \sum_{s\geq 0} (-1)^s B_{i+1,s} A_{i+1,k-s}$$

$$= \sum_{s\geq 0} (-1)^s (B_{i,s} + T_{i+1} B_{i,s-1}) \sum_{r\geq 0} T_{i+1}^r A_{i,k-s-r}$$

(by (5.4) and (5.5))

$$= \sum_{r\geq 0} T_{i+1}^r U_{i,k-r} - \sum_{r\geq 0} T_{i+1}^{r+1} U_{i,k-r-1}$$

(interchanging the summation order and collecting terms). By induction hypothesis, $U_{i,k-r}$ vanishes for $r < k$ (and it vanishes a priori for $r > k$). Hence only the terms $U_{i,0}$ contribute, i.e. $U_{i+1,k} = T_{i+1}^k U_{i,0} - T_{i+1}^{(k-1)+1} U_{i,0} = 0$, which proves the lemma.

<u>5.7. Theorem:</u> Let $0 < j \leq i$ and $k \geq i - j + 1$. Then

$$\sum_{s\geq 0} (-1)^s B_{i,s} A_{j,k-s} = 0 \ .$$

<u>Proof:</u> As usual, by induction on i , the case $i = 1$ being included in the lemma. Let $V_{i,j,k}$ be the sum in question, and let $j \leq i + 1$, $k \geq (i + 1) - j + 1$. Then

$$V_{i+1,j,k} = \sum_{s\geq 0} (-1)^s B_{i+1,s} A_{j,k-s} = \sum_{s\geq 0} (-1)^s (B_{i,s} + T_{i+1} B_{i,s-1}) A_{j,k-s}$$

$$= V_{i,j,k} - T_{i+1} V_{i,j,k-1} \ .$$

If $j \leq i$, the requirements on (i,j,k) and on $(i,j,k-1)$ are satisfied, and both terms vanish by hypothesis. If, however, $j = i+1$, then $V_{i+1,j,k} = 0$ by (5.6).

5.8. Corollary: Assertion (4.11) is true.

Proof: Put $k = i-j+1$ in (5.7), then replace j by $j+1$ (so $0 \le j < i$ instead of $0 < j \le i$), and specialize $F \longrightarrow \mathbb{F}_q$, $T_r \longrightarrow T^{q^{r-1}}$ as stated in (5.2).

5.9. Remark: Let $A_{i,k}$, $B_{i,k}$ be the elements of $A = \mathbb{F}_q[T]$ defined by (4.4), (4.5), respectively. Then $A_{i,k} = \sum_n \alpha_{i,k}(n)T^n$, $B_{i,k} = \sum_n \beta_{i,k}(n)T^n$, where $\alpha_{i,k}(n)$ (resp. $\beta_{i,k}(n)$) is the number of representations of n by k powers (resp. k different powers) of q less than q^i, considered mod p. Then (5.7) gives congruences mod p for these numbers.

6. Applications to zeta values

For $k \ge 0$, let $Z(X,k) \in A[X]$ be the polynomial $\sum_{i\ge0} s_i(k)X^i$, which is of degree $\le \ell(k)/(q-1)$ by (2.12). Then $Z(X,k)$ is closely related to the value at $-k$ of Goss's K_∞-valued zeta function (see [6], Ch. 5).

6.1 Lemma: If $0 < k \equiv 0 \bmod (q-1)$, then $Z(1,k) = 0$.

Proof:

$$Z(1,k) = \sum a^k \qquad (a \in A \text{ monic of degree } < N \text{ , some } N >> 0)$$

$$= - \sum (ca)^k \quad (a \text{ as above, } c \in \mathbb{F}_q^*)$$

$$= P_{N,k}(0) \qquad (\text{see } (3.3))$$

which is zero for N large enough.

(6.2) We define the polynomial $f_k(X) = Z(X,k)$, in case $k \not\equiv 0 \bmod (q-1)$, and $f_k(X) = Z(X,k)/(X-1)$ otherwise. Hence $f_k(1)$ equals the Goss-Bernoulli number $\beta(k)$ whose congruence properties are related to a Kummer-type criterion ([5], see also [9]). Write

$$f_k(X) = \sum f_{j,k} X^j \ .$$

(6.3) Let now k be a number of the form $k = (q^i - 1) + cq^i$, $0 < c < q$. Making extensive computations (see [6], 5.2, or [12]), Goss observed the following empirical facts:

(i) $\deg f_k(X) = i$;

(ii) $\deg f_{j,k}$ strictly increases with j , as long as $j \leq i$;

(iii) $\deg f_{i-1,k} = \deg f_{i,k} - cq^i$;

(iv) $f_{i,k} = \pm\Gamma_k$.

All of this is now included in our results. Distinguish two cases:

(6.4) <u>$c < q-1$</u> , so k is not divisible by $q-1$, and $f_{j,k} = s_j(k)$. Now $\rho^i(k) = cq^i$, $\rho^{i+1}(k) = -\infty$, and all the binomial coefficients $\binom{k}{\rho^j(k)}$ are $\not\equiv 0 \bmod p$. Thus (i), (ii), (iii) result from (2.11), and (3.13) yields $(-1)^i\Gamma_k$ for the leading coefficient, i.e. (iv).

(6.5) <u>$c = q-1$</u> , so $k \equiv 0 \bmod (q-1)$, and $f_{j,k} = -\sum_{n\leq j} s_n(k)$. We have $\rho^{i+1}(k) = 0$ and $\binom{k}{\rho^j(k)} \not\equiv 0 \bmod p$ for $j \leq i+1$. Again (2.11), combined with (6.1), implies (i), (ii), (iii). Finally, $f_{i,k}$ = leading coefficient of $f_k(X)$ = ℓ.c. of $Z(X,k) = s_{i+1}(q^{i+1}-1) = (-1)^{i+1}D_{i+1}/L_{i+1}$ (by (4.1)) $= (-1)^{i+1}\Gamma_k$ since $k = (q-1)(1+q+\ldots+q^i)$. Of course, (4.1) gives much better information in this case.

References

[1] N. Bourbaki: Algèbre. Paris: Masson 1981

[2] L. Carlitz: On certain functions connected with polynomials in a Galois field. Duke Math. J. 1, 137-168, 1935

[3] E.-U. Gekeler: On the coefficients of Drinfeld modular forms. MPI Prèprint. Bonn 1987

[4] D. Goss: Von Staudt for $\mathbb{F}_q[T]$. Duke Math. J. 45, 885-910, 1978

[5] D. Goss: Kummer and Herbrand criterion in the theory of function fields. Duke Math. J. 49, 377-384, 1982

[6] D. Goss: The arithmetic of function fields 2: The "cyclotomic" theory. J. of Algebra 81, 107-149, 1983

[7] D. Goss - W. Sinnott: Class groups of function fields. Duke Math. J. 52, 507-516, 1985

[8] K. Ireland - D. Small: A note on Bernoulli - Goss polynomials. Canad. Math. Bull. 27, 179-184, 1984

[9] S. Okada: Kummer's theory for function fields. To appear

[10] D. Thakur: Gamma functions and Gauss sums for function fields and periods of Drinfeld modules. Harvard Thesis. Cambridge 1987

[11] E. Thomas: On the zeta function for function fields over $\mathbb{F}_p$. Pacific J. Math. 107, 251-256, 1983

[12] D. Goss: The Γ-function in the arithmetic of function fields. To appear in Duke Math. J.