TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 365, Number 3, March 2013, Pages 1669–1685
S 0002-9947(2012)05699-6

ON THE ZEROES OF GOSS POLYNOMIALS

ERNST-ULRICH GEKELER

Abstract. Goss polynomials provide a substitute of trigonometric functions and their identities for the arithmetic of function fields. We study the Goss polynomials $G_k(X)$ for the lattice $A = \mathbb{F}_q[T]$ and obtain, in the case when q is prime, an explicit description of the Newton polygon $NP(G_k(X))$ of the k-th Goss polynomial in terms of the q-adic expansion of $k-1$. In the case of an arbitrary q, we have similar results on $NP(G_k(X))$ for special classes of k, and we formulate a general conjecture about its shape. The proofs use rigid-analytic techniques and the arithmetic of power sums of elements of A.

Introduction

Throughout, $\mathbb{F} = \mathbb{F}_q$ will denote a finite field with q elements, where q is a power of the natural prime p and $A = \mathbb{F}[T]$ is the polynomial ring over A in an indeterminate T. It is a well-established fact that the arithmetic of A and its quotient field $K := \mathbb{F}(T)$ is largely similar to that of their number theoretical counterparts $\mathbb{Z}$ and $\mathbb{Q}$. Both $\mathbb{Z}$ and A are euclidean rings, discrete in the completions $\mathbb{R}$ (resp. $K_\infty := \mathbb{F}((T^{-1}))$) of $\mathbb{Q}$ at the archimedean valuation (resp. of K at the place at infinity) with compact quotients $\mathbb{R}/\mathbb{Z}$ and K_∞/A. The finite abelian extensions of $\mathbb{Q}$ and K, described in both cases by classical abelian class field theory, may be explicitly constructed through the adjunction of roots of unity or torsion points of the Carlitz module, respectively. Comparable similarities hold for the non-abelian class field theories of $\mathbb{Q}$ and K, presumably governed by the predictions of the Langlands conjectures, and for topics like elliptic curves and (semi-) abelian varieties over $\mathbb{Q}$, which to some extent correspond to Drinfeld modules and their generalizations over K. Likewise, there is a strong analogy between classical (elliptic) modular forms/modular curves and Drinfeld modular forms/curves.

In both cases, the arithmetic behind modular forms is encoded in their series expansions around cusps and in the action of Hecke operators. The study of these questions for Drinfeld modular forms requires substitutes for certain classical, notably trigonometric, functions and their identities, which are routinely used in elliptic modular forms theory. The required substitute is provided by the *Goss polynomials* $G_{k,\Lambda} = G_{k,\Lambda}(X)$ of $\mathbb{F}$-lattices Λ in C_∞, the completed algebraic closure of K_∞, and in particular, the polynomials $G_k := G_{k,A}$ for the $\mathbb{F}$-lattice $\Lambda = A$. It turns out that the series $(G_k)_{k\geq 1}$ of these is crucial for the understanding of modular forms and modular curves for the group $\mathrm{GL}(2, A)$ and its congruence subgroups, and for many other topics in the arithmetic of A and K; see, e.g., [3], [4] and [9].

Received by the editors December 22, 2010 and, in revised form, August 31, 2011.
2010 *Mathematics Subject Classification.* Primary 11F52; Secondary 11G09, 11J93, 11T55.

The most important question is about the size and arithmetic nature of their zeroes. The behavior of G_k is rather erratic, depending in a complicated fashion on the p-adic expansion of $k-1$ and the vanishing/non-vanishing of certain multinomial coefficients $(\mathrm{mod}\, p)$, and a general answer, though desirable, is not in sight.

Nevertheless, besides some incomplete results for general q, we succeed in giving an explicit description of the Newton polygon of G_k over the valued field K_∞ (equivalent with the description of the size of its zeroes), in the important special case where $q = p$ is prime; see Theorem 6.12, which is our principal result. Its proof uses non-archimedean contour integration and the arithmetic of power sums of elements of A. In a weakened form, this result may be (hypothetically) generalized to arbitrary finite fields $\mathbb{F} = \mathbb{F}_q$, which is the content of Conjecture 3.10. It is compatible with extensive numerical calculations and may perhaps be approached by means different from those in this paper.

The research leading to the present result was partially carried out when the author was on sabbatical leave at the Centre de Recerca Matematica CRM at Bellaterra, Spain. With pleasure he acknowledges the support of that institution and heartily thanks its staff for their hospitality.

Notation. $A = \mathbb{F}[T]$, where $\mathbb{F} = \mathbb{F}_q$, $\#(\mathbb{F}) = q =$ power of the prime p.

$K = \mathbb{F}(T)$, endowed with the valuation v_∞ at infinity and the absolute value $|\,.\,|$ normalized such that $v_\infty(T) = -1$ and $|T| = q$.

$K_\infty = \mathbb{F}((T^{-1}))$, the completion of K w.r.t. $|\,.\,|$, with ring of integers O_∞ and maximal ideal $\mathfrak{m}_\infty$.

$C_\infty =$ the completed algebraic closure of K_∞, with its canonical extensions of $|\,.\,|$ and v_∞, denoted by the same symbols.

$B(z,r)$ the open ball $\{w \in C_\infty \mid |w-z| < r\}$ around $z \in C_\infty$ with radius $r \in |C_\infty^*|$ and corresponding closed ball $B^+(z,r) = \{w \in C_\infty \mid |w-z| \leq r\}$.

Review of Goss polynomials (see [4])**.** An $\mathbb{F}$-*lattice* (lattice for short) in C_∞ is a discrete $\mathbb{F}$-subspace Λ of C_∞. Discreteness means that Λ intersected with each ball $B^+(0,q^r)$ in C_∞ is finite. Hence

$$\Lambda = \bigcup_{r\in\mathbb{N}} \Lambda_r \tag{2.1}$$

with finite lattices $\Lambda_r = \Lambda \cap B^+(0,q^r)$, and many of the following considerations easily turn over from finite to general lattices. Assume for the moment that Λ is finite, of dimension $d \geq 1$ over $\mathbb{F}$. The *exponential function* e_Λ of Λ is defined as

$$e_\Lambda(z) := z \prod_{0\neq\lambda\in\Lambda} \left(1 - \frac{z}{\lambda}\right), \tag{2.2}$$

which is easily seen to be $\mathbb{F}$-linear, of shape

$$e_\Lambda(z) = \sum_{0\leq i\leq d} \alpha_i z^{q^i} \tag{2.3}$$

with coefficients $\alpha_i = \alpha_i(\Lambda)$, $\alpha_0 = 1$, $\alpha_d \neq 0$. Applying logarithmic differentiation, we find

$$t_\Lambda(z) := \frac{e'_\Lambda(z)}{e_\Lambda(z)} = \frac{1}{e_\Lambda(z)} = \sum_{\lambda\in\Lambda} \frac{1}{z-\lambda}. \tag{2.4}$$

The basic observation, due to David Goss [8], is that the sum

$$C_{k,\Lambda}(z) := \sum_{\lambda\in\Lambda} \frac{1}{(z-\lambda)^k}, \tag{2.5}$$

a rational function in z, may be expressed as a polynomial in t_Λ.

2.6. Theorem ([8]). *There exists a unique series* $G_{k,\Lambda}(X)$ $(k = 1, 2, 3, \ldots)$ *of polynomials with coefficients in* $\mathbb{F}(\Lambda)$ *such that* $C_{k,\Lambda}(z) = G_{k,\Lambda}(t_\Lambda(z))$. *The* Goss polynomials $G_{k,\Lambda}$ *satisfy:*

- (i) $G_{k,\Lambda}$ *is monic of degree* k *with* $G_{k,\Lambda}(0) = 0$*;*
- (ii) $G_{k,\Lambda}(X) = X(G_{k-1,\Lambda}(X) + \alpha_1 G_{k-q,\Lambda}(X) + \cdots + \alpha_i G_{k-q^i,\Lambda}(X) + \cdots)$, *where we formally put* $G_{k,\Lambda} = 0$ *for* $k \le 0$*;*
- (iii) $G_{pk,\Lambda} = (G_{k,\Lambda})^p$ $(p = \mathrm{char}(\mathbb{F}))$*;*
- (iv) $X^2 G'_{k,\Lambda}(X) = kG_{k+1,\Lambda}(X)$.

Recursion (ii) implies

$$G_{k,\Lambda}(X) = X^k \quad \text{if } k \le q, \tag{2.7}$$

and it translates to the generating function

$$G_\Lambda(u, X) := \sum_{k\ge 1} G_{k,\Lambda}(X)u^k = \frac{uX}{1 - Xe_\Lambda(u)} \tag{2.8}$$

with another indeterminate u. From (2.8) we may derive the following closed formula ([4], 3.8):

$$G_{k,\Lambda}(X) = \sum_{0\le j<k} \sum_{\underline{i}} \binom{j}{\underline{i}} \alpha^{\underline{i}} X^{j+1}, \tag{2.9}$$

where $\underline{i} = (i_0, i_1, \ldots, i_s)$ runs through the set of $(s+1)$-tuples $(s \ge 0)$ that satisfy $i_0 + i_1 + \cdots + i_s = j$ and $i_0 + i_1 q + \cdots + i_s q^s = k - 1$, $\binom{j}{\underline{i}}$ is the multinomial coefficient $\frac{j!}{i_0!\cdots i_s!}$, evaluated in $\mathbb{F}_p \hookrightarrow C_\infty$, and $\alpha^{\underline{i}} = \alpha_0^{i_0}\alpha_1^{i_1}\cdots\alpha_s^{i_s}$.

The preceding generalizes to arbitrary (not necessarily finite) lattices, where the exponential function $e_\Lambda(z)$ of (2.2) becomes a convergent possibly infinite product with an everywhere convergent power series expansion

$$e_\Lambda(z) = \sum_{i\ge 0} \alpha_i z^{q^i} \tag{2.3$'$}$$

and $C_{k,\Lambda}$ is a meromorphic function on C_∞ with poles of order k at Λ. Put for the moment $e_r := e_{\Lambda_r}$, $C_{k,r} := C_{k,\Lambda_r}$ and $G_{k,r} := G_{k,\Lambda_r}$, with Λ_r as in (2.1). Standard estimates show that for $r \longrightarrow \infty$ we have

- $e_r \longrightarrow e_\Lambda$ locally uniformly;
- $C_{k,r} \longrightarrow C_{k,\Lambda}$ uniformly on closed balls disjoint from Λ.

As a consequence, the $G_{k,r}$ converge coefficientwise toward a polynomial $G_{k,\Lambda}$ with the property $C_{k,\Lambda}(z) = G_{k,\Lambda}(t_\Lambda(z))$, where $t_\Lambda(z) = \frac{1}{e_\Lambda(z)}$. Hence all the assertions of Theorem 2.6 along with their consequences (2.7), (2.8), (2.9) remain valid for Λ.

2.10. Proposition. *Let* $c \in C_\infty$ *be a non-zero constant. The functions attached to the lattices* Λ *and* $\Lambda' = c\Lambda$ *are related by*

- (i) $e_{c\Lambda}(cz) = ce_\Lambda(z)$*;*
- (ii) $\alpha_i(c\Lambda) = c^{1-q^i}\alpha_i(\Lambda)$*;*

(iii) *$C_{k,c\Lambda}(cz) = c^{-k}C_{k,\Lambda}(z)$;*
(iv) *$G_{k,c\Lambda}(c^{-1}X) = c^{-k}G_{k,\Lambda}(X)$;*
(v) *if we write $G_{k,\Lambda}(X) = \sum_{i\leq k} g_{k,i}(\Lambda)X^{k-i}$, then*

$$g_{k,i}(c\Lambda) = c^{-i}g_{k,i}(\Lambda).$$

Proof. (i), (ii) and (iii) are straightforward from definitions. We have

$$\begin{aligned} G_{k,c\Lambda}(c^{-1}t_\Lambda(z)) &\overset{(i)}{=} G_{k,c\Lambda}(t_{c\Lambda}(cz)) = C_{k,c\Lambda}(cz) \\ &\overset{(iii)}{=} c^{-k}(C_{k,\Lambda}(z) = c^{-k}G_{k,\Lambda}(t_\Lambda(z)), \end{aligned}$$

hence (iv), and (v) is a trivial consequence. □

Note that (ii) and (v) mean that α_i (resp. $g_{k,i}$) regarded as a function on the set of lattices has weight $q^i - 1$ (resp. i).

3. THE CONJECTURE

Let $\overline{\pi} \in C_\infty$ be the Carlitz period, which is the A-analogue of the period $2\pi i$ of the classical exponential function $\exp(z)$. It is characterized up to $(q-1)$-th roots of unity through the fact that $L := \overline{\pi}A$ uniformizes the Carlitz module, the A-analogue of the multiplicative group scheme $\mathbb{G}_m$. For all of this and its arithmetic significance, see [9]. Several "classical" formulas for $\overline{\pi}$ are known ([4], 4.9–4.11); we will only need the following facts:

$$|\overline{\pi}|^{q-1} = q^q, \tag{3.1}$$

$$e_L(z) = \sum_{i\geq 0} \frac{1}{D_i} z^{q^i}, \tag{3.2}$$

where $D_0 = 1$, $D_i = [i][i-1]^q \cdots [1]^{q^{i-1}}$ for $i \geq 1$, and $[j] = T^{q^j} - T \in A$. For arithmetical reasons we are primarily interested in the $G_{k,L}$, but in view of (2.10) we may restrict ourselves to studying $G_{k,A}$, which is technically more convenient.

Therefore, from now on $\Lambda = A$, and the functions e, t, C_k, G_k without a subscript Λ will always refer to $\Lambda = A$. It is easy to verify directly (and it follows formally from the conjunction of (3.1), (3.2) and Proposition 2.10(ii)) that

$$e(z) = \sum_{k\geq 0} \alpha_k z^{q^k} \tag{3.3}$$

with $\alpha_0 = 1$, $|\alpha_1| = 1$ and $|\alpha_k| < 1$ for $k \geq 2$.

Next, let

$$\begin{array}{rccl} |\,.\,|_i : & C_\infty & \longrightarrow & \mathbb{R}, \\ & z & \longmapsto & |z|_i := \inf_{x\in K_\infty} |z-x| = \min_{x\in K_\infty} |z-x| \end{array}$$

be the "imaginary part" function on C_∞. We define the following subsets (actually, analytic subspaces) of C_∞:

$$\begin{array}{lcl} \mathcal{F} & := & \{z \in C_\infty \mid |z| = |z|_i \geq 1\}, \\ \mathcal{F}_n & := & \{z \in C_\infty \mid |z| = |z|_i = q^n\},\ n \in \mathbb{N}_0 = \{0,1,2,\ldots\}, \\ \Omega_1 & := & \{z \in C_\infty \mid |z|_i \geq 1\}. \end{array} \tag{3.4}$$

Note that always $|z|_i \leq |z|$, with equality if $\log_q |z| \notin \mathbb{Z}$. The additive group A acts through shifts $z \longmapsto z + a$ on Ω_1, and each $z \in \Omega_1$ is A-equivalent with at least one and at most finitely many $z' \in \mathcal{F}$. Hence the canonical map $A \setminus \mathcal{F} \longrightarrow A \setminus \Omega_1$ is biholomorphic, and the A-periodic meromorphic function $C_k = C_{k,A}$ (cf. (2.5)),

$$C_k(z) = \sum_{a \in A} \frac{1}{(z-a)^k} = G_k(t(z)),$$

is determined through its restriction to $\mathcal{F}$.

3.5. Lemma. *The absolute value of* $t^{q-1}(z)$ *on* $\mathcal{F}$ *is given by*

$$\log_q |t^{q-1}(z)| = q - q^{n+1}(1 - \tfrac{q-1}{q}\epsilon), \text{ if } |z| = q^{n-\epsilon},\ n \in \mathbb{N},\ 0 \le \epsilon \le 1.$$

In particular, $\log_q |t^{q-1}(z)| = q - q^{n+1}$ *for* $z \in \mathcal{F}_n$.

Proof. This follows from (2.2) and a tedious but straightforward calculation, counting the $a \in A$ below some bound and their degrees. Note that $\log_q |t_L^{q-1}| = \log_q |\overline{\pi}^{q-1}| + \log_q |t^{q-1}|$, which gives the formula (2.3) in [6]. □

3.6. Corollary. *The function* t *provides a biholomorphic isomorphism between the quotient space* $A \setminus \mathcal{F}$ *and the pointed closed ball* $B^+(0,1) \setminus \{0\}$.

Proof. We have $A \setminus \mathcal{F} \xrightarrow{\cong} A \setminus \Omega_1 \xrightarrow{\cong} B^+(0,1) \setminus \{0\}$, where the second isomorphism comes from Lemma 3.5 and the surjectivity of $e = e_A = t^{-1}$ as a map from C_∞ onto itself. □

We also note that

(3.7) For $a \in A$, the following are equivalent:

- (i) $(\mathcal{F}_n + a) \cap \mathcal{F} \neq \emptyset$;
- (ii) $\mathcal{F}_n + a = \mathcal{F}_n$;
- (iii) $a \in A_n := \{a \in A \mid \deg a \le n\}$.

It is obvious that C_k cannot have any zeroes $z \in C_\infty$ with $|z| < 1$. Accordingly, all the zeroes x of $G_k(X)$ satisfy $|x| \le 1$.

In what follows, we adopt the notation of [10], II sect. 6 for Newton polygons. That is:

(3.8) If $f(z) = \sum a_i z^i$ is a polynomial (or power series) with coefficients in C_∞, the Newton polygon $NP(f)$ of f is the lower convex hull of the points $(i, v_\infty(a_i))$ in $\mathbb{R}^2$. Then we have the following equivalent conditions about the zeroes of C_k and $G_k(X)$:

3.9. Proposition. *Let* $k \in \mathbb{N}$ *be given. The following assertions are equivalent:*

- (i) *all the zeroes* z *of* C_k *satisfy* $|z| = q^n$ *for some* $n \in \mathbb{N}_0$;
- (ii) *all the zeroes* z *of* C_k *in* $\mathcal{F}$ *lie in* $\mathcal{F}_n$ *for some* $n \in \mathbb{N}_0$;
- (iii) *all the zeroes* $x \neq 0$ *of* $G_k(X)$ *satisfy* $\log_q |x| = -q(\frac{q^n-1}{q-1})$ *for some* $n \in \mathbb{N}_0$;
- (iv) *all the slopes of the Newton polygon of* $G_k(X)$ *are of the form* $-q(\frac{q^n-1}{q-1})$ *for some* $n \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

Proof. The equivalence of (i) and (ii) comes from the A-periodicity of C_k, the equivalence of (i) or (ii) with (iii) from the definition of $G_k(X)$ and (3.5), and the equivalence of (iii) and (iv) is the characterizing property of the Newton polygon ([10], II Theorem 6.3). □

Based on numerical calculations and the study of many special cases, we make the following

3.10. Conjecture. *For each $k \in \mathbb{N}$, the equivalent assertions in Proposition* 3.9 *hold.*

We succeed in proving the conjecture in the case where $q = p$ is prime; see Theorem 6.12, which provides a neat description of the Newton polygon $NP(G_k(X))$. Its proof will occupy the largest part of this paper.

3.11. *Remark.* The Goss polynomials $G_k(X)$ of $\Lambda = A$ have their coefficients in K_∞. As elements $z \in C_\infty$ algebraic over K_∞ with $|z|_i$ not of the form q^n with some $n \in \mathbb{N}_0$ generate ramified extensions of K_∞, the conjecture would follow if the splitting field of $G_k(X)$ could be shown to be unramified over K_∞.

3.12. *Remark.* Instead of C_k, consider the complex-valued meromorphic function $\mathbf{C}_k(z) = \sum\limits_{a \in \mathbb{Z}} \frac{1}{(z-a)^k}$, with $k \geq 2$ to ensure convergence. From $\mathbf{C}_2(z) = (2\pi i)^2 \sum\limits_{n \geq 1} n q^n = (2\pi i)^2 \frac{q}{(1-q)^2}$ with $q(z) = e^{2\pi i z}$, we find by applying $\frac{d}{dz} = 2\pi i q \frac{d}{dq}$ that $\mathbf{C}_k(z)$ may be written as const. $\times \frac{\mathbf{G}_k(q(z))}{(1-q(z))^k}$ with some polynomial $\mathbf{G}_k(X) \in \mathbb{Q}[X]$. That is, $\mathbf{C}_k(z)$ vanishes for some z with $\mathrm{im}(z) > 0$ if and only if $q(z)$ is a zero of $\mathbf{G}_k(X)$. Thus $\mathbf{G}_k(X)$, some variant of an Eulerian polynomial (see [12]), is the classical counterpart of the polynomial G_k considered in the present paper.

4. CONTOUR INTEGRATION

Our argument will be based on non-archimedean contour integration as presented in [7], pp. 93–95. We briefly recall the main ingredients.

Let $B = B(z_0, q^r)$ be the "open" ball around $z_0 \in C_\infty$ with radius $q^r \in |C_\infty^*| = q^{\mathbb{Q}}$, and let $B^+ = B^+(z_0, q^r)$ be the corresponding "closed" ball, with boundary $\partial B := \{z \in C_\infty \mid |z - z_0| = q^r\}$. The ring of holomorphic functions $\mathcal{O}(\partial B)$ of ∂B is isomorphic with $C_\infty\langle v, v^{-1}\rangle$, the ring of convergent (possibly doubly infinite) Laurent series in a coordinate v of absolute value 1 on ∂B, for which we can choose $v = \frac{z - z_0}{w_0}$, where $w_0 \in C_\infty$ has absolute value $|w_0| = q^r$. An invertible element of $\mathcal{O}(\partial B)$ has the form

$$f = v^m \sum_{n \in \mathbb{Z}} a_n v^n \qquad \text{with } |a_0| > \max_{n \neq 0} |a_n|. \tag{4.1}$$

Conversely, each f with such a Laurent expansion is invertible on ∂B. The number m is well defined through the choice of an orientation on ∂B (implicit in our choice $v = \frac{z - z_0}{w_0}$) and is called the *order* $\mathrm{ord}_{\partial B}(f)$ of f at ∂B. Now if f is meromorphic on B^+, without zeroes or poles on ∂B, the formula

$$\sum_{x \in B} \mathrm{ord}_x(f) = \mathrm{ord}_{\partial B}(f) \tag{4.2}$$

holds, where $\mathrm{ord}_x(f)$ is the zero order of f at $x \in B$ (negative if f presents a pole at x).

(4.3) Let w_0 be a fixed element of C_∞ of absolute value $|w_0| = q^{r+\epsilon}$, $r \in \mathbb{N}_0$, $0 < \epsilon < 1$, and let $v := z/w_0$ be the coordinate on ∂B, where $B = B(0, q^{r+\epsilon})$.

We calculate the Laurent expansion of $C_k(z)$ on ∂B. We have for $z = w_0 v \in \partial B$, $|v| = 1$:

$$C_k(z) = \sum_{a\in A} \frac{1}{(z-a)^k} = \sum_{a\in A} \frac{1}{(w_0 v - a)^k} = \sum\nolimits_1 + \sum\nolimits_2,$$

where the first sum $\sum_1$ is over those $a \in A$ of degree at least $r+1$, i.e., $|a| > |w_0|$, and $\sum_2$ the sum over the finite set $A_r = \{a \in A \mid \deg a \le r\}$. For $|a| > |w_0|$ we find

$$\frac{1}{(z-a)^k} = \left(\frac{-1}{a(1-\frac{z}{a})}\right)^k = (-a)^{-k} \sum_{i\ge 0} \binom{-k}{i} a^{-i}(-w_0)^i v^i,$$

where the binomial coefficients $\binom{-k}{i} = (-1)^i \binom{k-1+i}{i}$ must be evaluated in C_∞. As the inner sum converges sufficiently fast, we may change the summation order and get for the first term $\sum_1$:

$$\begin{aligned} \sum_{\substack{a\in A\\ |a|>|w_0|}} \tfrac{1}{(z-a)^k} &= (-1)^k \sum_a a^{-k} \sum_{i\ge 0} \binom{k-1+i}{i} a^{-i} w_0^i v^i \\ &= (-1)^k \sum_{i\ge 0} \binom{k-1+i}{i} w_0^i \sum_{\substack{a\in A\\ |a|>|w_0|}} a^{-k-i} v^i. \end{aligned} \tag{4.4}$$

Next, let $a \in A_r$, i.e., $|a| < |w_0|$. Then

$$\frac{1}{(z-a)^k} = z^{-k} \frac{1}{(1-\frac{a}{z})^k} = w_0^{-k} v^{-k} \sum_{i\ge 0} \binom{k-1+i}{i} a^i w_0^{-i} v^{-i};$$

hence the $\sum_2$-term is

$$\sum_{a\in A_r} \frac{1}{(z-a)^k} = \sum_{i>0} \binom{k-1+i}{i} w_0^{-k-i} \sum_{a\in A_r} a^i v^{-k-i}. \tag{4.5}$$

Note that the term corresponding to $i = 0$ in (4.5) vanishes, since $\sum\limits_{a\in A_r} a^0$ is the sum over a non-trivial $\mathbb{F}$-vector space, and therefore cancels. Together with (4.4), the wanted Laurent expansion of $C_k(z)$ on $\partial B = \{z \in C_\infty \mid |z| = q^{r+\epsilon}\}$ results in

$$\begin{aligned} C_k(z) &= \sum_{n\in\mathbb{Z}} a_n v^n && \text{with} \\ a_n &= (-1)^k \tbinom{k-1+n}{n} w_0^n \sum_{a\in A,\ \deg\ a>r} a^{-k-n} && (n \ge 0), \\ a_{-k-n} &= \tbinom{k-1+n}{n} w_0^{-k-n} \sum_{a\in A_r} a^n && (n > 0) \end{aligned} \tag{4.6}$$

and $a_{-1}, \dots, a_{-k} = 0$.

It will turn out (see Lemma 6.5) that the contribution of $\sum_1$ (i.e., of those a_n with $n \ge 0$) will be negligible for our question. Therefore we focus on studying the coefficients a_{-k-n}.

5. Power sums

For $n, r \in \mathbb{N}_0$ we define the power sums

$$\begin{aligned} s_r(n) &:= \sum_{\substack{a\in A \text{ monic}\\ \text{of degree } r}} a^n \quad \text{and} \\ S_r(n) &:= \sum_{a\in A_{r-1}} a^n\ , \end{aligned} \tag{5.1}$$

where we adopt the convention that $\deg 0 = -\infty$, so $A_{-1} = \{0\}$, $S_0(n) = 0$ if $n > 0$ and $S_0(0) = 1$. Then the coefficient a_{-k-n} in (4.6) equals $w_0^{-k-n}\binom{k-1+n}{n} S_{r+1}(n)$.

Obviously, for $r > 0$,

$$\begin{aligned} S_r(n) &= 0 && \text{if } n \not\equiv 0 \pmod{q-1} \\ &= -\sum_{0\le i<r} s_i(n) && \text{if } n \equiv 0 \pmod{q-1}. \end{aligned} \tag{5.2}$$

The $s_r(n)$ are studied in [5]. For the moment we need the recursion (*loc. cit.* 2.3)

$$s_r(n) = -\sum_{\substack{m<n\\ m\equiv n \pmod{q-1}}} \binom{n}{m} T^m s_{r-1}(m),\ s_0(n) = 1, \tag{5.3}$$

which in view of (5.2) translates to the same recursion

$$S_r(n) = -\sum_{\substack{m<n\\ m\equiv n \pmod{q-1}}} \binom{n}{m} T^m S_{r-1}(m), S_0(n) = 0,\ n > 0,\ S_0(0) = 1$$

for the $S_r(n)$.

Let m, n be non-negative integers, written in their p-adic expansions

$$\begin{aligned} m &= m_{0,p} + m_{1,p}p + m_{2,p}p^2 + \cdots\ , \\ n &= n_{0,p} + n_{1,p}p + \cdots \qquad \text{with } m_{i,p}, n_{i,p} \in \{0, 1, \ldots, p-1\}, \end{aligned}$$

from which we get in the obvious way the q-adic expansions

$$\begin{aligned} &m = m_0 + m_1q + m_2q^2 + \cdots\ , \\ &n = n_0 + n_1q + \cdots \qquad \text{with } m_i, n_i \in \{0, 1, \ldots, q-1\}. \end{aligned}$$

Define the p-adic (resp. q-adic) digit sum $\ell_p(n) := n_{0,p} + n_{1,p} + \cdots$ (resp. $\ell(n) = n_0 + n_1 + \cdots$). The Lucas congruence

$$\binom{n}{m} \equiv \prod_{i\ge 0} \binom{n_{i,p}}{m_{i,p}} \pmod{p}$$

with the usual convention that $\binom{n}{m} = 0$ if $n < m$ implies

$$\begin{aligned} \tbinom{n}{m} \neq 0 \quad &\Leftrightarrow \quad (m_{i,p} \le n_{i,p} \text{ for all } i) \\ &\Leftrightarrow \quad \ell_p(n) = \ell_p(m) + \ell_p(n-m) \\ &\Rightarrow \quad (m_i \le n_i \text{ for all } i) \Rightarrow \ell(m) \le \ell(n), \end{aligned} \tag{5.4}$$

where we abuse language (as we will do in the sequel) and write "=" for the congruence of integers in $\mathbb{F}_p \hookrightarrow C_\infty$.

(5.5) Let $\rho :\ \mathbb{N}_0 \cup \{-\infty\} \longrightarrow \mathbb{N}_0 \cup \{-\infty\}$ be the following operator. Write $n \in \mathbb{N}_0$ as a sum $\sum_{1\le s\le \ell(n)} q^{i_s}$ of $\ell(n)$ powers of q, where always $i_s \le i_{s+1}$ and q^i occurs precisely n_i often. Then $\rho(n) = -\infty$ if $\ell(n) < q-1$ and $\rho(n) = n - \sum_{1 \le s \le q-1} q^{i_s}$ otherwise. Further, $\rho(-\infty) = -\infty$, $\rho^k = \rho \circ \rho^{k-1}$ for $k \geq 2$. Note that $\rho(n)$ depends only on the q-expansion of n and therefore also makes sense for arbitrary p-adic numbers $n \in \mathbb{Z}_p$. With the conventions $\deg(0) = -\infty$ and $-\infty + n = -\infty$ for $n \in \mathbb{N}_0$, we have:

5.6 Proposition ([5], Prop. 2.11). *For $r, n \in \mathbb{N}$,*

$$\deg s_r(n) \leq \rho(n) + \rho^2(n) + \cdots + \rho^r(n),$$

with equality if the the following condition is satisfied:

$$(*) \qquad \text{For } 0 < s \leq r, \ \binom{n}{\rho^s(n)} \not\equiv 0 \pmod{p}.$$

It follows from (5.4) *that* $(*)$ *always holds if $q = p$ is prime; therefore, we have an exact formula for* $\deg s_r(n)$ *in this case.*

5.7. Corollary. *$s_r(n) = 0$ if $r > \ell(n)/(q-1)$. In particular, $s_r(n) = 0$ if $n < q^r - 1$.* □

5.8. Corollary.

(i) *We also have $S_r(n) = 0$ if $r > \ell(n)/(q-1)$.*
(ii) *If $0 < n \equiv 0 \pmod{q-1}$, then $S_1(n) = -1$.*
(iii) *Let (n, r) satisfy condition $(*)$, $n \equiv 0 \pmod{q-1}$, and $2 \leq r \leq \ell(n)/(q-1)$. Then* $\deg S_r(n) = \rho(n) + \cdots + \rho^{r-1}(n)$.

Proof.

(i) Recall that $n \equiv \ell(n) \pmod{q-1}$. Further, $m < n$, $m \equiv n \pmod{q-1}$ and $\binom{n}{m} \neq 0$ implies $\ell(m) \leq \ell(n) - (q-1)$. Therefore the assertion results via induction from the recursion (5.3) for $S_r(n)$.
(ii) $S_1(n) = \sum_{c \in \mathbb{F}} c^n = -1$.
(iii) By (5.2), $S_r(n) = \sum_{i<r} s_i(n)$. The $\deg s_i(n)$ are given by (5.6), and $\deg S_r(n)$ $= \deg s_{r-1}(n) = \rho(n) + \cdots + \rho^{r-1}(n)$, since $\rho^{r-1}(n) > 0$ excludes cancellation between the $s_i(n)$. □

For later use, we add the following definitions related to ρ. Given $k \in \mathbb{N}$, let the p-adic expansion of $k-1$ be given as

$$k - 1 = k_{0,p} + k_{1,p}p + k_{2,p}p^2 + \cdots .$$

Put

$$(k-1)^* = (p-1-k_{0,p}) + (p-1-k_{1,p})p + (p-1-k_{2,p})p^2 + \cdots . \tag{5.9}$$

5.10. *Remarks.*

(i) $(k-1)^* + k - 1 = (p-1)(1 + p \cdots) = -1$, i.e., $(k-1)^* = -k$ as a p-adic number, but we will suppress this identity since it could create some confusion.
(ii) Instead of the p-adic expansion, we can use the q-adic expansion of $k-1$ in defining $(k-1)^*$, which by (i) gives the same number $(k-1)^* = -k$.

Consider the q-adic expansion

$$\begin{aligned}(k-1)^* &= \sum_{i\geq 0} \ell_i q^i, \quad \ell_i = (q-1-k_i) \in \{0,1,\ldots,q-1\}, \\ &\qquad\qquad \text{with } \ell_i = q-1 \text{ for } i \gg 0 \\ &= \sum_{s\geq 1} q^{i_s} \quad \text{with } i_s \leq i_{s+1}, \text{ where the term } q_i \text{ occurs} \\ &\qquad\qquad \text{precisely } \ell_i \text{ times as in (5.5).}\end{aligned}$$

Given $r \in \mathbb{N}_0$, define

$$\lambda_r(k) := \sum_{1\leq s\leq r(q-1)} q^{i_s}. \tag{5.11}$$

Then $\lambda_0(k) = 0 = \rho^r(\lambda_r(k))$.

6. THE CASE $q = p$ PRIME

We now come back to the situation (4.3) and the Laurent expansion (4.6) of $C_k(z)$.

6.1. Proposition. *Assume $q = p$ prime, and let $n_0 = n_0(k,r)$ be the least natural number n such that the coefficient $a_{-k-n} = w_0^{-k-n}\binom{k-1+n}{n}S_{r+1}(n)$ in* (4.6) *doesn't vanish. Then the coefficient a_{-k-n_0} dominates in the Laurent expansion* (4.6)*, i.e., $|a_{-k-n_0}| > \max\limits_{n\neq -k-n_0} |a_n|$.*

6.2. Corollary. *Conjecture* 3.10 *holds true if $q = p$. That is, all the zeroes of $C_k(z)$ in $\mathcal{F}$ actually lie in $\bigcup\limits_{r\geq 0} \mathcal{F}_r$, and the Newton polygons of the Goss polynomials $G_k(X)$ have the slopes described in Proposition* 3.9*(iv).*

Proof (modulo (6.1)*).* This has been described in (4.1). □

Before starting the proof of Proposition 6.1, we collect a number of facts and definitions.

(6.3) For $r \in \mathbb{N}_0$, let $\widetilde{\gamma}_r(k)$ be the number of zeroes z of $C_k(z)$ in $\mathcal{F}$ which satisfy $q^r \leq |z| = |z|_i < q^{r+1}$. As $A_r = \{a \in A \mid \deg a \leq r\}$ acts by shifts $z \longmapsto z + a$ on these z, $\widetilde{\gamma}_r(k) = \gamma_r(k)q^{r+1}$ with $\gamma_r(k) \in \mathbb{N}_0$.

6.4. Lemma. *Let $B^+(0,R)$ be the closed ball in C_∞ with radius $R \geq 1$. The number of zeroes minus the number of poles of C_k in $B^+(0,R)$ (counted with multiplicities) is always negative.*

Proof. Let $r_0 \in \mathbb{N}_0$ be maximal with $q^{r_0} \leq R$. The poles of C_k on $B^+(0,R)$ are the elements of A_{r_0}, each of order k, which gives $k \cdot q^{r_0+1}$ for the order of the pole divisor. Each zero z of C_k has absolute value $|z| \geq 1$ and is A-equivalent with some $z_0 \in \mathcal{F}$. Two such, z_0 and z_1, are identified under $t:\ A \setminus \mathcal{F} \xrightarrow{\cong} B^+(0,1) \setminus \{0\}$ if and only if they differ by an element of A_{r_1}, where $q^{r_1} \leq |z_0| = |z_1| < q^{r_1+1}$. Hence

$$\sum_{r_1=0}^{r_0} \gamma_{r_1}(k)$$

is an upper bound for the number of zeroes of G_k on the annulus

$$\{w \in C_\infty \mid w = t(z),\, z \in \mathcal{F},\, 1 \leq |z| = |z|_i \leq R\} \hookrightarrow B^+(0,1),$$

which is strictly less than k since $G_k(X)$ has degree k and is divisible by X. On the other hand, each zero $z \in B^+(0,R)$ of C_k is modulo A_{r_0} represented by some $z_0 \in \mathcal{F}$ as above with $q^{r_1} \le |z_0| = |z_0|_i < q^{r_1+1}$, for which there are q^{r_1+1} choices.

Hence there are at most

$$\sum_{r_1=0}^{r_0} \tilde{\gamma}_{r_1}(k) \cdot \frac{q^{r_0+1}}{q^{r_1+1}} < k \cdot q^{r_0+1}$$

many zeroes of C_k on $B^+(0,R)$. □

The lemma implies that, under the assumption that some coefficient a_m of (4.6) dominates, the corresponding index m must be negative. We may enforce that conclusion.

Assume that in the situation (4.3) C_k is not invertible on ∂B. Let $n_0 < n_1$ be the minimal and the maximal subscripts such that $|a_{n_0}| = |a_{n_1}|$ and $|a_n| \le |a_{n_0}|$ for $n \ne n_0, n_1$. In this case, C_k has $n_1 - n_0$ zeroes on ∂B. Increasing the radius $q^{r+\epsilon}$ of B slightly so that we don't pick up new zeroes or poles of C_k, we get a slightly larger open ball B', where C_k restricted to $\partial B'$ is invertible. In the resulting Laurent expansion $\sum_{z\in\mathbb{Z}} a'_n(v')^n$ of C_k on $\partial B'$ the term a'_{n_1} will dominate. Therefore, again by Lemma 6.4, $n_1 < 0$. Thus we have shown:

6.5. Lemma. *Let $m \in \mathbb{Z}$ be an index such that in the expansion* (4.6) *the equality $|a_m| = \max_{n\in\mathbb{Z}} |a_n|$ holds. Then m is strictly negative.* □

In particular, in our attempt to prove Proposition 6.1 we may restrict ourselves to considering the coefficients a_{-k-n} in (4.6):

$$a_{-k-n} = w_0^{-k-n} \binom{k-1+n}{n} S_{r+1}(n). \tag{6.6}$$

Its non-vanishing requires

$$\text{(a)} \quad \binom{k-1+n}{n} \ne 0\,; \quad \text{(b)} \quad S_{r+1}(n) \ne 0.$$

Let $k-1 = \sum_i k_{i,p}p^i$ and $n = \sum_i n_{i,p}p^i$ be the p-adic expansions. Then (a) is equivalent with $n_{i,p} + k_{i,p} < p$ for each $i \ge 0$, which is the same as $n <_p (k-1)^*$, where $(k-1)^*$ is defined in (5.9) and $a <_p b$ denotes the ordering on $\mathbb{Z}_p$ defined by the majorization of the p-adic digits of a by those of b.

The non-vanishing of $S_{r+1}(n)$ implies (and for $q = p$ is equivalent with) $\ell(n) \ge (r+1)(q-1)$ and $\ell(n) \equiv 0 \pmod{q-1}$, as follows from Corollary 5.8.

We assume for the remainder of this section that $\boxed{q = p \text{ is prime}}$, except for Remark 6.8, Proposition 6.9 and Remark 6.15, where we discuss implications for the general case. Then the minimal $n > 0$ such that a_{-k-n} doesn't vanish is

$$n_0(k,r) = \lambda_{r+1}(k) \tag{6.7}$$

with $\lambda_{r+1}(k)$ as defined in (5.11), as a moment's thought shows. (We have $\ell(n_0) = \ell_p(n_0) = (r+1)(q-1)$, the minimal value allowed by (b), $S_{r+1}(n_0) \ne 0$ by Corollary 5.8 and the assumption $q = p$, and the $(r+1)(q-1)$ digits of n_0 are placed such that n_0 is minimal with $n_0 <_p (k-1)^*$ among all n with $\ell(n) = (r+1)(q-1)$.)

Proof of Proposition 6.1. Let $n > n_0$ be such that $a_{-k-n} \neq 0$. We must show that $|a_{-k-n}| < |a_{-k-n_0}|$, which in view of $|\binom{k-1+n}{n}| = |\binom{k-1-n_0}{n_0}| = 1$ and $|w_0| = q^{r+\epsilon}$ is equivalent with

$$\deg S_{r+1}(n) - \deg S_{r+1}(n_0) < (r+\epsilon)(n-n_0).$$

Now the left-hand side is 0 for $r = 0$ and equals $(\rho(n)-\rho(n_0)) + (\rho^2(n)-\rho^2(n_0)) + \cdots + (\rho^r(n)-\rho^r(n_0))$ for $r \geq 1$, as follows from Corollary 5.8. For each $s = 1, 2, \dots r$, the numbers composed of the first $s(q-1)$ digits of n_0 (resp. n) satisfy

$$n_0 - \rho^s(n_0) \leq n - \rho^s(n),$$

since $m := n_0 - \rho^s(n_0)$ is minimal with $\ell(m) = s(q-1)$ and $m <_q (k-1)^*$. Hence, for $r \geq 1$ all the $\rho^s(n) - \rho^s(n_0)$ are less than or equal to $n - n_0$, and $\deg S_{r+1}(n) - \deg S_{r+1}(n_0) \leq r(n-n_0) < (r+\epsilon)(n-n_0)$ as desired. ☐

6.8. *Remark.* Suppress for the moment the assumption of $q = p$, and define $n_0' = n_0'(k,r)$ by the formula (6.7), i.e., $n_0' = \lambda_{r+1}(k)$. If $\binom{k-1+n_0'}{n_0'} \neq 0 \neq S_{r+1}(n_0')$, then it is obvious from Corollary 5.8 that n_0' is minimal with that property, that is, $n_0' = n_0$ as in Proposition 6.1. If moreover $(n_0, r+1)$ satisfies condition $(*)$ of Proposition 5.6, then we have an exact formula for $\deg S_{r+1}(n)$, and the proof of Proposition 6.1 also applies to this case.

On the other hand, if $r = 0$ and n_0 is as in Proposition 6.1, then since $S_1(n_0) = -1$, Proposition 6.1 also holds in this case. This means, unconditionally (i.e., for general q):

6.9. Proposition. *The function C_k has no zeroes z in $\mathcal{F}$ with $1 < |z| < q$ or, equivalently, $NP(G_k(X))$ has no slopes strictly between 0 and $-q$.*

We return to the $\boxed{\text{assumption } q = p}$ and have a closer look at the zeroes of C_k in $\mathcal{F}$. As in (6.3), and taking Corollary 6.2 into account, we let $\gamma_r(k)q^{r+1}$ be the number of zeroes of C_k in $\mathcal{F}_r$. Then $\gamma_r(k)$ equals the number of zeroes x of $G_k(X)$ with $\log_q|x| = -q(\frac{q^r-1}{q-1})$, and

$$\gamma(k) := k - \sum_{r\geq 0} \gamma_r(k) \tag{6.10}$$

is the multiplicity of 0 as a zero of G_k. We now determine these numbers.

Consider the situation (4.3) with the ball $B = B(0, q^{r+\epsilon})$. As follows from the proof of Lemma 6.4, $(\gamma_0(k) + \gamma_1(k) + \cdots \gamma_r(k))q^{r+1}$ is the number of zeroes of C_k in B, and so

$$(k - \gamma_0(k) - \cdots - \gamma_r(k))q^{r+1} = -\mathrm{ord}_{\partial B}(C_k) = k + n_0(k,r), \tag{6.11}$$

where $n_0(k,r) = \lambda_{r+1}(k)$ is the quantity that occurs in Proposition 6.1 and (6.7). This allows us to solve for $\gamma_i(k)$. The result, which encompasses all of our knowledge of the zero distribution of C_k and $G_k(X)$, is contained in the next theorem.

6.12. Theorem. *Suppose that $q = p$ is prime, and let $k-1$ be written in its q-adic expansion $k-1 = k_0 + k_1q + \cdots + k_Nq^N$, $k_N \neq 0$, $k_i = 0$ for $i > N = N(k)$. Further, let $(k-1)^* = \sum_{i\geq 0} \ell_i q^i$ with $\ell_i = q-1-k_i$ and $\lambda_i(k)$ be the numbers defined in* (5.9) *and* (5.11).

(i) *All the zeroes of* C_k *in* $\mathcal{F}$ *actually lie in* $\bigcup_{r\geq 0}\mathcal{F}_r$. *Accordingly, all the slopes of the Newton polygon of* $G_k(X)$ *are of shape* $-q(\frac{q^r-1}{q-1})$ *for some* $r\in\mathbb{N}_0$.

(ii) *The number of zeroes of* C_k *in* $\mathcal{F}_r$ *is* $\gamma_r(k)q^{r+1}$. *Accordingly, the length of the segment with slope* $-q(\frac{q^r-1}{q-1})$ *in* $NP(G_k(X))$ *is* $\gamma_r(k)$, *where* $\gamma_r(k)$ *is given by*

$$\gamma_r(k)=\frac{(q-1)k+q\lambda_r(k)-\lambda_{r+1}(k)}{q^{r+1}},\quad r\geq 0.$$

(iii) *Let* $\overline{r}(k)$ *be the least integer* r *such that* $\lambda_r(k)+k\equiv 0\,(\operatorname{mod} q^N)$. *Then* $\gamma_r(k)=0$ *for* $r\geq\overline{r}(k)$ *and* $\gamma_r(k)\neq 0$ *for* $0\leq r<\overline{r}(k)$.

(iv) *Let* $\ell(k-1)=\sum_{i\geq 0}k_i$ *be the sum of* q*-adic digits of* $k-1$, *with representative* $R(k)$ *modulo* $q-1$ *in* $\{0,1,\ldots,q-2\}$. *Then the multiplicity* $\gamma(k)$ *of* 0 *as a zero of* $G_k(X)$ *is given by*

$$\gamma(k)=(R(k)+1)q^{[\ell(k-1)/(q-1)]}$$

with Gauß brackets [.].

Proof. (i) has already been shown, and (ii) comes from solving the system (6.11) for $\gamma_r(k)$.

(iii) Given k and r, write the q-adic expansion

$$\lambda_r(k)=\sum_{i\geq 0}\ell_{r,i}q^i$$

and let $\overline{i}(r,k)$ be the least integer i such that $\ell_{r,i}<\ell_i=q-1-k_i$. E.g., $\overline{i}(0,k)=\min\{i\mid k_i<q-1\}$. Further,

- $\overline{i}(r+1,k)\geq\overline{i}(r,k)+1$ by the construction of $\lambda_r(k)$ and
- $\ell_{r,i}=0$ for $i>\overline{i}(r,k)$.

We have

$$k+\lambda_r(k)=(k_{\overline{i}(r,k)}+\ell_{r,\overline{i}(r,k)}+1)q^{\overline{i}(r,k)}+k_{\overline{i}(r)+1}q^{\overline{i}(r)+1}+\cdots.$$

Therefore, $q(k+\lambda_r(k))=k+\lambda_{r+1}(k)$ is equivalent with $\overline{i}(r+1,k)=\overline{i}(r,k)+1$ and the set of identities (with $\overline{i}:=\overline{i}(r,k)$)

$$\begin{array}{rcl} k_{\overline{i}}+\ell_{r,\overline{i}} & = & k_{\overline{i}+1}+\ell_{r+1,\overline{i}+1},\\ k_{\overline{i}+1} & = & k_{\overline{i}+2},\\ k_{\overline{i}+2} & = & k_{\overline{i}+3},\\ & \vdots & \end{array}$$

As $k_i=0$ for i large, the latter holds if and only if $k_{\overline{i}}+\ell_{r,\overline{i}}=\ell_{r+1,\overline{i}+1}$ and $k_{\overline{i}+1}=k_{\overline{i}+2}=\cdots=0$. Now we have the equivalences:

$$\begin{aligned}
&\gamma_r(k)=0\Leftrightarrow q(k+\lambda_r(k))=k+\lambda_{r+1}(k)\quad\text{(from (ii))}\\
&\Leftrightarrow\overline{i}(r+1,k)=\overline{i}(r,k)+1\text{ and, with }\overline{i}=\overline{i}(r,k),\ k_{\overline{i}}+\ell_{r,\overline{i}}=\ell_{r+1,\overline{i}+1},\\
&\qquad k_{\overline{i}+1}=k_{\overline{i}+2}=\cdots=0\\
&\Leftrightarrow\overline{i}(r,k)\geq N(k)\\
&\Leftrightarrow\lambda_r(k)+k\equiv 0\,(\operatorname{mod} q^{N(k)})\\
&\Leftrightarrow r\geq\overline{r}(k).
\end{aligned}$$

This shows (iii).

(iv) From (6.10) and (6.11) we see that $\gamma(k) = \lim_{r\to\infty} \dfrac{k+\lambda_r(k)}{q^r}$, where by (iii) the limit is attained for $r = \overline{r} := \overline{r}(k)$. Now $\overline{r}$ is minimal such that $\overline{r}(q-1) \geq \ell_0+\ell_1+\cdots+\ell_{N-1} = N(q-1)-\ell(k-1)+k_N$, i.e., such that

$$(N-\overline{r})(q-1)+k_N \leq \ell(k-1).$$

Our $\lambda_{\overline{r}}(k)$ has q-expansion $\ell_0+\ell_1 q+\cdots+\ell_{N-1}q^{N-1}+aq^N+bq^{N+1}$ with $b=0$ if $a+k_N < q-1$. The remainder $a+b$ satisfies $a+b \in \{0,1,\ldots,q-2\}$ and

$$a+b = \overline{r}(q-1)-(\ell_0+\ell_1+\cdots+\ell_{N-1}) = \ell(k-1)-k_N-(N-\overline{r})(q-1).$$

Let $R := R(k)$ be the representative $(\operatorname{mod} q-1)$ of $\ell(k-1)$ in $\{0,1,\ldots,q-2\}$, and consider the cases

$$\text{(I)} \quad R \geq k_N \quad \text{and} \quad \text{(II)} \quad R < k_N.$$

In case (I), $a+b = R-k_N$ and $N-\overline{r} = [\frac{\ell(k-1)}{q-1}]$. As $R-k_N \leq q-1-k_N$, $a = R-k_N$ and $b=0$. We find $k+\lambda_{\overline{r}}(k) = (R+1)q^N$, and thus $\gamma(k) = (R+1)q^{N-\overline{r}} = (R+1)q^{[\ell(k-1)/(q-1)]}$.

In case (II), $a+b = q-1+R-k_N$, $a = q-1-k_N$, $b=R$, and $N-\overline{r} = [\ell(k-1)/(q-1)]-1$. In this case, $k+\lambda_{\overline{r}}(k) = (R+1)q^{N+1}$, and so $\gamma(k) = (R+1)q^{N+1-\overline{r}} = (R+1)q^{[\ell(k-1)/(q-1)]}$. □

6.13. *Remark.* The formula in Theorem 6.12(iv) for $\gamma(k)$ has been found empirically by F. Pellarin, in a slightly different but equivalent form. The quantity $\gamma(k)$ plays a crucial role in the study of Drinfeld modular forms, their expansions around cusps [8], [4], the geometry of Drinfeld modular curves [3], and presumably for zero estimates in the transcendence theory of Drinfeld modular forms and related functions [1], [2], [11].

We present two numerical examples which display all the ingredients of the theorem.

6.14. Examples.

(i) Let $q=p=3$ and $k=43$, $k-1 = 2\cdot 3+3^2+3^3$. Then $\ell(k-1)=4$ and $R(k)=0$. Further, $(k-1)^* = 2+0\cdot 3+3^2+3^3+2\cdot 3^4+2\cdot 3^5+\cdots$, so $\lambda_0(k)=0$, $\lambda_1(k)=2$, $\lambda_2(k)=2+3^2+3^3$, $\lambda_3(k)=2+3^2+3^3+2\cdot 3^4, \cdots$. The formulas of Theorem 6.12 imply $\gamma_0(k)=28$, $\gamma_1(k)=6$, $\gamma_2(k)=\gamma_3(k)\cdots=0$, $\gamma(k)=9$, which is equivalent to stating that the breakpoints of $NP(G_{43}(X))$ are $(9,18),(15,0),(43,0)$.

(ii) Let $q=p=2$ and $k=49$, $k-1=2^4+2^5$. Then $\ell(k-1)=2$ and $R(k)=0$, $(k-1)^* = 1+2^2+2^3+2^6+2^7+\cdots$, so $\lambda_0(k)=0$, $\lambda_1(k)=1$, $\lambda_2(k)=3$, $\lambda_3(k)=7$, $\lambda_4(k)=15$, $\lambda_5(k)=79$. Theorem 6.12 gives $\gamma_0(k)=24$, $\gamma_1(k)=12$, $\gamma_2(k)=6$, $\gamma_3(k)=3$, $\gamma_4(k)=\gamma_5(k)=\cdots=0$, $\gamma(k)=4$. The breaks of $NP(G_{49}(X))$ are $(4,102),(7,60),(13,24),(25,0),(49,0)$.

6.15. *Remark.* Again suppress the assumption $q=p$, and let $k-1 = \sum_{0\leq i\leq N} k_i q^i$, $k_N \neq 0$, be the q-adic expansion. Let k have the following property:

(A) For $r \geq 0$, the number $n_0' = n_0'(k,r) := \lambda_{r+1}(k)$ satisfies $\binom{k-1+n_0'}{n_0'} \neq 0$, that is, $\lambda_{r+1}(k) <_p (k-1)^*$.

Note that for $0 \leq s \leq r+1$ the relation

$$\rho^s(\lambda_{r+1}(k)) = \lambda_{r+1}(k)-\lambda_s(k)$$

holds. The identities $\binom{a}{b}\binom{b}{c} = \binom{a}{c}\binom{a-c}{a-b}$ and $\binom{a}{b} = \binom{a}{a-b}$ for binomial coefficients show that the following condition is also satisfied:

(B) For $r \geq 0$ and $0 < s \leq r+1$, $\binom{n_0'(k,r)}{\rho^s(n_0'(k,r))} \neq 0$ in C_∞.

Therefore Remark 6.8 applies, $n_0'(k,r) = n_0(k,r)$ as in Proposition 6.1, and all the statements of Proposition 6.1, Corollary 6.2 and also of Theorem 6.12 remain valid for such k even if q fails to be prime. That is, $G_k(X)$ has only the slopes described in Theorem 6.12(ii), with widths given by the formulas in Theorem 6.12(iii) and (iv).

7. Results for general q

In this last section q is allowed to be an arbitrary prime power. We first point out that Proposition 6.9, covering a small part of the assertions of Conjecture 3.10, is established for such general q. Next, we describe two series of natural numbers k where condition (A) (thus also (B)) of Remark 6.15 is fulfilled. In these cases, we have complete control of the Newton polygon of $G_k(X)$.

7.1. Example. Let k have the shape $q^r - 1$ with $r \in \mathbb{N}$. In that case, a closed expression for $G_k(X)$ is known ([4], (3.10) and (4.3)):

$$G_{k,L}(X) = X^{q^r-1} + \widetilde{\beta}_1 X^{q^r-q} + \cdots + \widetilde{\beta}_{r-1} X^{q^r-q^{r-1}}$$

with $\widetilde{\beta}_i = \frac{(-1)^i}{L_i}$, where $L_i := [i][i-1]\cdots[1] \in A$ has degree $q(\frac{q^i-1}{q-1})$ (see (3.2)). Together with $L = \overline{\pi}A$ and Proposition 2.10(v), we find

$$G_k(X) = G_{k,A}(X) = X^{q^r-1} + \beta_1 X^{q^r-q} + \cdots + \beta_{r-1} X^{q^r-q^{r-1}}$$

with coefficients $\beta_i \in C_\infty$ that satisfy $|\beta_i| = 1$ for $1 \leq i \leq r-1$. Hence we know a priori for such k that $\gamma_0(k) = q^{r-1} - 1$, $\gamma_i(k) = 0$ for $i > 0$, and $\gamma(k) = q^r - q^{r-1}$. This may also be seen using Remark 6.15.

Viz, the q-adic expansions for $k = q^r - 1$ are

$$\begin{aligned} k-1 &= (q-2) + (q-1)q + \cdots (q-1)q^{r-1}, \\ (k-1)^* &= 1 + (q-1)q^r + (q-1)q^{r+1} + \cdots , \end{aligned}$$

so $\lambda_1(k) = 1 + (q-2)q^r$, $\lambda_2(k) = 1 + (q-1)q^r + (q-2)q^{r+1}, \ldots$. Therefore, condition (A) is fulfilled, and the formulas of Theorem 6.12 yield $\gamma_0(k) = \frac{(q-1)k - \lambda_1(k)}{q} = q^{r-1} - 1$, $\gamma_1(k) = \gamma_2(k) = \cdots = 0$, $\ell(k-1) = r(q-1) - 1$, $R = q-2$, $\gamma(k) = (q-1)q^{r-1}$.

7.2. Example. Let k have the shape $q^r + 1$ with $r \in \mathbb{N}$. Then

$$\begin{aligned} k-1 &= q^r, \\ (k-1)^* &= (q-1) + (q-1)q + \cdots + (q-1)q^{r-1} + (q-2)q^r + (q-1)q^{r+1} + \cdots , \\ \lambda_i(k) &= (q-1) + (q-1)q + \cdots + (q-1)q^{i-1} \quad (i \leq r), \\ \lambda_{r+s}(k) &= (q-1) + \cdots (q-1)q^{r-1} + (q-2)q^r + (q-1)q^{r+1}, \\ &\quad + \cdots (q-1)q^{r+s-1} + q^{r+s} (s > 0). \end{aligned}$$

Obviously, condition (A) is fulfilled, and we get

$$\begin{array}{lcl} \gamma_0(k) & = & (q-1)q^{r-1}, \\ \gamma_1(k) & = & (q-1)q^{r-2}, \\ & \vdots & \\ \gamma_{r-1}(k) & = & q-1, \\ \gamma_r(k) & = & 0 = \gamma_{r+1}(k) = \gamma_{r+2}(k) = \cdots . \end{array}$$

Furthermore, $\ell(k-1) = 1$, so $R = 1$ (resp. 0) if $q > 2$ (resp. $q = 2$), and in both cases $\gamma(k) = 2$.

Now we give two formulas for $\gamma_0(k)$ valid for arbitrary k and q.

7.3. Proposition. *Given k, let $\overline{j} = \overline{j}(k)$ be the largest integer j such that the binomial coefficient $\binom{k-1-j(q-1)}{j}$ doesn't vanish in $\mathbb{F}_p$, and let $n_0(k,0)$ be the least natural number n divisible by $q-1$ and such that $\binom{k-1+n}{n} \neq 0$. Then* (i) *$\gamma_0(k) = (q-1)\overline{j}(k)$ and* (ii) *$\gamma_0(k) = \frac{(q-1)k - n_0(k,0)}{q}$ hold.*

Remarks.

(i) In view of Corollary 5.8(ii), $n_0(k,0)$ agrees with the quantity defined in Proposition 6.1. By (6.7) it equals $\lambda_1(k)$ if $q = p$.

(ii) Going through painful case distinctions on the p-adic expansion of k, we could directly show the identity of the two expressions for $\gamma_0(k)$. It is however easier to verify both formulas independently.

Proof of Proposition 7.3.

(i) Consider the series expansions (2.3) of $e_A(z) = \sum_{i \geq 0} \alpha_i z^{q^i}$ ($\alpha_i \in O_\infty$) and $e_{\mathbb{F}}(z) = z - z^q$. Right from definitions, we have the coefficientwise congruence $e_A(z) \equiv e_{\mathbb{F}}(z)$ modulo the maximal ideal $\mathfrak{m}_\infty$ of O_∞, which implies

$$G_k(X) = G_{k,A}(x) \equiv G_{k,\mathbb{F}}(X) \pmod{\mathfrak{m}_\infty}.$$

Therefore,

$$\begin{array}{lcl} \gamma_0(k) & = & \text{number of zeroes (counted with multiplicities)} \\ & & \text{of } G_k(X) \text{ of absolute value } 1 \\ & = & \text{number of zeroes } x \neq 0 \text{ of } G_{k,\mathbb{F}}(X). \end{array}$$

From (2.9) we may derive the closed formula (see also [4], 3.7),

$$G_{k,\mathbb{F}}(X) = \sum_{j \geq 0} (-1)^j \binom{k-1-j(q-1)}{j} X^{k-j(q-1)},$$

which implies the assertion.

(ii) Due to Remark 6.8 and Proposition 6.9, the identity (6.11) is valid for $r = 0$ and arbitrary q with our value of $n_0(k,0)$. □

The number $\overline{j}(k)$ may be easily determined for $k = q^r - 1$ or $q^r + 1$, which of course reproduces the results of Examples 7.1 and 7.2, respectively. We finish with an example (necessarily with $q \neq p$) where the formulas of Proposition 7.3 produce a result different from the formula in Theorem 6.12(ii), i.e., where $n_0(k,0) \neq \lambda_1(k)$.

7.4. Example. Let $q = p^2$, and let the q-expansion of $k-1$ start with

$$\begin{array}{lcl} k-1 & = & 1 + (p-1)q + \cdots , \\ (k-1)^* & = & (q-2) + (0 + (p-1)p)q + \cdots . \end{array}$$

Then $\lambda_1(k) = (q-2)+q$, so $\binom{k-1+\lambda_1(k)}{\lambda_1(k)}$ vanishes by the Lucas congruence. Therefore, $n_0(k,0)$ is strictly larger than $\lambda_1(k)$.

Conclusion

Since Conjecture 3.10 is of a qualitative nature, there is some hope for a conceptual proof valid in the general case (q not necessarily prime), perhaps by rigid-analytic means and using properties of the functions C_k, or following Remark 3.11. On the other hand, as the behavior $(\bmod\, p)$ of the multinomial coefficients in (2.9) or the binomial coefficients in (4.6) is difficult to control, it is hardly imaginable that there exists a general description of $NP(G_k(X))$ similarly explicit as the one supplied by Theorem 6.12 in the case $q = p$.

References

[1] Bosser, V.; Pellarin, F.: Hyperdifferential properties of Drinfeld quasi-modular forms. Int. Math. Res. Not. 11 (2008). MR2428858 (2009e:11092)

[2] Bosser, V.; Pellarin, F.: On certain families of Drinfeld quasi-modular forms. J. Number Theory 129, 2952–2990 (2009). MR2560846 (2010k:11075)

[3] Gekeler, E.-U.: Drinfeld modular curves. Lect. Not. Math. 1231, Springer-Verlag 1986. MR874338 (88b:11077)

[4] Gekeler, E.-U.: On the coefficients of Drinfeld modular forms. Invent. Math. 93, 667–700 (1988). MR952287 (89g:11043)

[5] Gekeler, E.-U.: On power sums of polynomials over finite fields. J. Number Theory 30, 11–26 (1988). MR960231 (89k:11122)

[6] Gekeler, E.-U.: Zero distribution and decay at infinity of Drinfeld modular coefficient forms. Int. J. Numb. Theory 7, no. 3, 671–693 (2011). MR2805575

[7] Gerritzen L.; van der Put, M.: Schottky groups and Mumford curves. Lect. Not. Math. 817, Springer-Verlag 1980. MR590243 (82j:10053)

[8] Goss, D.: The algebraist's upper half-plane. Bull. Am. Math. Soc. NS 2, 391–415 (1980). MR561525 (81g:10042)

[9] Goss, D.: Basic structures of function field arithmetic. Ergeb. Math. Grenzgeb. Vol. 35, Springer-Verlag 1996. MR1423131 (97i:11062)

[10] Neukirch, J.: Algebraic number theory. Grundlehren der Math. Wiss. 322, Springer-Verlag 1999. MR1697859 (2000m:11104)

[11] Pellarin, F.: Aspects de l'indépendance algébrique en caractéristique non-nulle (d'après Anderson, Brownawell, Denis, Papanikolas, Thakur, Yu, et al.). Séminaire Bourbaki Vol. 2006/2007, Esp. No. 973. Astérisque 317, 205–242 (2008). MR2487735 (2010c:11086)

[12] http://oeis.org/wiki/Eulerian_polynomials.

FR 6.1 Mathematik, Universität des Saarlandes, Postfach 15 11 50, D-66041 Saarbrücken, Germany

E-mail address: `gekeler@math.uni-sb.de`