Rend. Sem. Mat. Univ. Padova, DRAFT, 1–37

# Hasse-Witt matrices for polynomials, and applications

Régis Blache (∗)

Abstract – In a classical paper, Manin gives a congruence [15, Theorem 1] for the characteristic polynomial of the action of Frobenius on the Jacobian of a curve $C$, defined over the finite field $\mathbf{F}_q$, $q = p^m$, in terms of its Hasse-Witt matrix.

The aim of this article is to prove a congruence similar to Manin's one, valid for any $L$-function $L(f, T)$ associated to the exponential sums over affine space attached to an additive character of $\mathbf{F}_q$, and a polynomial $f$. In order to do this, we define a Hasse-Witt matrix $\mathrm{HW}(f)$, which depends on the characteristic $p$, the set $D$ of exponents of $f$, and its coefficients.

We also give some applications to the study of the Newton polygon of Artin-Schreier (hyperelliptic when $p = 2$) curves, and zeta functions of varieties.

Mathematics Subject Classification (2010). Primary: 11M38; Secondary: 11T23, 14G15, 11G25.

Keywords. Zeta and $L$-functions in characteristic $p$, $p$-adic estimates for character sums, Newton polygons of curves.

## Contents

1. Introduction . . . . . 2
1.1 – *Description of the main result* . . . . . 2
1.2 – *Applications to Artin-Schreier (hyperelliptic) curves* . . . . 4
1.3 – *Applications to zeta functions* . . . . . 5
1.4 – *Structure of the paper* . . . . . 6

(∗) *Indirizzo dell'A.*: Équipe LAMIA, INSPÉ de la Guadeloupe Morne Ferret 97139 Les Abymes F.W.I.
E-mail: regis.blache@univ-antilles.fr

2. The congruence . . . . . 7
2.1 – *Dwork's trace formula* . . . . . 8
2.2 – *Decomposition of the coefficients of a Fredholm determinant* 10
2.3 – *Minors and solutions of modular equations: the convergence radius* . . . . . 13
2.4 – *Minimal solutions of modular equations* . . . . . 15
2.5 – *Minimal minors and minimal solutions.* . . . . . 20
2.6 – *The Hasse-Witt matrix of a polynomial* . . . . . 21
2.7 – *The main theorem.* . . . . . 22
3. Examples and applications . . . . . 25
3.1 – *Some polynomials in one variable, and Artin-Schreier curves* 25
3.2 – *Some hyperelliptic curves in characteristic two* . . . . . 27
3.3 – *Hasse-Witt matrix of a polynomial, when the characteristic is large enough* . . . . . 29
3.4 – *Zeta functions of affine varieties* . . . . . 32
References . . . . . 35

## 1. Introduction

### 1.1 – *Description of the main result*

Let $n \geq 1$ denote an integer, and

$$f(\mathbf{x}) = \sum c_{\mathbf{d}} \mathbf{x}^{\mathbf{d}} \in \mathbf{F}_q[x_1, \ldots, x_n]$$

a $n$-variable polynomial having its coefficients in $\mathbf{F}_q$. For any $r \geq 1$, we denote by $\mathbf{F}_{q^r}$ the degree $r$ extension of the field $\mathbf{F}_q$ inside a fixed algebraic closure $\overline{\mathbf{F}}_q$. Choose a non trivial additive character $\psi$ of $\mathbf{F}_p$. We define the family of exponential sums $(S_r(f))_{r\geq 1}$ and the associated $L$-function

$$S_r(f) := \sum_{\mathbf{x}\in(\mathbf{F}_{q^r})^n} \psi\left(\mathrm{Tr}_{\mathbf{F}_{q^r}/\mathbf{F}_p} f(\mathbf{x})\right);\ L(f;T) := \exp\left(\sum_{r\geq 1} S_r(f)\frac{T^r}{r}\right)$$

This is a rational function with coefficients in $\mathbf{Z}[\zeta_p]$ [8]. Let us write it

$$L(f,T) = \frac{\prod_{i=1}^{s}(1-\alpha_i T)}{\prod_{j=1}^{t}(1-\beta_j T)}$$

Its reciprocal roots $\alpha_1, \dots, \alpha_s$ and poles $\beta_1, \dots, \beta_t$ are algebraic integers whose complex absolute values lie in the set $\{q^{\frac{i}{2}},\ 0 \leq i \leq 2n\}$; moreover they are $\ell$-adic units for any prime $\ell \neq p$.

Here we are concerned with the $p$-adic values of these numbers. From now on we consider all numbers above as elements of $\overline{\mathbf{Q}}_p$, the algebraic closure of the field of $p$-adic numbers. We use the absolute value on the field $\overline{\mathbf{Q}}_p$ that extends $|\cdot|_p$ on $\mathbf{Q}_p$ defined by $|p|_p = p^{-1}$.

Set $R := \max\{|\alpha_i|_p, |\beta_j|_p\}^{-1}$. The function $L(f,T)$ converges in the open disk $D(0, R^-)$ of $\mathbf{C}_p$, the completion of $\overline{\mathbf{Q}}_p$ with respect to $|\cdot|_p$, and we have $||L(f,T)|| = 1$ in this disk. We denote by $\mathfrak{R}_R$ the ring of functions bounded by 1 in this disk, and by $\mathfrak{I}_R$ the ideal of functions strictly bounded by 1. Our main result is Theorem 1, that gives a (generically) nontrivial congruence for $L(f,T)$ modulo the ideal $\mathfrak{I}_R$ when $f$ varies among polynomials with prescribed exponents.

Let us describe what radius $R$ we shall use. Given a polynomial $f$, the radius $R$ is not known in general. But when $f$ varies in a family, good bounds are available. A general strategy to estimate $R$ is to give, for any $r \geq 1$, a lower bound $\delta$ on the $q^r$-adic valuation of the sum $S_r(f)$ that is independant on $r$; then one can choose $R = q^\delta$. Note that since we consider exponential sums on the whole affine space, we always have $\delta > 0$, and $R > 1$. As a consequence, the $L$-function always has trivial unit root factor.

The divisibility of exponential sums has drawn much attention, and we describe only some relevant results here. Sperber [26, Theorem 1.2] has given a bound depending on the degree of the polynomial $f$; later Adolphson and him have refined it [1, Theorem 1.2], taking into account the Newton polytope at infinity of $f$. Both bounds are independent on the characteristic, and can be tight only for primes $p$ in certain congruence classes [26, Theorem 3.14], [27, Theorem 2]. Thus we shall not use them, since we want our congruence to be non trivial as often as possible. We have to consider smaller families, and sharper bounds.

Let us fix a finite $D \subset \mathbf{N}^n$, not contained in any coordinate hyperplane; we denote by $\mathbf{F}_q[D]$ the vector space of polynomials having their coefficients in $\mathbf{F}_q$ and their exponents in $D$. Moreno *et al.* [18] have given a tight bound on the divisibility of the sums $S_r(f)$, $f \in \mathbf{F}_{q^r}[D]$. It is the minimal $p$-weight of a solution $U = (u_{\mathbf{d}})_{\mathbf{d}\in D} \in \{0, \dots, q^r - 1\}^{|D|}$ of the equation

$$\sum_D u_{\mathbf{d}}\mathbf{d} \equiv 0 \mod q^r - 1,\ \sum_D u_{\mathbf{d}}\mathbf{d} \in (\mathbf{N}_{>0})^n.$$

But this depends on $p, D$ and $r$, and is not uniform enough for our purposes.

In [7], we have studied the system formed by these equations when $r$ varies. We have introduced an invariant $\delta_p(D) \in \mathbf{Q}_{>0}$, the $p$-density of the set $D$, and we have shown that for any $f \in \mathbf{F}_q[D]$, each of the reciprocal roots and poles of the $L$-function $L(f;T)$ has $p$-adic absolute value at most $q^{-\delta_p(D)}$ [7, Theorem 2.1]. We shall choose $R = q^\delta$ in the following with $\delta := \delta_p(D)$.

Our proof is based on Dwork's trace formula: we express the $L$-function as an alternate product of Fredholm determinants. We express the coefficients of these entire functions from minors of $p$-adic (infinite) matrices. We use a suitable decomposition of such a minor in terms of some products of coefficients of the matrix. Then we show that such a product corresponds to a solution of the modular equation defined above, and that its valuation is at least the $p$-weight of the corresponding solution. We are lead to the study of solutions with minimal $p$-weight of the modular equation. These solutions can be written from finite sets of base $p$ digits, which are used to define the Hasse-Witt matrix $\mathrm{HW}(f)$ for the polynomial $f$. This gives the right hand side of the congruence.

Notice that the only hypothesis on the polynomial $f$ is that all variables effectively appear, and we have no hypothesis on the prime $p$. Note also that a common feature of the congruence given here and Manin's one is that they are "generic" congruences. In other words the congruence can be trivial (the right hand side is 1) for a given polynomial (Manin's congruence is trivial when the curve has $p$-rank 0), but when $f$ varies among polynomials with prescribed exponents, it is generically non trivial, even if the matrix $\mathrm{HW}(f)$ can be generically singular. Finally, notice that all invariants defined here really depend on the set $D$, not on its convex closure.

We turn to applications. Our aim is twofold: on one hand we generalize known results, on the other we illustrate the calculations, and the phenomena that can occur.

### 1.2 – *Applications to Artin-Schreier (hyperelliptic) curves*

Assume here that the $L$-function (or its inverse) is a polynomial for any $f \in \overline{\mathbf{F}}_q[D]$ (this is the case when $n = 1$); then we can consider its Newton polygon $\mathrm{NP}_q(f) := \mathrm{NP}_q(L(f;T)^{(-1)^{n+1}})$ with respect to the $q$-adic valuation. The study of these polygons has drawn some attention (see for instance [21, 27, 29, 6]), but not much is known.

It is shown in [7] that the first slope of the generic Newton polygon is the density $\delta = \delta_p(D)$. From Theorem 1, we deduce that the length of the segment with slope $\delta$ is the stable rank $\mathrm{s}(f)$ of the semi-linear matrix

$\mathrm{HW}(f)$. When $f$ varies in $\overline{\mathbf{F}}_q[D]$, the stable rank attains a maximum s in a Zariski open subset. In other words, the first vertex of the generic Newton polygon associated to this family of $L$-functions is $(\mathrm{s}, \mathrm{s}\,\delta)$, and we can compute the Hasse polynomial associated to this vertex, i.e. the equation of the Zariski closed subset of those $f$ such that $\mathrm{NP}_q(f)$ passes strictly above this vertex.

This problem has been studied when $n = 1$, in the cases $p >> \max D$ [25], and $p = 2$ [24], in connection with the study of the first slope of Newton polygons of Artin-Schreier curves (hyperelliptic curves when $p = 2$). The technique in these papers (see also [19]) is to compute the Verschiebung action on the first de Rham cohomology space of a curve by taking power series expansions at a rational point, and to use Katz' sharp slope estimate [14].

The above Theorem provides a new treatment of these questions, that gives more precise results and further generalizations. For instance, we compute the Hasse-Witt matrix of a polynomial of degree $p^h - 1$ in characteristic $p$, and deduce Theorem 2: there does not exist any supersingular $p$-cyclic covering of the projective line in characteristic $p$ having genus $(p-1)(p^h-2)/2$ when $h(p-1) > 2$ (the case $p = 2$ is [24, Theorem 1.2]).

Then we treat the case of genus $g = 10$ hyperelliptic curves in characteristic 2 having 2-rank zero; the case of genera $1 \leq g \leq 9$ has been studied in [23]. This illustrates some phenomena: the Hasse-Witt matrix can be generically singular, and it really depends on the set $D$, not only on its convex closure. This also gives a way to produce curves having "high" Newton polygon, and a counterexample to an expectation of Oort [20]: see Remark 3.3.

Finally, we consider the higher dimensional case when the characteristic is large enough; we show Proposition 3.9 that generalizes [25, Theorem 1.1].

### 1.3 – *Applications to zeta functions*

We turn to the study of zeta functions of varieties.

The question of the $p$-divisibility of their numbers of points in characteristic $p$ has drawn much attention since the celebrated Chevalley-Warning theorem [28]. In particular, Ax' Theorem [4] gives the generic radius of convergence of the zeta function of an affine hypersurface with fixed degree, and Katz' Theorem [11, Theorem 1.0] gives the same result for an intersection of hypersurfaces having fixed degrees.

Let us first consider the case of hypersurfaces of fixed degree in projective space. It can easily be deduced from the affine case by considering the primitive part of the zeta function. First one can recover from Theorem 1 the congruences of Katz [13] or Miller [17] for $n$-dimensional smooth hypersurfaces. But from Ax' Theorem these are trivial when the dimension is larger than the degree of the hypersurface; a general result is that the Newton polygon of the primitive part of the zeta function lies on or above the Hodge polygon (Katz' conjecture [11, 2.9] proved by Mazur [16] and Ogus [5]). As a consequence, the first slope of the zeta function is greater than, or equal to the least integer $\boldsymbol{\mu}$ such that the Hodge number $h^{n-\boldsymbol{\mu},\boldsymbol{\mu}}$ is non zero [1, Section 5]. Even in this case (or more generally in the case of a projective variety having Hodge type $\boldsymbol{\mu}$ given by Ax' or Katz' Theorem), Theorem 1 gives a generically non-trivial congruence for the slope $\boldsymbol{\mu}$ part of the zeta function.

In this paper we treat the case of any (we do not make any assumption of smoothness) affine variety $X$, intersection of $a$ hypersurfaces of respective degrees $d_1, \ldots, d_a$. We show Theorem 3 that gives a generically non trivial congruence for its zeta function. Note that the matrices appearing there are a slight modification of the Hasse-Witt matrices defined in this paper: they are defined over the field $\mathbf{F}_q$, and we get a congruence modulo $p$ for the function $Z(X, q^{-\boldsymbol{\mu}}T)$ in the spirit of [13].

Note that in the case of projective hypersurfaces, the congruence we give boils down to [3, Theorem 1.4] when the degree does not divide the dimension of the ambient projective space, and to [3, Theorem 6.2] else. We finally quote the following sentence from the same authors, whose conclusion unfortunately also holds here: "Presumably our matrix is the matrix of a *higher Hasse-Witt* operation as defined by Katz [12, Section 2.4] but so far we have not been able to prove this."

### 1.4 – *Structure of the paper*

Here is a brief outline of the paper.

Section 2 is devoted to the proof of Theorem 1. It relies on a link between a $p$-adic expression for the $L$-functions and the solutions of certain modular equations. We give a detailed summary at the beginning of the section.

In Section 3, we treat examples to illustrate our methods, and give some applications. First we look at the case $D = \{1, \ldots, p^h - 1\}$ in characteristic $p$, and derive Theorem 2 in 3.1. Then in 3.2 we consider genus 10 hyperelliptic curves having 2-rank 0 in characteristic 2. We compute explicitly some

Hasse-Witt matrices in the higher dimensional case when the characteristic is large enough in 3.3. Applying the last result to zeta functions is sufficient to prove Theorem 3; this is done in 3.4.

**Notations**

| | | |
|---|---|---|
| $p$ | a prime | |
| $D \subset \mathbf{N}^n$ | exponents of the polynomial $f$ | |
| $\tau$ | a generator of $\mathrm{Gal}(\mathbf{Q}_p(\zeta_{q-1}, \zeta_p)/\mathbf{Q}_p(\zeta_p))$ | Sec 2.1 |
| $A, B$ | $p$-adic matrices | Equ (1) |
| $[\mathbf{i}] \subset \{1, \ldots, n\}$ | nonzero components of $\mathbf{i} \in \mathbf{N}^n$ | Def 2.3 |
| $A_I, A_{I+}, B_I, B_{I+}$ | submatrices of $A, B$ | Def 2.3 |
| $\mathfrak{R}_\rho$ | ring of $p$-adic series | Def 2.7 |
| $\mathfrak{I}_\rho$ | ideal in $\mathfrak{R}_\rho$ | Def 2.7 |
| $\delta$ | $p$-density of the set $D$ | Def 2.9 |
| $R := q^\delta$ | generic radius of convergence | Cor 2.12 |
| $\Sigma,\ N$ | minimal support, its cardinality | Def 2.17 |
| $V(\mathbf{e}, \mathbf{e}')$ | set of digits associated to $\mathbf{e}$, $\mathbf{e}'$ in $\Sigma$ | Def 2.17 |
| $\mathrm{HW}(f)$ | Hasse-Witt matrix of the polynomial $f$ | Def 2.22 |
| $I$ | subset of $\{1, \ldots, n\}$ | |
| $f_I, D_I, \ldots$ | objects associated to $I$ | Def 2.26 |
| $\boldsymbol{\mu}$ | Hodge type of the variety $X$ | Equ (9) |
| $\mathrm{HW}_{J,K}(X)$ | Hasse-Witt matrices for the variety $X$ | Def 3.13 |

## 2. The congruence

We prove our main theorem 1 in this section.

Let $p$ be a prime; we set $q = p^m$. We also fix a finite $D \subset \mathbf{N}^n$, and $f(\mathbf{x}) := \sum_{\mathbf{d} \in D} c_{\mathbf{d}} \mathbf{x}^{\mathbf{d}}$, $c_{\mathbf{d}} \in \mathbf{F}_q$, a polynomial in $\mathbf{F}_q[D]$.

We begin this section by recalling Dwork's trace formula in 2.1. It gives a $p$-adic expression for the $L$-function $L(f, T)$ in terms of the Fredholm determinants of some completely continuous operators; our exposition is very close to [1, Section 3]. Then in 2.2 we reduce the study of the coefficients of a Fredholm determinant to the study of simpler terms, that we call minors with fixed support. We decompose these last terms one step further into products of coefficients of a $p$-adic series in 2.3. In equation (5) we associate a solution of the modular equation introduced in [18] to such a product. Then we express its valuation from the $p$-weight of the corresponding solution in equation (6). This link is fundamental in the

proof of Theorem 1; in order to begin the study of these equations, we recall the relevant notations and results from [7] in this section. We also deduce the convergence radius there.

Section 2.4 is completely elementary, but rather technical: we study minimal solutions of modular equations, and show that their base $p$-expansions can be described from finite sets of digits. In 2.5, we observe that the terms with minimal valuation in a minor with fixed support correspond to the minimal solutions of modular equations sharing the same support. Then we use the results of the preceding section to give a congruence for a minor with fixed support. The sets of digits of minimal solutions are used in 2.6 to define the Hasse-Witt matrix, from which we deduce a congruence for an individual Fredholm determinant. Finally, putting these results together, we show Theorem 1 in Section 2.7.

### 2.1 – *Dwork's trace formula*

Let $\pi \in \overline{\mathbf{Q}}_p$ be the root of the series $\sum_{n\geq 0} X^{p^n}/p^n$ such that $v_p(\pi) = 1/(p-1)$ and $\psi(1) \equiv 1+\pi \mod \pi^2$. The field $\mathbf{Q}_p(\pi) = \mathbf{Q}_p(\zeta_p)$ is a totally ramified extension of $\mathbf{Q}_p$ of degree $p-1$. We shall use the valuation $v := v_\pi$, normalized by $v_\pi(\pi) = 1$, instead of the usual $p$-adic valuation $v_p$.

We define the Artin-Hasse exponential series

$$E_p(X) = \exp\left(\sum_{n\geq 0} \frac{X^{p^n}}{p^n}\right) \in \mathbf{Z}_{(p)}[[X]]$$

and the power series $\theta(X) := E_p(\pi X) = \sum_{n\geq 0} \lambda_n X^n$; this is a *splitting function* in Dwork's terminology [10]. The series $E_p$ has its coefficients in $\mathbf{Z}_p$ from Dwork's lemma, and we have the inequality $v(\lambda_n) \geq n$. We stress on a trivial but useful consequence of this result.

Definition 2.1. For $n$ a non negative integer, we denote by $s_p(n)$ the *$p$-weight* of $n$: if $n = n_0 + pn_1 + \cdots + p^t n_t$, $0 \leq n_i \leq p-1$, is the base $p$ expansion of the integer $n$, $s_p(n) = n_0 + \cdots + n_t$.

Proposition 2.2. *In the ring $\mathbf{Z}_p[\zeta_p]$, the coefficients of the splitting function $\theta$ satisfy*

$$\lambda_n = \frac{\pi^n}{n!} \text{ if } \ 0 \leq n \leq p-1; \ v(\lambda_n) > s_p(n) \text{ if } \ n \geq p$$

The elements of finite order in $\mathbf{Q}_p(\zeta_{q-1})^\times$, the multiplicative group of the unramified extension of degree $m$ of $\mathbf{Q}_p$, form a group $\mathcal{T}_m^\times = \boldsymbol{\mu}_{q-1}$ of order $q-1$, and $\mathcal{T}_m := \mathcal{T}_m^\times \cup \{0\}$ is the *Teichmüller* of $\mathbf{Q}_p(\zeta_{q-1})$. Note that it is the image of a section of reduction modulo $p$ from the valuation ring $\mathbf{Z}_p[\zeta_{q-1}]$ of $\mathbf{Q}_p(\zeta_{q-1})$ to its residue field $\mathbf{F}_q$, called the *Teichmüller lift*.

Let $\gamma_{\mathbf{d}} \in \mathcal{T}_m$ denote the Teichmüller lift of $c_{\mathbf{d}}$. Let also $\tau$ denote the generator of the Galois group of the unramified extension $\mathbf{Q}_p(\zeta_{q-1}, \zeta_p)/\mathbf{Q}_p(\zeta_p)$ of degree $m$, defined by $\zeta_{q-1}^\tau = \zeta_{q-1}^p$.

Using Dwork's splitting function, we define two power series having their coefficients in $\mathbf{Q}_p(\zeta_{q-1}, \zeta_p)$

$$F_1(f, \mathbf{x}) := \prod_{\mathbf{d} \in D} \theta(\gamma_{\mathbf{d}} \mathbf{x}^{\mathbf{d}}) = \sum_{\mathbf{i} \in \mathbf{N}^n} \nu_{\mathbf{i}}(f) \mathbf{x}^{\mathbf{i}}, \quad F_m(f, \mathbf{x}) := \prod_{i=0}^{m-1} F_1^{\tau^i}(f, \mathbf{x}^{p^i})$$

Let $w := w_\Delta$ denote the weight on $\mathbf{N}^n$ defined from the polytope $\Delta \subset \mathbf{R}^n$ which is the convex hull of $D \cup \{(0, \ldots, 0)\}$. For any rational $b \in \mathbf{Q}$, we define the space

$$\mathrm{L}(b) := \left\{ \sum_{\mathbf{i} \in \mathbf{N}^n} u_{\mathbf{i}} \mathbf{x}^{\mathbf{i}},\ a_{\mathbf{i}} \in \mathbf{C}_p,\ v_p(u_{\mathbf{i}}) \geq bw(\mathbf{i}) + O(1) \right\}$$

We define an operator $\Psi$ from $\mathrm{L}(b)$ to $\mathrm{L}(pb)$ by $\Psi\left(\sum_{\mathbf{i} \in \mathbf{N}^n} a_{\mathbf{i}} \mathbf{x}^{\mathbf{i}}\right) := \sum_{\mathbf{i} \in \mathbf{N}^n} a_{p\mathbf{i}} \mathbf{x}^{\mathbf{i}}$. We consider the completely continuous operator $\alpha := \alpha(f)$ defined over $\mathrm{L}(p/(p-1))$ as the composition

$$\mathrm{L}\left(\frac{p}{p-1}\right) \overset{\iota}{\hookrightarrow} \mathrm{L}\left(\frac{p}{q(p-1)}\right) \xrightarrow{F_m} \mathrm{L}\left(\frac{p}{q(p-1)}\right) \xrightarrow{\Psi^m} \mathrm{L}\left(\frac{p}{p-1}\right)$$

where $F_m$ denotes multiplication by the series $F_m$.

One can factorize $\alpha$ in terms of the semi-linear ($\mathbf{Q}_p(\zeta_p)$-linear, but not $\mathbf{Q}_p(\zeta_{q-1}, \zeta_p)$-linear) operator $\beta = \beta(f) := \tau^{-1} \circ \Psi \circ F_1(f, \mathbf{x})$, simply as $\alpha = \beta^m$.

We denote respectively by $A$ and $B$ the matrices of the operators $\alpha$ and $\beta$ with respect to the orthonormal basis $\{\pi^{w(\mathbf{i})} \mathbf{x}^{\mathbf{i}},\ \mathbf{i} \in \mathbf{N}^n\}$. We have the equality

$$A = (a_{\mathbf{ij}}) = B^{\tau^{m-1}} B^{\tau^{m-2}} \cdots B$$

Moreover the $(\mathbf{i}, \mathbf{j})$ coefficient of $B$ comes from a coefficient of the series $F_1$ [27, Equation 2.16]

$$b_{\mathbf{ij}} = \pi^{w(\mathbf{j}) - w(\mathbf{i})} \nu_{p\mathbf{i} - \mathbf{j}}(f) = \pi^{w(\mathbf{j}) - w(\mathbf{i})} \sum \prod_D \lambda_{v_{\mathbf{d}}} \gamma_{\mathbf{d}}^{v_{\mathbf{d}}} \tag{1}$$

where the sum is over those $(v_{\mathbf{d}}) \in \mathbf{N}^{|D|}$ such that $\sum v_{\mathbf{d}}\mathbf{d} = p\mathbf{i} - \mathbf{j}$.

The trace and Fredholm determinant of the operator $\alpha$ are well defined and we compute them from the matrix $A$. Dwork's trace formula expresses the exponential sum $S_1(f)$ from the traces of $A$ and close matrices that we introduce now.

Definition 2.3. Let $I$ denote a subset of $\{1, \dots, n\}$.

For any $\mathbf{i}(i_1, \dots, i_n)$ in $\mathbf{N}^n$, we set $[\mathbf{i}] := \{k, i_k \neq 0\} \subset \{1, \dots, n\}$.

We denote by $B_I$ (*resp.* $A_I$) the matrix whose coefficients are the $b_{\mathbf{ij}}$ (*resp.* $a_{\mathbf{ij}}$) with $[\mathbf{i}], [\mathbf{j}] \supset I$.

We denote by $B_{I+}$ (*resp.* $A_{I+}$) the matrix whose coefficients are the $b_{\mathbf{ij}}$ (*resp.* $a_{\mathbf{ij}}$) with $[\mathbf{i}], [\mathbf{j}] = I$.

When $I = \{1, \dots, n\}$, we set $A_+ := A_{I+}$ and $B_+ := B_{I+}$.

Consider the space $\mathrm{L}_I(p/(p-1))$ of those series in $\mathrm{L}(p/(p-1))$ such that $u_{\mathbf{i}} = 0$ when $[\mathbf{i}]$ does not contain $I$. It is stable under $\alpha$ and $\beta$, and the trace and Fredholm determinant of the restriction $\alpha_I := \alpha_{|\,\mathrm{L}_I}$ can be computed from the matrix

$$A_I = B_I^{\tau^{m-1}} B_I^{\tau^{m-2}} \dots B_I$$

Applying Dwork's trace formula, we get the following expressions (see [1, Equation 3.14])

$$S_1(f) = \sum_{I \subset \{1,\dots,n\}} (-1)^{|I|} q^{n-|I|} \operatorname{Tr} A_I, \tag{2}$$

$$L(f;T) = \prod_{I \subset \{1,\dots,n\}} \det(\mathbf{I} - q^{n-|I|} T A_I)^{(-1)^{|I|+1}} \tag{3}$$

2.2 – *Decomposition of the coefficients of a Fredholm determinant*

In this section, we decompose the coefficients of the Fredholm determinant of the matrix $A_+$ defined above. Then we derive a congruence for such determinants.

Set $\det(\mathbf{I} - TA_+) := 1 + \sum_{s \geq 1} C_s T^s$. From [22, Proposition 7], since $A_+ = (a_{\mathbf{ij}})_{\mathbf{i},\mathbf{j} \in (\mathbf{N}_{>0})^n}$, we have

$$C_s = (-1)^s \sum_{F,\kappa} \operatorname{sgn}(\kappa) \prod_{\mathbf{i} \in F} a_{\mathbf{i}\kappa(\mathbf{i})}$$

where the sum is over the subsets $F \subset (\mathbf{N}_{>0})^n$, $|F| = s$, and the permutations $\kappa \in \mathfrak{S}(F)$.

We use the cycle decomposition of $\kappa$ to rewrite the last product; let $\kappa = \widetilde{\eta}_1 \cdots \widetilde{\eta}_t$ where the $\widetilde{\eta}_j$ (say of length $\ell_j$) are cycles whose supports form a partition of $F$.

Such a cycle can be represented in a unique way as $(\eta_j(0), \ldots, \eta_j(\ell_j - 1))$, where $\eta_j : \mathbf{Z}/\ell_j\mathbf{Z} \to F$ is an injective map satisfying $\eta_j(0) = \min \operatorname{Im} \eta_j$ (here the minimum is taken with respect to the lexicographic order in $(\mathbf{N}_{>0})^n$). We get $\operatorname{sgn}(\kappa) \prod_{\mathbf{i} \in F} a_{\mathbf{i}\kappa(\mathbf{i})} = \prod_{j=1}^{t} (-1)^{\ell_j - 1} a(\eta_j) = (-1)^{s-t} \prod_{j=1}^{t} a(\eta_j)$, where we have set $a(\eta_j) := \prod_{k=0}^{\ell_j - 1} a_{\eta_j(k)\eta_j(k+1)}$. From this we deduce an expression for $C_s$

$$C_s = \sum (-1)^t \sum a(\eta_1) \cdots a(\eta_t)$$

where the first sum is over the partitions $\ell_1 + \cdots + \ell_t = s$ of the integer $s$, and the second over the $(\eta_1, \ldots, \eta_t)$ with $\eta_i : \mathbf{Z}/\ell_i\mathbf{Z} \to (\mathbf{N}_{>0})^n$, $\eta_i(0) = \min \operatorname{Im} \eta_i$ and $|\cup_{i=1}^{t} \operatorname{Im} \eta_i| = s$.

Fix a map $\eta$ from $\mathbf{Z}/\ell\mathbf{Z}$ to $(\mathbf{N}_{>0})^n$ as above. We use the factorization $A_+ = B_+^{\tau^{m-1}} B_+^{\tau^{m-2}} \cdots B_+$ to express $a(\eta)$ from the $b_{\mathbf{ij}}$

$$a(\eta) = \sum \prod_{k=0}^{\ell-1} b_{\eta(k)\mathbf{i}_{1k}}^{\tau^{m-1}} b_{\mathbf{i}_{1k}\mathbf{i}_{2k}}^{\tau^{m-2}} \cdots b_{\mathbf{i}_{m-1k}\eta(k+1)}$$

where the sum is over those $(\mathbf{i}_{jk},\ 1 \le j \le m-1,\ 0 \le k \le \ell - 1) \in (\mathbf{N}_{>0}^n)^{(m-1)\ell}$.

To each $(\mathbf{i}_{jk})$, we associate a map $\varphi : \mathbf{Z}/m\ell\mathbf{Z} \to (\mathbf{N}_{>0})^n$, defined by $\varphi(m\ell - mk - j) = \mathbf{i}_{jk}$, $1 \le j \le m-1$, $0 \le k \le \ell - 1$ and $\varphi(m\ell - mk) = \eta(k)$ for $0 \le k \le \ell - 1$.

We get $a(\eta) = \sum \mu(B_+, \varphi)$, where the sum is over the maps from $\mathbf{Z}/m\ell\mathbf{Z}$ to $(\mathbf{N}_{>0})^n$ such that $\varphi(m\ell - mk) = \eta(k)$ for any $0 \le k \le \ell - 1$, and we have set

Definition 2.4. Let $\varphi : \mathbf{Z}/m\ell\mathbf{Z} \to (\mathbf{N}_{>0})^n$. The *minor with support* $\varphi$ of the product matrix $A_+ = B_+^{\tau^{m-1}} B_+^{\tau^{m-2}} \cdots B_+$ is

$$\mu(B_+, \varphi) := \prod_{k=0}^{\ell-1} \prod_{j=0}^{m-1} b_{\varphi(m\ell-mk-j)\varphi(m\ell-mk-j-1)}^{\tau^{m-1-j}} = \prod_{i=0}^{m\ell-1} b_{\varphi(m\ell-i)\varphi(m\ell-i-1)}^{\tau^{m-1-i}}$$

Remark 2.5. Note that we have set $i = j + mk$ to get the second equality above, and that the coefficients of the matrix $B_+$ are fixed by $\tau^m$ since they lie in $\mathbf{Q}_p(\zeta_{q-1}, \zeta_p)$.

We will study thoroughly the minors with fixed support in the following, since they provide the link with solutions of modular equations.

Let us summarize the preceding discussion

PROPOSITION 2.6. *Notations being as above, the degree $s$ coefficient $C_s$ of the Fredholm determinant* $\det(\mathbf{I} - TA_+)$ *can be written*

$$C_s = \sum (-1)^t \sum \mu(B_+, \varphi_1) \cdots \mu(B_+, \varphi_t)$$

*where the first sum is over the partitions $\ell_1 + \cdots + \ell_t = s$ of the integer $s$, and the second over the $(\varphi_1, \ldots, \varphi_t)$ with $\varphi_i : \mathbf{Z}/m\ell_i\mathbf{Z} \to (\mathbf{N}_{>0})^n$ such that*

- *we have $\varphi_i(0) = \min\{\varphi_i(mj),\ 0 \leq j \leq \ell_i - 1\}$, and*
- *$|\cup_{i=1}^t \{\varphi_i(mj),\ 0 \leq j \leq \ell_i - 1\}| = s$*

We now introduce the ring of functions, and its ideal, that we will use in the congruence.

DEFINITION 2.7. Let $\rho > 0$ denote a real number. We define the ring

$$\mathfrak{R}_\rho := \left\{ \sum_{i \geq 0} a_i T^i,\ a_i \in \mathbf{Z}_p[\zeta_p],\ |a_i|_p \leq \rho^{-i} \right\}$$

and its ideal

$$\mathfrak{I}_\rho := \left\{ \sum_{i \geq 0} a_i T^i,\ a_i \in \mathbf{Z}_p[\zeta_p],\ |a_i|_p < \rho^{-i} \right\}$$

The following corollary is a direct consequence of the above proposition

COROLLARY 2.8. *(1) Assume that for any $\ell$ and $\varphi : \mathbf{Z}/m\ell\mathbf{Z} \to (\mathbf{N}_{>0})^n$ as above, we have the inequality $v(\mu(B_+, \varphi)) \geq \delta m\ell(p-1)$; then the Fredholm determinant* $\det(\mathbf{I} - TA_+)$ *lies in the ring $\mathfrak{R}_{q^\delta}$;*

*(2) Assume that $A_1 = B_1^{\tau^{m-1}} B_1^{\tau^{m-2}} \cdots B_1$ and $A_2 = B_2^{\tau^{m-1}} B_2^{\tau^{m-2}} \cdots B_2$ both satisfy the conditions in (1), and that moreover we have for any $\ell$ and $\varphi : \mathbf{Z}/m\ell\mathbf{Z} \to (\mathbf{N}_{>0})^n$ the congruence*

$$\mu(B_1, \varphi) \equiv \mu(B_2, \varphi) \mod \pi^{\delta m\ell(p-1)+1}$$

*in the ring $\mathbf{Z}_p[\zeta_p, \zeta_{q-1}]$; then we have the congruence*

$$\det(\mathbf{I} - TA_1) \equiv \det(\mathbf{I} - TA_2) \mod \mathfrak{I}_{q^\delta}$$

*in the ring $\mathfrak{R}_{q^\delta}$.*

2.3 – *Minors and solutions of modular equations: the convergence radius*

In this section we apply the first part of the above corollary.

We fix a map $\varphi$ from $\mathbf{Z}/m\ell\mathbf{Z}$ to $(\mathbf{N}_{>0})^n$.

We replace the coefficients of the matrix $B_+$ by their expression (1) in the definition of $\mu(B_+,\varphi)$. When we develop the product, we first remark that the powers of $\pi$ cancel. Moreover, the $\gamma_{\mathbf{d}}$ are in the Teichmüller $\mathcal{T}_m$, and we have $\gamma_{\mathbf{d}}^{\tau}=\gamma_{\mathbf{d}}^{p}$ and $\gamma_{\mathbf{d}}^{p^m}=\gamma_{\mathbf{d}}$. We get

$$\mu(B_+,\varphi)=\sum b_V,\ b_V:=\prod_{i=0}^{m\ell-1}\left(\prod_D \lambda_{v_{\mathbf{d}i}}\gamma_{\mathbf{d}}^{p^{m-1-i}v_{\mathbf{d}i}}\right) \tag{4}$$

where $V=(V_i)_{0\le i\le m\ell-1}$, and each $V_i:=(v_{\mathbf{d}i})_D$, $0\le i\le m\ell-1$, runs over the solutions in $\mathbf{N}^{|D|}$ of the equation $\sum_D v_{\mathbf{d}i}\mathbf{d}=p\varphi(m\ell-i)-\varphi(m\ell-i-1)$.

To such a $V$ we associate $U=(u_{\mathbf{d}})_D$, $u_{\mathbf{d}}:=\sum_{i=0}^{m\ell-1}p^{m\ell-1-i}v_{\mathbf{d}i}$. We get a telescoping series

$$\sum_D u_{\mathbf{d}}\mathbf{d}=p^{m\ell}\varphi(m\ell)-\varphi(0)=(p^{m\ell}-1)\varphi(0). \tag{5}$$

Moreover, the following inequalities on the valuation of $b_V$ follow from Proposition 2.2, the definition of $U$ and the inequalities $s_p(a)+s_p(b)\ge s_p(a+b)$ and $s_p(p^b a)=s_p(a)$ valid for all $a,b\in\mathbf{N}$

$$v(b_V)=\sum_{i=0}^{m\ell-1}\sum_D v(\lambda_{v_{\mathbf{d}i}})\ge\sum_{i=0}^{m\ell-1}\sum_D s_p(v_{\mathbf{d}i})\ge\sum_D s_p(u_{\mathbf{d}}) \tag{6}$$

The above equations (5) and (6) are fundamental for us: they motivate the study of the $p$-weights of solutions of a modular equation that we introduce now. Note that most of the material presented here comes from [7].

Definition 2.9. For any $\ell\ge 1$, let $F(\ell)$ denote the set of solutions $U=(u_{\mathbf{d}})_{\mathbf{d}\in D}\in\mathbf{N}^{|D|}$ of

$$\sum_D u_{\mathbf{d}}\mathbf{d}\equiv 0 \mod p^\ell-1,\ \sum_D u_{\mathbf{d}}\mathbf{d}\in(\mathbf{N}_{>0})^n.$$

and $E(\ell)$ the subset of those solutions in $\{0,\dots,p^\ell-1\}^{|D|}$.

The *p-weight* of $U\in F(\ell)$ is the integer $s_p(U):=\sum_{\mathbf{d}\in D}s_p(u_{\mathbf{d}})$; its *length* is $\ell(U):=\ell$.

We set $s(\ell) := \min\{s_p(U),\ U \in E(\ell)\}$; the *p-density* of the set $D$ is $\delta_p(D) := \infty$ if all $E(\ell)$ are empty; else it is the rational number

$$\delta := \delta_p(D) = \frac{1}{p-1} \min_{\ell \geq 1} \left\{ \frac{s(\ell)}{\ell} \right\}$$

The *density* of $U \in E(\ell)$ is $\delta(U) := \frac{s_p(U)}{(p-1)\ell}$. The solution $U$ is *minimal* when $\delta(U) = \delta$.

Note that for any $\ell \geq 1$, and $U \in E(\ell)$, we have $\delta(U) \geq \delta$. The existence of the minimum defining the density is not trivial; this is the content of [7, Proposition 1.5]. This invariant is particularly important here. As mentioned in the introduction, it gives a sharp lower bound for the valuations of the reciprocal roots and poles of the $L$-functions coming from polynomials in $\overline{\mathbf{F}}_q[D]$ [7, Theorem 2.1].

Let us consider the $p$-weights of the solutions in $F(\ell)$

LEMMA 2.10. *For any $(u_{\mathbf{d}}) \in F(\ell)$, we have the inequality $s_p(U) \geq s(\ell)$.*

PROOF. For $u$ a positive integer, let $\bar{u} \in \{1, \cdots, p^\ell - 1\}$ be the integer defined by $u \equiv \bar{u} \bmod p^\ell - 1$. If $u = 0$, we set $\bar{u} := 0$.

For $(u_{\mathbf{d}})$ as above, we have $\sum_D \bar{u}_{\mathbf{d}}\mathbf{d} \equiv 0 \mod p^\ell - 1$, and the sum $\sum_D \bar{u}_{\mathbf{d}}\mathbf{d}$ has all its coordinates positive. Thus $(\bar{u}_{\mathbf{d}}) \in E(\ell)$, and we get $\sum_D s_p(\bar{u}_{\mathbf{d}}) \geq s(\ell)$. The result is a consequence of the inequality $s_p(u) \geq s_p(\bar{u})$ that we now prove.

Write the Euclidean division of $u$ by $p^\ell$, $u = p^\ell u_1 + v_1$. The $p$-weights of these integers satisfy $s_p(u) = s_p(u_1) + s_p(v_1) \geq s_p(u_1 + v_1)$. Replacing $u$ by $u_1 + v_1 = u - (p^\ell - 1)u_1$, and repeating the same process, we finally get $\bar{u}$ and the result. □

We consider the valuations of the minors with fixed support

PROPOSITION 2.11. *Let $\varphi : \mathbf{Z}/m\ell\mathbf{Z} \to (\mathbf{N}_{>0})^n$ be as above. Then we have the inequality*

$$v(\mu(B_+, \varphi)) \geq \delta m\ell(p-1)$$

PROOF. Fix some $V = (v_{\mathbf{d}i})$ as in (4), to which we associate $U$ as above; from (6), the valuation of the term $b_V$ satisfies $v(b_V) \geq s_p(U)$. Since $\varphi(0) \in (\mathbf{N}_{>0})^n$, $U$ is in $F(m\ell)$ from (5). Lemma 2.10 gives $v(b_V) \geq s(m\ell)$ for any $V$. Finally we get the result from the inequality $s(m\ell) \geq \delta m\ell(p-1)$ in Definition 2.9. □

This result, joint to Corollary 2.8 (1), gives a lower bound for the convergence radius of the Fredholm determinant. Following Definition 2.7, we deduce

COROLLARY 2.12. *Let $R =: q^\delta$; the Fredholm determinant* $\det(\mathbf{I} - TA_+)$ *lies in the ring* $\mathfrak{R}_R$.

### 2.4 – *Minimal solutions of modular equations*

This section is devoted to the study of the minimal solutions of modular equations, from which we will deduce congruences for minors with a given support in the next section. We first introduce some material.

DEFINITION 2.13. Let $U \in E(\ell)$ as above.

We define the *shift* map $u \mapsto u'$ from the set $\{0, \dots, p^\ell - 1\}$ to itself; it sends an integer $0 \leq u \leq p^\ell - 2$ to the unique integer $0 \leq u' \leq p^\ell - 2$ such that $u \equiv pu' \mod p^\ell - 1$, and $p^\ell - 1$ to itself. We extend this map coordinatewise to $\{0, \dots, p^\ell - 1\}^{|D|}$, by $U = (u_{\mathbf{d}}) \mapsto U' := (u'_{\mathbf{d}})$.

For any integer $k$, we denote the $k$-th iterate of the maps $u \mapsto u'$ and $U \mapsto U'$ respectively by $u \mapsto u^{(k)}$ and $U \mapsto U^{(k)}$.

The *support* of a solution $U = (u_{\mathbf{d}}) \in E(\ell)$ is the map $\varphi_U : \mathbf{Z}/\ell\mathbf{Z} \to (\mathbf{N}_{>0})^n$ defined by

$$(p^\ell - 1)\varphi_U(i) := \sum_D u^{(i)}_{\mathbf{d}} \mathbf{d}$$

We say that $U$ is *irreducible* when $\varphi_U$ is an injection, else it is *reducible*.

For $0 \leq i \leq \ell - 1$, the *vector of $p^i$-digits* of $U$ is $U_i := (u_{\mathbf{d}i})$, where $u_{\mathbf{d}} := \sum_{i=0}^{\ell-1} p^i u_{\mathbf{d}i}$, $0 \leq u_{\mathbf{d}i} \leq p - 1$ denotes the base $p$ expansion of $(u_{\mathbf{d}})$. .

REMARK 2.14. Note the following facts, that we shall use in the sequel

(1) the map $u \mapsto u'$ is a bijection of order $\ell$, that shifts the $p$-digits, and $U \mapsto U'$ is a bijection from $E(\ell)$ to itself. This map preserves the $p$-weight, and minimality. Moreover we have $(U^{(i)})_0 = U_i$ for any $0 \leq i \leq \ell - 1$.

(2) from the definition of the map $\varphi_U$, we have the equality $\varphi_{U^{(k)}}(i) = \varphi_U(i + k)$ for any $i, k$ and $U$. As a consequence, the map $U \mapsto U'$ also shifts the supports and preserves irreducibility.

(3) as in the proof of [7, Proposition 1.5], the image of $\varphi_U$, $U \in E(\ell)$, is bounded independently of $\ell$; thus irreducible solutions have bounded length. There exists only a finite number of irreducible solutions.

The following result is a rewriting of [7, Lemma 1.4 (ii)]

LEMMA 2.15. *Let $U = (u_{\mathbf{d}}) \in E(\ell)$, and $0 \leq i \leq \ell - 1$. We have the equalities*

*(1)* $\sum_D u_{\mathbf{d}i}\mathbf{d} = p\varphi_U(i+1) - \varphi_U(i)$.

*(2) For any $\mathbf{d} \in D$, let $u_{\mathbf{d}} := p^i q_{\mathbf{d}} + r_{\mathbf{d}}$ denote the Euclidean division of $u_{\mathbf{d}}$ by $p^i$. Then we have the following*

$$\sum_D r_{\mathbf{d}}\mathbf{d} = p^i\varphi_U(i) - \varphi_U(0), \ \sum_D q_{\mathbf{d}}\mathbf{d} = p^{\ell-i}\varphi_U(0) - \varphi_U(i)$$

PROOF. First assume $i = 0$. The definition of the support gives $\sum_D u_{\mathbf{d}}\mathbf{d} = (p^\ell - 1)\varphi_U(0)$ and $\sum_D u'_{\mathbf{d}}\mathbf{d} = (p^\ell - 1)\varphi_U(1)$. We deduce from the base $p$ expansion of $u_{\mathbf{d}}$ that $u_{\mathbf{d}} - pu'_{\mathbf{d}} = (1 - p^\ell)u_{\mathbf{d}0}$, and the equality $\sum_D u_{\mathbf{d}0}\mathbf{d} = p\varphi_U(1) - \varphi_U(0)$. Applying it to $U^{(i)}$, we get assertion (1).

To show assertion (2), remark that we have $r_{\mathbf{d}} = \sum_{k=0}^{i-1} p^k u_{\mathbf{d}k}$ and $q_{\mathbf{d}} = \sum_{k=i}^{\ell-1} p^{k-i} u_{\mathbf{d}k}$; using (1), we get telescoping series and the two equalities. □

We turn to the decomposition of reducible elements in $E(\ell)$. The following result will be used in most of the subsequent constructions

LEMMA 2.16. *(1) Let $S = (s_{\mathbf{d}}) \in E(\ell)$, and $T = (t_{\mathbf{d}}) \in E(\ell')$ denote two solutions, such that $\varphi_S(0) = \varphi_T(0)$. Set $S + p^\ell T := (s_{\mathbf{d}} + p^\ell t_{\mathbf{d}})$. We have*

*(1i) $S + p^\ell T$ is in $E(\ell + \ell')$;*

*(1ii) $\varphi_{S+p^\ell T}(i) = \varphi_S(i)$ for $0 \leq i < \ell$, and $\varphi_{S+p^\ell T}(i) = \varphi_T(i - \ell)$ for $\ell \leq i < \ell + \ell'$;*

*(1iii) the density of $\delta(S+p^\ell T)$ equals the barycenter $\mathrm{Bar}\,((\delta(S), \ell), (\delta(T), \ell'))$. As a consequence, $S + p^\ell T$ is minimal if, and only if both $S$ and $T$ are.*

*(2) Choose some $U \in E(\ell)$ such that $U$ is reducible. Then there exist two solutions $S$ and $T$ with respective lengths $1 \leq \ell_1 \leq \ell - 1$ and $\ell_2 = \ell - \ell_1$ and an integer $t$ such that $U = (S + p^{\ell_1} T)^{(t)}$.*

PROOF. We set $U := S + p^\ell T$. Assertion (1i) comes from the following observation

$$\begin{aligned}\sum_D u_{\mathbf{d}}\mathbf{d} &= p^\ell \sum_D t_{\mathbf{d}}\mathbf{d} + \sum_D s_{\mathbf{d}}\mathbf{d} \\ &= p^\ell(p^{\ell'} - 1)\varphi_T(0) + (p^\ell - 1)\varphi_S(0) \\ &= (p^{\ell+\ell'} - 1)\varphi_S(0)\end{aligned}$$

and we get $\varphi_U(0) = \varphi_S(0) = \varphi_T(0)$.

We turn to (1ii). First choose some $0 \leq i \leq \ell - 1$. The remainder $r_{\mathbf{d}}$ of the Euclidean division of $u_{\mathbf{d}}$ by $p^i$ is the same as that of $s_{\mathbf{d}}$ by $p^i$. From Lemma 2.15 (2), we get $\sum_D r_{\mathbf{d}}\mathbf{d} = p^i\varphi_U(i) - \varphi_U(0) = p^i\varphi_S(i) - \varphi_S(0)$, and $\varphi_U(i) = \varphi_S(i)$ since $\varphi_U(0) = \varphi_S(0)$.

Now assume we have $\ell \leq i \leq \ell + \ell' - 1$. Then the remainder $r_{\mathbf{d}}$ of the Euclidean division of $u_{\mathbf{d}}$ by $p^i$ is $r_{\mathbf{d}} = s_{\mathbf{d}} + p^\ell r'_{\mathbf{d}}$, where $r'_{\mathbf{d}}$ is the remainder of the Euclidean division of $t_{\mathbf{d}}$ by $p^{i-\ell}$. Again from Lemma 2.15 (2), we have

$$p^i\varphi_U(i) - \varphi_U(0) = \sum_D r_{\mathbf{d}}\mathbf{d} = \sum_D s_{\mathbf{d}}\mathbf{d} + p^\ell \sum_D r'_{\mathbf{d}}\mathbf{d} = p^i\varphi_T(i-\ell) - \varphi_T(0)$$

and the result follows since $\varphi_T(0) = \varphi_U(0)$.

To show (1iii), we remark that for any $\mathbf{d}$ we have $s_p(u_{\mathbf{d}}) = s_p(s_{\mathbf{d}}) + s_p(t_{\mathbf{d}})$. We deduce that $(p-1)(\ell+\ell')\delta(U) = s_p(U) = s_p(S) + s_p(T) = (p-1)\ell\delta(S) + (p-1)\ell'\delta(T)$, which is the result. The assertion about minimality is straightforward since we have $\delta(S), \delta(T), \delta(U) \geq \delta$.

We show assertion (2); since $U$ is reducible, there exists some $0 \leq i < j \leq \ell - 1$ such that $\varphi_U(i) = \varphi_U(j)$. If we set $\ell_1 := j - i$, then we have $\varphi_U(i) = \varphi_U(i + \ell_1)$, i.e. $\varphi_{U^{(i)}}(0) = \varphi_{U^{(i)}}(\ell_1)$. For any $\mathbf{d}$, let $u^{(i)}_{\mathbf{d}} := p^{\ell_1}t_{\mathbf{d}} + s_{\mathbf{d}}$ denote the Euclidean division of $u^{(i)}_{\mathbf{d}}$ by $p^{\ell_1}$. From Lemma 2.15 (2), we have $S := (s_{\mathbf{d}}) \in E(\ell_1)$, $T := (t_{\mathbf{d}}) \in E(\ell - \ell_1)$, and $U^{(i)} = S + p^{\ell_1}T$. Setting $t = \ell - i$ and shifting $t$ times we get the result. □

We now define new objects associated to the set $D$ and the prime $p$; they are the building blocks for all minimal solutions, and the Hasse-Witt matrix.

Definition 2.17. The *minimal support* $\Sigma \subset (\mathbf{N}_{>0})^n$ is the union of the images of the supports of minimal irreducible solutions. We set $N := |\Sigma|$.

For any $\mathbf{e}, \mathbf{e}' \in \Sigma$, the *set of digits* associated to $(\mathbf{e}, \mathbf{e}')$ is the following subset of $\{0, \ldots, p-1\}^{|D|}$

$$V(\mathbf{e}, \mathbf{e}') := \{U_0,\ U \text{ minimal irreducible },\ \varphi_U(0) = \mathbf{e},\ \varphi_U(1) = \mathbf{e}'\}$$

Note that from Remark 2.14 (3), there exists only a finite number of minimal irreducible solutions; as a consequence, the sets defined above are finite. Note also that from Lemma 2.15 (2) we have the equality $\sum_D v_{\mathbf{d}}\mathbf{d} = p\mathbf{e}' - \mathbf{e}$ for all $V = (v_{\mathbf{d}}) \in V(\mathbf{e}, \mathbf{e}')$.

First remark the following

LEMMA 2.18. *Let $\mathbf{e}, \mathbf{e}' \in \Sigma$, and assume $V(\mathbf{e}, \mathbf{e}')$ is non empty. Then the quantity $\sum_D v_{\mathbf{d}}$ does not depend on $V = (v_{\mathbf{d}}) \in V(\mathbf{e}, \mathbf{e}')$. We denote it by $w(\mathbf{e}, \mathbf{e}')$.*

PROOF. Choose $V, W \in V(\mathbf{e}, \mathbf{e}')$, and assume we have $\sum_D v_{\mathbf{d}} < \sum_D w_{\mathbf{d}}$. We can find some $\ell \geq 1$ and minimal irreducible $U$ of length $\ell$ with $U_0 = W$. Define $T$ by setting $t_{\mathbf{d}} = u_{\mathbf{d}} - w_{\mathbf{d}} + v_{\mathbf{d}}$ for any $\mathbf{d} \in D$. We have $\sum_D v_{\mathbf{d}}\mathbf{d} = \sum_D w_{\mathbf{d}}\mathbf{d} = p\mathbf{e}' - \mathbf{e}$, and $\sum_D t_{\mathbf{d}}\mathbf{d} = \sum_D u_{\mathbf{d}}\mathbf{d}$; we get $T \in E(\ell)$. Moreover we have $s_p(T) = s_p(U) - \sum_D w_{\mathbf{d}} + \sum_D v_{\mathbf{d}} < s_p(U)$, contradicting the minimality of $U$. This shows the result. □

We now show that the support of any (perhaps reducible) minimal solution is contained in the minimal support, and its vectors of digits lie in one of the sets of digits defined above. We also consider a glueing process for digits.

LEMMA 2.19. *(1) Let $U \in E(\ell)$ denote a minimal solution. Then we have $\operatorname{Im}\varphi_U \subset \Sigma$, and for any $0 \leq i \leq \ell - 1$, we have $U_i \in V(\varphi_U(i), \varphi_U(i+1))$.*

*(2) Choose $\mathbf{e}_0, \ldots, \mathbf{e}_k$ in $\Sigma$, and $V_i \in V(\mathbf{e}_i, \mathbf{e}_{i+1})$ for $0 \leq i \leq k-1$. Then there exists a minimal solution $U$ with $U_i = V_i$ for $0 \leq i \leq k-1$ and $\varphi_U(i) = \mathbf{e}_i$ for $0 \leq i \leq k$.*

PROOF. If $U$ is irreducible, the first assertion is a direct consequence of the definition of the minimal support. Else we use Lemma 2.16 (2) to write $U = (S + p^{\ell_1}T)^{(t)}$. Again from Lemma 2.16, we get $\operatorname{Im}\varphi_U = \operatorname{Im}\varphi_S \cup \operatorname{Im}\varphi_T$. If both $S$ and $T$ are irreducible, we are done; else we apply the same process to $S$ or $T$, until we end with irreducible solutions.

To show $U_i \in V(\varphi_U(i), \varphi_U(i+1))$, it suffices to prove the case $i = 0$; then we apply it to $U^{(i)}$. If $U$ is irreducible, the result comes from the definition.

Else there exist $0 \leq i < j \leq \ell - 1$ such that $\varphi_U(i) = \varphi_U(j)$, and we can write $U = (S + p^{\ell_1}T)^{(t)}$ from Lemma 2.16 (2), where $\ell_1 = j - i$ and $t = \ell - i$. As a consequence, we have $\varphi_{S+p^{\ell_1}T}(t) = \varphi_U(0)$ and $\varphi_{S+p^{\ell_1}T}(t+1) = \varphi_U(1)$. Now we have $\ell_1 = j - i < \ell - i = t$, we get $U_0 = T_{t-\ell_1}$, $\varphi_T(t-\ell_1) = \varphi_{S+p^{\ell_1}T}(t) = \varphi_U(0)$, and $\varphi_T(t-\ell_1+1) = \varphi_{S+p^{\ell_1}T}(t+1) = \varphi_U(1)$ from Lemma 2.16 (1ii).

Set $P := T^{(t-\ell_1)} \in E(\ell - \ell_1)$; it is minimal from Lemma 2.16 (1iii). We have $P_0 = U_0$, and $\varphi_P(0) = \varphi_T(t - \ell_1) = \varphi_U(0)$, $\varphi_P(1) = \varphi_T(t - \ell_1 + 1) = \varphi_U(1)$. If $P$ is irreducible, we get the result. Else we continue the decomposition process until we end with an irreducible solution. This ends the proof of assertion (1).

We use induction on $k$ to show (2). The case $k = 1$ comes from the definition of $V(\mathbf{e}_0, \mathbf{e}_1)$.

Assume we have chosen $\mathbf{e}_0, \ldots, \mathbf{e}_{k+1}$ in $\Sigma$, and $V_i := (v_{\mathbf{d}i}) \in V(\mathbf{e}_i, \mathbf{e}_{i+1})$ for $0 \le i \le k$. We construct a minimal solution $U$ with $U_i = V_i$ for $0 \le i \le k$ and $\varphi_U(i) = \mathbf{e}_i$ for $0 \le i \le k+1$.

From the induction hypothesis, there exists a minimal solution $S = (s_{\mathbf{d}})$ of length $\ell \ge k$ such that $S_i = V_i$ for any $0 \le i \le k-1$, and $\varphi_S(i) = \mathbf{e}_i$ for $0 \le i \le k$; as a consequence, we have the Euclidean division $s_{\mathbf{d}} = p^k q_{\mathbf{d}} + r_{\mathbf{d}}$, with $r_{\mathbf{d}} = \sum_{i=0}^{k-1} p^i v_{\mathbf{d}i}$ and $0 \le q_{\mathbf{d}} \le p^{\ell-k} - 1$ for all $\mathbf{d}$.

On the other hand, there exists a minimal (irreducible) $T = (t_{\mathbf{d}}) \in E(\ell')$ with $T_0 = V_k$, i.e. $t_{\mathbf{d}} = p x_{\mathbf{d}} + v_{\mathbf{d}k}$ for all $\mathbf{d}$, $0 \le x_{\mathbf{d}} \le p^{\ell'-1} - 1$, and we have $\varphi_T(0) = \mathbf{e}_k$, $\varphi_T(1) = \mathbf{e}_{k+1}$.

Remark that $T + p^{\ell'} S^{(k)}$ is in $E(\ell + \ell')$ from Lemma 2.16 (1i), as $\varphi_T(0) = \mathbf{e}_k = \varphi_S(k) = \varphi_{S^{(k)}}(0)$. We define $U \in E(\ell + \ell')$ by $U^{(k)} := T + p^{\ell'} S^{(k)}$; it is minimal from Lemma 2.16 (1iii).

From above we have $s^{(k)}_{\mathbf{d}} = p^{\ell-k} r_{\mathbf{d}} + q_{\mathbf{d}}$ for all $\mathbf{d}$; we deduce that $u^{(k)}_{\mathbf{d}} = t_{\mathbf{d}} + p^{\ell'} s^{(k)}_{\mathbf{d}} = p x_{\mathbf{d}} + v_{\mathbf{d}k} + p^{\ell'}(p^{\ell-k} r_{\mathbf{d}} + q_{\mathbf{d}})$, and shifting $k$ times in the other direction we get

$$u_{\mathbf{d}} = p^{\ell'+k} q_{\mathbf{d}} + p^{k+1} x_{\mathbf{d}} + p^k v_{\mathbf{d}k} + r_{\mathbf{d}} = p^{\ell'+k} q_{\mathbf{d}} + p^{k+1} x_{\mathbf{d}} + \sum_{i=0}^{k} p^i v_{\mathbf{d}i}$$

that gives $U_i = V_i$ for $0 \le i \le k$.

Finally we have $\varphi_U(i) = \varphi_S(i) = \mathbf{e}_i$ for $0 \le i \le k$ and $\varphi_U(k+1) = \varphi_{U^{(k)}}(1) = \varphi_T(1) = \mathbf{e}_{k+1}$ from Lemma 2.16 (1ii). □

We end with a description of minimal solutions having fixed support

PROPOSITION 2.20. *Let $\varphi$ denote a map from $\mathbf{Z}/\ell\mathbf{Z}$ to $\Sigma$. We denote by* $\mathrm{Min}(\varphi)$ *the set of minimal solutions $U \in E(\ell)$ with $\varphi_U = \varphi$.*

*The map*

$$B_\varphi : \mathrm{Min}(\varphi) \to \prod_{i=0}^{\ell-1} V(\varphi(i), \varphi(i+1))$$

*sending $U$ to its vectors of digits $(U_i)_{0 \le i \le \ell-1}$, is a bijection.*

PROOF. First note that $B_\varphi$ is well defined from the first part of Lemma 2.19.

It is sufficient to show that the map from $\prod_{i=0}^{\ell-1} V(\varphi(i), \varphi(i+1))$ to $\mathrm{Min}(\varphi)$ sending $(V_i)$ to $U$ defined by $u_{\mathbf{d}} := \sum_{i=0}^{\ell-1} p^i v_{\mathbf{d}i}$ is well defined: it is the reciprocal bijection of $B_\varphi$.

From the second part of Lemma 2.19, there exists a minimal solution $S$ of length $\ell' \geq \ell$ with $S_i = V_i$ for $0 \leq i \leq \ell - 1$. Moreover, we have $\varphi_S(i) = \varphi(i)$ for any $0 \leq i \leq \ell$, and we get $\varphi_S(0) = \varphi(0) = \varphi_S(\ell)$. If $u_{\mathbf{d}}$ is the remainder of the Euclidean division of $s_{\mathbf{d}}$ by $p^\ell$, then $U = (u_{\mathbf{d}}) \in E(\ell)$ from Lemma 2.15 (2), it is minimal from Lemma 2.16 (1iii), and we have $\varphi_U = \varphi$ from Lemma 2.16 (1ii). □

2.5 – *Minimal minors and minimal solutions*

We now look for a congruence for the Fredholm determinant $\det(\mathbf{I} - TA_+)$ modulo the ideal $\mathfrak{I}_R$. From Corollary 2.8 (2), we are reduced to find a congruence modulo $\pi^{\delta m\ell(p-1)+1}$ for the minor $\mu(B_+, \varphi)$ for any $\varphi : \mathbf{Z}/m\ell\mathbf{Z} \to (\mathbf{N}_{>0})^n$.

We fix a map $\varphi$ as above, and consider a term $b_V$ in the development (4) of $\mu(B_+, \varphi)$ which satisfies the equality $v(b_V) = \delta m\ell(p-1)$.

Recall that we have associated $U := (u_{\mathbf{d}})_D$ to $V$, where $u_{\mathbf{d}} = \sum_{i=0}^{m\ell-1} p^{m\ell-1-i} v_{\mathbf{d}i}$ for any $\mathbf{d}$. From (5), $U$ is in $F(m\ell)$. Since we have $s_p(U) \geq s(m\ell)$ from Lemma 2.10 and $s(m\ell) \geq \delta m\ell(p-1)$, all inequalities in (6) are equalities.

Thus we must have $0 \leq v_{\mathbf{d}i} \leq p-1$ for any $i, \mathbf{d}$ from Proposition 2.2, and $\lambda_{v_{\mathbf{d}i}} = \frac{\pi^{v_{\mathbf{d}i}}}{v_{\mathbf{d}i}!}$. We get

$$(7) \qquad b_V = \frac{\Gamma^U}{\rho(U)} \pi^{\delta m\ell(p-1)} \text{ with } \Gamma^U := \prod_D \gamma_{\mathbf{d}}^{u_{\mathbf{d}}},\ \rho(U) := \prod_D \prod_{i=0}^{m\ell-1} v_{\mathbf{d}i}!$$

Moreover, we have the inequalities $0 \leq u_{\mathbf{d}} \leq p^{m\ell-1}$; thus $U \in E(m\ell)$, and its $p$-weight satisfies $s_p(U) = \sum_{i=0}^{m\ell-1} \sum_D v_{\mathbf{d}i} = \delta m\ell(p-1)$. We deduce that $U$ is a minimal solution.

From the definition of $U$, we have $V_i = U_{m\ell-i-1}$ for all $0 \leq i \leq m\ell - 1$, and from Lemma 2.15 (1), we get $p\varphi_U(m\ell - i) - \varphi_U(m\ell - i - 1) = p\varphi(m\ell - i) - \varphi(m\ell - i - 1)$. Since we have $\varphi_U(0) = \varphi(0)$ from (5), we deduce that the support of $U$ is $\varphi$, that is $U \in \mathrm{Min}(\varphi)$. Moreover, it follows from Lemma 2.19 (1) that $V_i = U_{m\ell-i-1} \in V(\varphi(m\ell - i - 1), \varphi(m\ell - i))$.

Conversely, for any $V = (V_i) \in \prod_{i=0}^{m\ell-1} V(\varphi(m\ell - i - 1), \varphi(m\ell - i))$, we have shown that $U = \sum_{i=0}^{m\ell-1} p^{m\ell-1-i} V_i$ is a minimal solution in the proof of Proposition 2.20. Thus the term $b_V$ satisfies $v(b_V) = \sum_{i=0}^{m\ell-1} \sum_D v_{\mathbf{d}i} = s_p(U) = \delta m\ell(p-1)$.

Summarizing, we obtain the following congruence, where the sum is over $\prod_{i=0}^{m\ell-1} V(\varphi(m\ell-i-1),\varphi(m\ell-i))$

$$\mu(B_+,\varphi) \equiv \sum b_V \mod \pi^{\delta m\ell(p-1)+1}$$

Using the bijection $B_\varphi$ defined in Proposition 2.20, we deduce from (7) the following

LEMMA 2.21. *We have the congruence*

$$\mu(B_+,\varphi) \equiv \sum_{U\in Min(\varphi)} \frac{\Gamma^U}{\rho(U)}\pi^{\delta m\ell(p-1)} \mod \pi^{\delta m\ell(p-1)+1}$$

2.6 – *The Hasse-Witt matrix of a polynomial*

We now define the matrix $\mathrm{HW}(f)$ associated to a polynomial $f\in\mathbf{F}_q[D]$. It is constructed from the base $p$ digits of the minimal solutions associated to $D$ and $p$, and the coefficients $(\gamma_{\mathbf{d}})_{\mathbf{d}\in D}$ of $\widetilde{f}$, the Teichmüller lifting of $f$.

In the following, we fix an ordering of the minimal support $\Sigma = \{\mathbf{e}_1,\dots,\mathbf{e}_N\}$.

DEFINITION 2.22. The *Hasse-Witt matrix of* $f$ is the matrix $\mathrm{HW}(f)\in \mathbf{M}_N(\mathbf{Q}_p(\zeta_p,\zeta_{q-1}))$ whose coefficients are given for any $1\le i,j\le N$ by

$$m_{\mathbf{e}_i\mathbf{e}_j}(f) := \pi^{w(\mathbf{e}_i,\mathbf{e}_j)} \sum_{V\in V(\mathbf{e}_i,\mathbf{e}_j)} \frac{\Gamma^V}{V!}$$

where we have set $\Gamma^V := \prod_D \gamma_{\mathbf{d}}^{v_{\mathbf{d}}}$ and $V! := \prod_D v_{\mathbf{d}}!$ for $V=(v_{\mathbf{d}})$.

REMARK 2.23. Note that from Lemma 2.18 the sum appearing in the definition of the coefficient $m_{\mathbf{e}_i\mathbf{e}_j}(f)$ is a homogeneous polynomial of degree $w(\mathbf{e}_i,\mathbf{e}_j)$ in $\mathbf{Z}_{(p)}[(\gamma_{\mathbf{d}})_{\mathbf{d}\in D}]$. Moreover, its reduction modulo $p$ in $\mathbf{F}_p[(c_{\mathbf{d}})_{\mathbf{d}\in D}]$ is the solution given by [2, Equation (2.4)] of the mod $p$ $D$-hypergeometric system with parameter $p\mathbf{e}_j-\mathbf{e}_i$ defined in [2, Equations (2.2) (2.3)].

We determine the minors with fixed support of the transpose of the product $\mathrm{HW}(f)\cdots\mathrm{HW}(f)^{\tau^{m-1}}$. Recall from (7) that for any $U=(u_{\mathbf{d}})\in E(\ell)$, we have set $\Gamma^U := \prod_D \gamma_{\mathbf{d}}^{u_{\mathbf{d}}}$, and $\rho(U) := \prod_{i=0}^{l-1} U_i!$.

LEMMA 2.24. *For any map* $\varphi:\mathbf{Z}/m\ell\mathbf{Z}\to\Sigma$, *we have*

$$\mu({}^t\mathrm{HW}(f),\varphi) = \pi^{\delta m\ell(p-1)} \sum_{U\in Min(\varphi)} \frac{\Gamma^U}{\rho(U)}$$

PROOF. From Definition 2.4, we have

$$\mu({}^t\mathrm{HW}(f),\varphi) = \prod_{j=0}^{m\ell-1} m_{\varphi(m\ell-j-1)\varphi(m\ell-j)}(f)^{\tau^{m-1-j}} = \prod_{i=0}^{m\ell-1} m_{\varphi(i)\varphi(i+1)}(f)^{\tau^i}$$

where the last equality comes the change of index $i = m\ell - 1 - j$. Develop the last product

$$\prod_{i=0}^{m\ell-1} m_{\varphi(i)\varphi(i+1)}(f)^{\tau^i} = \sum \pi^{\sum w(\varphi(i),\varphi(i+1))} \prod_{i=0}^{m\ell-1} \left(\frac{\Gamma^{V_i}}{V_i!}\right)^{\tau^i}$$

where the sum is over the elements $(V_i)_{0\le i\le m\ell-1}$ in $\prod_{i=0}^{m\ell-1} V(\varphi(i),\varphi(i+1))$. Since the $\gamma_{\mathbf{d}}$ are Teichmüller liftings, we have $(\Gamma^{V_i})^{\tau^i} = \Gamma^{p^i V_i}$, and the denominators are invariant under the action of $\tau$.

We use Proposition 2.20. For any $V$ as above, set $U = (u_{\mathbf{d}}) := B_\varphi^{-1}((V_i)_{0\le i\le m\ell-1})$; we have $u_{\mathbf{d}} = \sum_{i=0}^{m\ell-1} p^i v_{\mathbf{d}i}$, $U$ describes $\mathrm{Min}(\varphi)$ when $V$ varies, and $\Gamma^U = \prod_{i=0}^{m\ell-1}(\Gamma^{V_i})^{\tau^i}$, $\rho(U) = \prod_{i=0}^{m\ell-1} V_i!$. We also have $\sum_{i=0}^{m\ell-1} w(\varphi(i),\varphi(i+1)) = \sum_{i=0}^{m\ell-1}\sum_D v_{\mathbf{d}i} = s_p(U) = \delta m\ell(p-1)$. We have reached the right hand side of the equality. □

When we have $\mathrm{Im}\,\varphi \subset \Sigma$ the minimal support, we get $v(\mu(B_+,\varphi) - \mu({}^t\mathrm{HW}(f),\varphi)) > \delta m\ell(p-1)$ from Lemma 2.21 and Lemma 2.24. On the other hand, if $\mathrm{Im}\,\varphi$ is not contained in the minimal support $\Sigma$, we must have $v(\mu(B_+,\varphi)) > \delta m\ell(p-1)$ from Lemma 2.19 (1).

Now we can apply Corollary 2.8 (2) to $A_+$ and the transpose of $\mathrm{HW}(f)\cdots\mathrm{HW}(f)^{\tau^{m-1}}$. Since a matrix and its transpose have the same characteristic polynomial, we get

PROPOSITION 2.25. *In the ring $\mathfrak{R}_R$, we have the congruence*

$$\det(\mathbf{I} - TA_+) \equiv \det\left(\mathbf{I}_N - \mathrm{HW}(f)\cdots\mathrm{HW}(f)^{\tau^{m-1}}T\right) \mod \mathfrak{I}_R$$

*where* $\mathrm{HW}(f)$ *is the Hasse-Witt matrix from Definition* 2.22.

### 2.7 – *The main theorem*

We are almost ready to show our main result; it just remains to take into account the factors in (3).

DEFINITION 2.26. For any subset $I \subset \{1, \dots, n\}$, denote by $f_I$ the polynomial obtained from $f$ by setting $x_j = 0$ for any $j \notin I$, $D_I = D \cap \{x_j = 0,\ j \notin I\}$ the set of its exponents, $\delta_I$ its density, $R_I := q^{\delta_I}$ the generic radius of convergence, $\Sigma_I$ the minimal support of $D_I$ having cardinality $N_I$, and $\mathrm{HW}(f_I)$ the Hasse-Witt matrix attached to $f_I$.

We need a last result, which gives an inequality between the densities of the set $D \subset \mathbf{N}^n$ and of a subset $D_I$. It explains the range of the product in Theorem 1; see also [2, Lemma 7.6].

LEMMA 2.27. *Let $I \subset \{1, \dots, n\}$. We have the inequality $\delta_I + n - |I| \geq \delta$.*

PROOF. If $D_I$ is contained in some coordinate hyperplane of $\{x_j = 0,\ j \notin I\}$, then we have $\delta_I = \infty$, and there is nothing to prove. Else let $U_I = (u_{\mathbf{d}})_{D_I}$ denote a minimal solution of length $\ell$ associated to $D_I$ and $p$; it has density $\delta_I$. Since $D$ is not contained in any of the coordinate hyperplanes of $\mathbf{R}^n$, we can choose some $\mathbf{d}_1 \in D \setminus D_I$: then $[\mathbf{d}_1]$ is not contained in $I$; if $I \cup [\mathbf{d}_1] = \{1, \dots, n\}$, we stop; else we choose some $\mathbf{d}_2$ such that $[\mathbf{d}_2] \not\subset I \cup [\mathbf{d}_1]$, until we get $\mathbf{d}_1, \mathbf{d}_2, \dots, \mathbf{d}_k$ with $I \cup [\mathbf{d}_1] \cup \dots \cup [\mathbf{d}_k] = \{1, \dots, n\}$. We must have $k \leq n - |I|$.

Now consider $U := (U_I, u_{\mathbf{d}_1} = p^\ell - 1, \dots, u_{\mathbf{d}_k} = p^\ell - 1)$; this is an element in $E(\ell)$. Since we have $s_p(p^\ell - 1) = \ell(p-1)$, its density satisfies $\delta \leq \delta(U) = \delta(U_I) + k \leq \delta_I + n - |I|$. □

We can now state the main result.

THEOREM 1. *Let $f \in \mathbf{F}_q[D]$ denote a polynomial; we have the following congruence in $\mathfrak{R}_R$*

$$L(f;T)^{(-1)^{n+1}} \equiv \prod \det\left(\mathbf{I}_{N_I} - q^{n-|I|}\,\mathrm{HW}(f_I)\cdots\mathrm{HW}(f_I)^{\tau^{m-1}}T\right)^{(-1)^{n-|I|}} \mod \mathfrak{I}_R$$

*where the product is over those subsets $I \subset \{1, \dots, n\}$ such that $\delta_I + n - |I| = \delta$.*

We emphasize a particular case, when we have $\delta_I + n - |I| > \delta$ for any subset $I \subsetneq \{1, \dots, n\}$. This is often verified, for instance when $n = 1$, or when the set $D$ contains an element with all its coordinates positive, since in these last cases we have $\delta \leq 1$.

Corollary 1. *Assume that we have $\delta_I + n - |I| > \delta$ for any subset $I \subsetneq \{1, \dots, n\}$; then we have the following congruence in the ring $\mathfrak{R}_R$*

$$L(f;T)^{(-1)^{n+1}} \equiv \det\left(\mathbf{I}_N - \mathrm{HW}(f)\cdots\mathrm{HW}(f)^{\tau^{m-1}}T\right) \mod \mathfrak{I}_R$$

Proof of Theorem 1. Recall from (3) that the function $L(f;T)$ is an alternating product of the Fredholm determinants $\det(\mathbf{I}-q^{n-|I|}A_IT)$, where $I$ runs over the subsets of $\{1,\cdots,n\}$.

We first show that all factors lie in $\mathfrak{R}_R$. We fix such an $I$, and a map $\varphi : \mathbf{Z}/m\ell\mathbf{Z} \to \mathbf{N}^n$ such that for all $i$ we have $[\varphi(i)] \supset I$. We factor $q^{n-|I|}A_I = p^{n-|I|}B_I^{\tau^{m-1}}\cdots p^{n-|I|}B_I$ and consider the minor $\mu(p^{n-|I|}B_I,\varphi) = q^{(n-|I|)\ell}\mu(B_I,\varphi)$ associated to $\varphi$. Since we have $\nu_{p\mathbf{i}-\mathbf{j}}(f) = 0$ (and $b_{\mathbf{ij}} = 0$) when $[\mathbf{j}] \not\subset [\mathbf{i}]$, the minor $\mu(B_I,\varphi)$ is non zero only if

$$[\varphi(0)] = [\varphi(m\ell)] \supset [\varphi(m\ell-1)] \supset \ldots \supset [\varphi(0)]$$

i.e. only if all $\varphi(i)$ are equal to some $J$. As a consequence, we have $\mu(B_I,\varphi) = \mu(B_{J+},\varphi)$. Applying Proposition 2.11 to the matrix $B_{J+}$, we get $v(\mu(B_{J+},\varphi)) \geq \delta_J m\ell(p-1)$, and $v(\mu(p^{n-|I|}B_{J+},\varphi)) \geq (\delta_J+n-|I|)m\ell(p-1)$. Since $J \supset I$, we have $\delta_J + n - |I| \geq \delta_J + n - |J|$ that is greater than or equal to $\delta$ from Lemma 2.27. We conclude from Corollary 2.8 (1) that $\det(\mathbf{I} - q^{n-|I|}A_IT)$ is in $\mathfrak{R}_R$.

We turn to the congruence. Consider a minor as above with $J \supsetneq I$; since we have $\delta_J + n - |I| > \delta_J + n - |J| \geq \delta$ in this case, we get $v(\mu(p^{n-|I|}B_I,\varphi)) > \delta m\ell(p-1)$. Then any term containing $\mu(p^{n-|I|}B_I,\varphi))$ in the decomposition from Proposition 2.6 of a coefficient of the Fredholm determinant $\det(\mathbf{I} - q^{n-|I|}A_IT)$ vanishes modulo $\mathfrak{I}_R$. The only remaining terms are those with $J = I$; we obtain

$$\det(\mathbf{I} - q^{n-|I|}A_IT) \equiv \det(\mathbf{I} - q^{n-|I|}A_{I+}T) \mod \mathfrak{I}_R$$

From Corollary 2.12 applied to $A_{I+}$, the right hand side lies in the ring $\mathfrak{R}_{q^{n-|I|}R_I}$, and it is 1 modulo $\mathfrak{I}_R$ when $\delta_I + n - |I| > \delta$. Thus the only Fredholm determinants that contribute to the congruence modulo $\mathfrak{I}_R$ are those coming from subsets $I \subset \{1,\dots,n\}$ with $\delta_I + n - |I| = \delta$. For those, Proposition 2.25 applied to $A_{I+}$ gives the congruence

$$\det(\mathbf{I}-q^{n-|I|}A_IT) \equiv \det\left(\mathbf{I}_{N_I} - q^{n-|I|}\,\mathrm{HW}(f_I)\cdots\mathrm{HW}(f_I)^{\tau^{m-1}}T\right) \mod \mathfrak{I}_R$$

This ends the proof of the theorem. □

Let us give a first application, about exponential sums. It follows from [7, Theorem 2.1] that for any $r \geq 1$ and any $f \in \mathbf{F}_q[D]$ the sum $S_r(f)$ is divisible by $q^{r\delta}$. Now we can use the congruence to give the principal parts of these sums, i.e. Hasse invariants, in the spirit of [2]

COROLLARY 2. *In the ring* $\mathbf{Z}_p[\zeta_p]$ *we have*

$$\left| S_r(f) - \sum (-1)^{|I|} q^{r(n-|I|)} \operatorname{Tr}\left( \mathrm{HW}(f_I) \cdots \mathrm{HW}(f_I)^{\tau^{m-1}} \right)^r \right|_p < q^{-r\delta}$$

*where the sum is over those* $I \subset \{1, \ldots, n\}$ *such that* $\delta_I + n - |I| = \delta$.

## 3. Examples and applications

We now treat some examples, in order to illustrate the definitions of Section 2.5, and compute explicitly the Hasse-Witt matrices of certain polynomials. We also present some applications of Theorem 1: we show that certain Artin-Schreier curves cannot be supersingular in Theorem 2, and we prove a congruence for zeta functions of varieties in Theorem 3.

### 3.1 – *Some polynomials in one variable, and Artin-Schreier curves*

We fix a prime $p$, $h > 1$ an integer, and set $D := \{0, \ldots, p^h - 1\} \subset \mathbf{N}$; let $d_0 := p^h - 1$.

From [7, Lemma 1.19 (i)], the $p$-density of $D$ is $\delta = \frac{1}{h(p-1)}$. We determine the minimal solutions. Let $U \in E(\ell)$ be such a solution; we have equality in [7, Lemma 1.8(iv)], and this implies $u_d = 0$ for all $d \neq d_0$ since then $s_p(d) < h(p-1)$. We are reduced to find some $k, \ell \geq 1$ and $1 \leq u_{d_0} \leq p^\ell - 1$ such that

$$(p^h - 1)u_{d_0} = k(p^\ell - 1),\ s_p(u_{d_0}) = \frac{\ell}{h},\ 1 \leq u_{d_0} \leq p^\ell - 1$$

We must have $\ell = th$ for some integer $t \geq 1$, and $u_{d_0} = k(1 + p^h + \cdots + p^{(t-1)h})$ for some $1 \leq k \leq p^h - 1$, $s_p(u_{d_0}) = t$. Then we have $s_p(u_{d_0}) = ts_p(k)$, and $s_p(k) = 1$, that is $k = p^i$ for some $0 \leq i \leq h-1$. We have found all minimal solutions of length $\ell$: they are defined, for $0 \leq i \leq h-1$, by $u_d = 0$ for $d \neq d_0$, $u_{d_0} = p^i(1 + p^h + \cdots + p^{(t-1)h})$.

The support of the solution described above is the map $\varphi_i$ sending any $k \in \mathbf{Z}/\ell\mathbf{Z}$ to $p^{k'}$, where $k'$ is the remainder of the Euclidean division of $i - k$ by $h$. Thus the minimal irreducible solutions are the minimal solutions of length $h$; they are the $S^{(h-i)}$, $0 \leq i \leq h-1$, where $S \in E(h)$ is

defined by $s_d = 0$ for $d \neq d_0$, $s_{d_0} = 1$. Moreover the minimal support is $\Sigma = \{p^i,\ 0 \leq i \leq h-1\}$. Considering the base $p$ digits of the minimal irreducible solution $S$, we get $V(p^{i+1}, p^i) = \{(0, \dots, 0)\}$ for $0 \leq i \leq h-2$, $V(1, p^{h-1}) = \{(0, \dots, 0, 1)\}$, and $V(p^i, p^j) = \emptyset$ else.

The Hasse-Witt matrix for the polynomial $f(x) = \sum_{d=0}^{p^h-1} c_d x^d \in \mathbf{F}_q[D]$.depends only on its leading coefficient: it is the $h \times h$ matrix

$$\mathrm{HW}(f) = \begin{pmatrix} 0 & \dots & \dots & 0 & \pi\gamma_{p^h-1} \\ 1 & \ddots & & & 0 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \dots & 0 & 1 & 0 \end{pmatrix}$$

Set $d = \gcd(m, h)$. In the ring $\mathfrak{R}_R$, we have the following congruence

$$L(f;T) \equiv \mathrm{N}_{\mathbf{Q}_p(\zeta_{p^d-1},\zeta_p)/\mathbf{Q}_p(\zeta_p)} \left(1 - \mathrm{N}_{\mathbf{Q}_p(\zeta_{p^m-1})/\mathbf{Q}_p(\zeta_{p^d-1})}(\gamma_{p^h-1})\pi^{\frac{m}{d}} T^{\frac{h}{d}}\right) \mod \mathfrak{I}_R$$

We get that the degree $h$ coefficient of $L(f;T)$ is $\mathrm{N}_{\mathbf{Q}_p(\zeta_{p^m-1})/\mathbf{Q}_p}(\gamma_{p^h-1})\pi^m$ modulo $\pi^{m+1}$. The first vertex of the Newton polygon $\mathrm{NP}_q(f)$ is $(h, \frac{1}{p-1})$ for any $f$ since we have $\gamma_{p^h-1} \neq 0$.

From this we deduce

THEOREM 2. *In characteristic $p$, there does not exist any supersingular $p$-cyclic covering of the projective line having genus $(p-1)(p^h-2)/2$ when $h(p-1) > 2$.*

PROOF. A supersingular $p$-cyclic covering of the projective line must have $p$-rank 0: the Newton polygon cannot have an horizontal part. From Deuring Shafarevic formula [9, Corollary 1.8], such a covering is ramified over exactly one point of the projective line. Moving it to infinity, we deduce that such a curve, defined over $k = \mathbf{F}_q$, has an equation of the form $y^p - y = f(x) = \sum_{i=1}^{d_0} c_i x^i,\ c_i \in k,\ c_{d_0} \neq 0$ since the genus of the above curve is $\frac{1}{2}(p-1)(d_0-1)$.

Now the Newton polygon of the numerator of the zeta function of this curve is $(p-1)\,\mathrm{NP}_q(f)$ (see for instance [8, Equation (93)]), and its first vertex is $((p-1)h, 1)$ for any $f$. This curve cannot be supersingular when $h(p-1) > 2$. □

3.2 – *Some hyperelliptic curves in characteristic two*

In this subsection, we consider hyperelliptic curves in characteristic two, having genus 10 and 2-rank zero. This case illustrates some interesting phenomena: the matrix $\mathrm{HW}(f)$ is singular for any $f \in \overline{\mathbf{F}}_q[D]$, and the invariants (density, minimal support...) really depend on the set $D$, and not on its convex hull.

Recall from Deuring-Shafarevich formula (see [23, Proposition 4.1]) that an hyperelliptic curve $C$ defined over $\mathbf{F}_{2^m}$, having genus 10 and 2-rank zero admits an equation of the form

$$y^2 + y = \sum_{i=0}^{10} c_{2i+1} x^{2i+1}$$

where the coefficients $c_i$ are in $\mathbf{F}_{2^m}$. Let $f(x)$ denote the polynomial in the right-hand side.

We first consider the set $D := \{1, 3, \ldots, 21\}$. Remark that 15 is the only element in $D$ having 2-weight 4. Reasoning as in the preceding section, we see that $D$ has 2-density $\frac{1}{4}$, and that the Newton polygon of $L(f, T)$ has first vertex $(4, 1)$ exactly when $c_{15} \neq 0$.

We assume $c_{15} = 0$; let $D' := D \setminus \{15\}$. The 2-density of the set $D'$ is $\frac{1}{3}$; since all elements in $D'$ have 2-weight less than or equal to 3, the minimal solutions for $D'$ are combinations of elements of 2-weight 3, which are elements in $\{7, 11, 13, 19, 21\}$. Using [7, Lemma 1.18], a computer search gives six minimal irreducible solutions (up to shift), namely

| Solution | weight | length | support |
|---|---|---|---|
| $1 \cdot 7$ | 1 | 3 | $(1, 4, 2)$ |
| $1 \cdot 21$ | 1 | 3 | $(3, 12, 6)$ |
| $3 \cdot 21$ | 2 | 6 | $(1, 11, 16, 8, 4, 2)$ |
| $4 \cdot 13 + 1 \cdot 11$ | 2 | 6 | $(1, 6, 3, 8, 4, 2)$ |
| $4 \cdot 11 + 1 \cdot 19$ | 2 | 6 | $(1, 10, 5, 8, 4, 2)$ |
| $32 \cdot 13 + 5 \cdot 19$ | 3 | 9 | $(1, 10, 5, 12, 6, 3, 8, 4, 2)$ |

The 2-minimal support of $D'$ is $\Sigma = \{1, 2, 4, 8, 16, 11, 3, 6, 5, 10, 12\}$, and with respect to this ordering, the Hasse-Witt matrix of $f$ is

$$\mathrm{HW}(f) = \begin{pmatrix} 0 & 0 & \pi\gamma_7 & 0 & 0 & \pi\gamma_{21} & 0 & \pi\gamma_{11} & 0 & \pi\gamma_{19} & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \pi\gamma_{13} & 0 & 0 & 0 & 0 & 0 & 0 & \pi\gamma_{21} \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \pi\gamma_{11} & 0 & 0 & 0 & 0 & 0 & 0 & \pi\gamma_{19} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

The polynomial $\det\left(\mathbf{I} - \mathrm{HW}(f)\cdots\mathrm{HW}(f)^{\tau^{m-1}}T\right)$ cannot have degree 11, as this matrix is never invertible. In the spirit of [13, Section 1], it is not difficult to compute the iterates of the semi-linear morphism of $\mathbf{F}_{2^m}^{11}$ having matrix $\mathrm{HW}(f)$ in order to determine its stable rank. Then one gets the following (as $p = 2$, the $L$-function $L(f, T)$ is exactly the numerator of the zeta function of $C$)

Proposition 3.1. *Consider the Newton polygon of the numerator of the zeta function of the genus* 10 *curve having equation* $y^2 + y = f(x)$*; some possible first vertices for it are*

- $(4, 1)$ *iff* $c_{15} \neq 0$*;*
- $(9, 3)$ *iff* $c_{15} = 0$*, and* $c_{11}^4 c_{19} + c_{13}^4 c_{19}^5 \neq 1$*;*
- $(6, 2)$ *iff* $c_{15} = 0$*,* $c_{11}^4 c_{19} + c_{13}^4 c_{19}^5 = 1$*, and* $(c_{19}^{10} + c_{11}^2)c_{13} + c_7^2 \neq 0$*;*
- $(3, 1)$ *iff* $c_{15} = 0$*,* $c_{11}^4 c_{19} + c_{13}^4 c_{19}^5 = 1$*,* $(c_{19}^{10} + c_{11}^2)c_{13} + c_7^2 = 0$ *and* $c_{13}(c_{19}^{80} + c_{11}^{16}) \neq 1$.

*The Newton polygon has first slope* $> \frac{1}{3}$ *if, and only if we have*

$$c_{15} = c_{11}^4 c_{19} + c_{13}^4 c_{19}^5 + 1 = (c_{19}^{10} + c_{11}^2)c_{13} + c_7^2 = c_{13}(c_{19}^{80} + c_{11}^{16}) + 1 = 0$$

Remark 3.2. This result stands in striking contrast with the ones in [23] for $g \leq 8$: in this case, the Newton polygon jumps along coordinates hyperplanes in the affine space parametrised by the coefficients of $f$. Applying the congruence repeatedly to smaller and smaller sets of exponents (as we did above from $D$ to $D'$), we end with all possible Newton polygons, and supersingular curves. Here it is clear that we cannot apply our results to the family of curves having first slope of their Newton polygon larger than $\frac{1}{3}$.

REMARK 3.3. Of course we can use the same method to study higher genera, and produce curves with "high" Newton polygon. For instance in genus 11, one can show that the Newton polygon associated to the curve $y^2 + y = x^{23} + x^{21} + x^{17} + x^7 + x^5$ over $\mathbf{F}_2$ has slopes 5/11, 6/11. But from a simple dimension argument [20, Expectation 8.5.3], one expects that the Newton stratum of abelian varieties having these slopes should not meet the Torelli locus. This gives an example of unlikely intersection.

### 3.3 – *Hasse-Witt matrix of a polynomial, when the characteristic is large enough*

We compute the Hasse-Witt matrix of a multivariate polynomial, when the characteristic is large enough, under a "saturation" hypothesis on the set $D$ of its exponents. This result will be used in the next subsection to give a congruence for zeta functions.

First recall some standard notations (see for instance [1, Section 2]). We fix $D \subset \mathbf{N}^n$, not contained in any of the hyperplanes $\{x_i = 0\}$. Let $\Delta$ be the convex hull of $D$ and the origin in $\mathbf{R}^n$. Let $C(\Delta)$ denote the cone generated by $\Delta$, $M_\Delta$ the monoid $C(\Delta) \cap \mathbf{N}^n$, and $w_\Delta : M_\Delta \to \mathbf{Q}_+$ the weight. We define $d_\Delta$ to be the denominator of $\Delta$, the least positive integer such that $d_\Delta w_\Delta$ has integer values. Let $\omega(\Delta)$ denote the least weight of an element in $M_\Delta \cap (\mathbf{N}_{>0})^n$, and

$$\Sigma(\Delta) := \{\mathbf{e}_1, \ldots, \mathbf{e}_{N_\Delta}\}$$

denote the set of elements in $M_\Delta \cap (\mathbf{N}_{>0})^n$ with weight $\omega(\Delta)$, $N_\Delta := \#\Sigma(\Delta)$.

Fix $f \in \mathbf{F}_q[D]$; it is known [1, Theorem 1.2] that $v_{q^r}(S_r(f)) \geq \omega(\Delta)$ for any polynomial $f$ having $D$ as its set of exponents. Moreover, the density satisfies the lower bound $\delta \geq \omega(\Delta)$ for any $p$ from [7, Proposition 1.11]. Here we show that under some "saturation" hypothesis, this last bound is almost optimal when the characteristic is large enough. We also deduce an explicit expression for the matrix $\mathrm{HW}(f)$.

In the following, we assume that the set $D$ satisfies the following hypothesis

HYPOTHESIS 3.4. *For any integer $r \geq 1$, the set*

$$rD := \{\mathbf{d}_1 + \cdots + \mathbf{d}_r,\ \mathbf{d}_1, \ldots, \mathbf{d}_r \in D \cup \{0\}\}$$

*is equal to the set of points in $M_\Delta$ with weight less than or equal to $r$.*

PROPOSITION 3.5. *Assume that $D$ satisfies Hypothesis* 3.4*, and that $p > 1 + (d_\Delta - 1)(N_\Delta + 1)$. Then the p-density of $D$ is $\delta = \frac{1}{p-1}\lceil (p-1)\omega(\Delta)\rceil$, and its minimal support satisfies $\Sigma = \Sigma(\Delta)$.*

PROOF. We assert that any $\mathbf{e} \in \Sigma(\Delta)$ is the support of a solution in $E(1)$ with weight $\lceil (p-1)\omega(\Delta)\rceil$.

Since $\mathbf{e}$ has weight $\omega(\Delta)$, we deduce from Hypothesis 3.4 that we have $(p-1)\mathbf{e} = \sum_D u_\mathbf{d}\mathbf{d}$ with $\sum_D u_\mathbf{d} \leq \lceil (p-1)\omega(\Delta)\rceil$. For any $\mathbf{d}$ let $\bar{u}_\mathbf{d}$ denote the remainder of the Euclidean division of $u_\mathbf{d}$ by $p-1$, or $p-1$ if $u_\mathbf{d}$ is a positive multiple of $p-1$. We obtain $\sum_D \bar{u}_\mathbf{d}\mathbf{d} = (p-1)\mathbf{e}'$ for some $\mathbf{e}'$ in $M_\Delta \cap (\mathbf{N}_{>0})^n$, and the inequalities:

$$(p-1)\omega(\Delta) \leq w_\Delta(\sum_D \bar{u}_\mathbf{d}\mathbf{d}) \leq \sum_D \bar{u}_\mathbf{d} \leq \sum_D u_\mathbf{d} \leq \lceil (p-1)\omega(\Delta)\rceil.$$

Since $\sum_D \bar{u}_\mathbf{d}$ is an integer, we must have $\bar{u}_\mathbf{d} = u_\mathbf{d}$ for all $\mathbf{d}$ and $\sum_D u_\mathbf{d} = \lceil (p-1)\omega(\Delta)\rceil$; thus we have $0 \leq u_\mathbf{d} \leq p-1$ for all $\mathbf{d}$, and this is the assertion at the beginning of the proof.

Note that as a consequence, we get the upper bound $\delta \leq \frac{1}{p-1}\lceil (p-1)\omega(\Delta)\rceil$.

We show the inclusion $\Sigma \subset \Sigma(\Delta)$; recall that $\Sigma$ is the union of the supports of the minimal irreducible solutions associated to $D$ and $p$. Let $U = (u_\mathbf{d})_{\mathbf{d}\in D} \in E(\ell)$ be such a solution, and $\mathbf{e}_0, \ldots, \mathbf{e}_{\ell-1}$ denote its support. First note that the $\mathbf{e}_i$ are pairwise distinct since we assumed $U$ irreducible; moreover they lie in $M_\Delta \cap (\mathbf{N}_{>0})^n$. Assume that exactly $k$ among the $\mathbf{e}_i$ have weight $\omega(\Delta)$, with $k < \ell$ (note that $k \leq N_\Delta$). The remaining $\ell - k$ ones have weight at least $\omega(\Delta) + \frac{1}{d_\Delta}$. From the definition of the support, we have $\sum_D u^{(t)}_\mathbf{d}\mathbf{d} = (p^\ell - 1)\mathbf{e}_t$ for any $0 \leq t \leq \ell - 1$. Thus $\sum_D u^{(t)}_\mathbf{d} \geq w_\Delta(\sum_D u^{(t)}_\mathbf{d}\mathbf{d}) = (p^\ell - 1)w_\Delta(\mathbf{e}_t)$.

For any integer $0 \leq u \leq p^\ell - 1$, we have $(p-1)\sum_{t=0}^{\ell-1} u^{(t)} = (p^\ell - 1)s_p(u)$; summing up the above inequalities for $0 \leq t \leq \ell - 1$ and simplfying by $p^\ell - 1$, we get

$$\delta\ell(p-1) = \sum_D s_p(u_\mathbf{d}) \geq (p-1)\sum_{t=0}^{\ell-1} w_\Delta(\mathbf{e}_t) \geq (p-1)(\ell\omega(\Delta) + \frac{\ell - k}{d_\Delta})$$

where the first equality holds since we assumed $U$ minimal. Now we use the upper bound on $\delta$ from the first part of the proof. From the definition of the denominator of $\Delta$, $\omega(\Delta)$ has denominator at most $d_\Delta$, and we get

$$\delta\ell(p-1) \leq \ell\lceil (p-1)\omega(\Delta)\rceil \leq \ell(p-1)\omega(\Delta) + \ell\frac{d_\Delta - 1}{d_\Delta}$$

Summing up we get $p \leq 1 + \frac{\ell}{\ell-k}(d_\Delta - 1)$. If $\ell \leq N_\Delta$ we have $\frac{\ell}{\ell-k} \leq \ell \leq N_\Delta$; if $\ell > N_\Delta$, we have $\frac{\ell}{\ell-k} \leq \frac{\ell}{\ell-N_\Delta} \leq N_\Delta + 1$. In any case we have $p \leq 1 + (d_\Delta - 1)(N_\Delta + 1)$, contradicting our hypothesis. As a consequence we must have $\ell = k$, the support of $U$ is contained in $\Sigma(\Delta)$, and we get the inclusion $\Sigma \subset \Sigma(\Delta)$.

We now determine the density. Choose some minimal $U \in E(\ell)$ with support $\varphi_U$; from the above inclusion we must have $\varphi_U(j) \in \Sigma(\Delta)$ for all $0 \leq j \leq \ell - 1$. From Lemma 2.15 (i), we have for any $0 \leq j \leq \ell - 1$ the equality $\sum_D \mathbf{d} u_{\mathbf{d}j} = p\varphi_U(j+1) - \varphi_U(j)$. Considering the weights, we get

$$(8)\quad \sum_D u_{\mathbf{d}j} \geq w_\Delta(\sum_D \mathbf{d} u_{\mathbf{d}j}) \geq p w_\Delta(\varphi_U(j+1)) - w_\Delta(\varphi_U(j)) = (p-1)\omega(\Delta)$$

Thus for any $j$ we get the inequality $\sum_D u_{\mathbf{d}j} \geq \lceil (p-1)\omega(\Delta) \rceil$. We deduce the inequality $s_p(U) = \sum_D \sum_{j=0}^{\ell-1} u_{\mathbf{d}j} \geq \ell \lceil (p-1)\omega(\Delta) \rceil$, and we must have $\delta = \frac{1}{p-1}\lceil (p-1)\omega(\Delta) \rceil$.

Consequently the length 1 solutions we have constructed at the beginning of the proof are minimal. Their supports lie in the minimal support, and we get the equality $\Sigma = \Sigma(\Delta)$. □

Remark 3.6. It follows from (8) that if $U$ is a minimal solution then for any $j$ we have $\sum_D u_{\mathbf{d}j} = \lceil (p-1)\omega(D) \rceil = \delta(p-1)$.

As a consequence, for any $\mathbf{e}, \mathbf{e}' \in \Sigma(\Delta)$, the set $V(\mathbf{e}, \mathbf{e}')$ can be written

$$V(\mathbf{e}, \mathbf{e}') := \left\{ (v_{\mathbf{d}})_D,\ 0 \leq v_{\mathbf{d}} \leq p-1,\ \sum_D v_{\mathbf{d}} = \delta(p-1),\ \sum_D \mathbf{d} v_{\mathbf{d}} = p\mathbf{e}' - \mathbf{e} \right\}$$

Now that we have determined all the invariants, we can write the matrix $\mathrm{HW}(f)$ explicitly; we begin with a

Definition 3.7. Let $F = \sum_D \gamma_{\mathbf{d}} \mathbf{x}^{\mathbf{d}} \in \mathbf{Q}_p(\zeta_{q-1})[\mathbf{x}]$ denote a polynomial, and $k$ an integer; we define the polynomial

$$F^{[k]}(\mathbf{x}) := \sum_{0 \leq v_{\mathbf{d}} \leq p-1,\ \sum v_{\mathbf{d}} = k} \left( \prod_D \frac{\gamma_{\mathbf{d}}^{v_{\mathbf{d}}}}{v_{\mathbf{d}}!} \right) \mathbf{x}^{\sum \mathbf{d} v_{\mathbf{d}}}$$

For any $\mathbf{e} \in \mathbf{N}^n$, we denote by $\{F\}_{\mathbf{e}}$ the degree $\mathbf{e}$ coefficient of the polynomial $F$.

Remark 3.8. For $1 \leq k \leq p-1$, we have $F^k = k! F^{[k]}$: this is a reason for the notation to look as divided powers.

With these notations at hand, the description of $V(\mathbf{e}, \mathbf{e}')$ gives

PROPOSITION 3.9. *Let $D$ satisfy Hypothesis* 3.4 *above, and $p > 1 + (d_\Delta - 1)(N_\Delta + 1)$; for any $1 \leq k, l \leq N_\Delta$, the $(k, l)$ coefficient of the Hasse-Witt matrix associated to $f$ is*

$$m_{kl}(f) = \pi^{\delta(p-1)} \left\{ \widetilde{f}^{[\delta(p-1)]} \right\}_{p\mathbf{e}_l - \mathbf{e}_k}$$

REMARK 3.10. In the one dimensional case we consider $D := \{1, \ldots, d\}$; we have $\Delta = [0, d]$, $\Sigma(\Delta) = \{1\}$, $N_\Delta = 1$ and $\omega(\Delta) = \frac{1}{d}$. If we assume $p > 2d - 1$, we get $\delta = \frac{1}{p-1}\lceil \frac{p-1}{d} \rceil$, and the Hasse-Witt matrix consists of the single coefficient

$$m_{11}(f) = \pi^{\delta(p-1)} \left\{ \widetilde{f}^{[\delta(p-1)]} \right\}_{p-1} = \frac{\pi^{\lceil \frac{p-1}{d} \rceil}}{\lceil \frac{p-1}{d} \rceil !} \left\{ \widetilde{f}^{\lceil \frac{p-1}{d} \rceil} \right\}_{p-1}$$

This is [25, Theorem 1.1].

3.4 – *Zeta functions of affine varieties*

Let $X \subset \mathbf{A}^n$ denote the affine variety defined over $\mathbf{F}_q$ by the vanishing of the polynomials $f_1, \ldots, f_a$ with respective degrees $d_1, \ldots, d_a$.

Let $\boldsymbol{\mu}$ denote the least nonnegative integer greater than or equal to

$$\frac{n - \sum_{i=1}^{a} d_i}{\max\{d_i,\ 1 \leq i \leq a\}} \tag{9}$$

Katz [11] has shown that for any $r \geq 1$, the number $N_r(X)$ of points of $X$ over the degree $r$ extension of $\mathbf{F}_q$ is divisible by $q^{r\boldsymbol{\mu}}$. Equivalently, in terms of the zeta function $Z(X, T)$, we have

(i) the reciprocal roots and poles of $Z(X, T)$ are algebraic integers divisible by $q^{\boldsymbol{\mu}}$,

(ii) $Z(X, T)$ lies in $\mathbf{Z}[[q^{\boldsymbol{\mu}} T]]$,

(iii) $Z(X, q^{-\boldsymbol{\mu}} T)$ has integer coefficients.

For each $1 \leq i \leq a$, we write $f_i := \sum_{D_i} c_{i\mathbf{d}} \mathbf{x}^{\mathbf{d}}$. We shall apply Theorem 1 to the polynomial $F(\mathbf{x}, x_{n+1}, \ldots, x_{n+a}) := \sum_{i=1}^{a} x_{n+i} f_i(\mathbf{x})$: from orthogonality relations on additive characters, we have $S_r(F) = q^{ar} N_r(X)$ for any $r \geq 1$, and

$$Z(X, T) = L(F, q^{-a} T) \tag{10}$$

We work in the affine space $\mathbf{R}^{n+a}$, and for any $1 \leq i \leq n+a$, we denote by $\mathbf{u}_i$ the point $(0, \ldots, 0, 1, 0, \ldots, 0)$, where the 1 sits at the $i$th place. We denote by $z_1, \ldots, z_{n+a}$ the coordinates in this space.

For each $1 \leq i \leq a$, we have $D_i = \Delta_i \cap \mathbf{N}^n$, with $\Delta_i$ the simplex in $\mathbf{R}^n \subset \mathbf{R}^{n+a}$ with vertices the origin and the points $d_i \mathbf{u}_j$, $1 \leq j \leq n$.

We recall the following from [1, Section 5]. Let $\Delta$ denote the polytope in $\mathbf{R}^{n+a}$ with vertices the origin, the points $\mathbf{u}_i$, $n+1 \leq i \leq n+a$, and the $d_i \mathbf{u}_j + \mathbf{u}_{n+i}$, $1 \leq j \leq n$, $1 \leq i \leq a$. Then $D = \Delta \cap \mathbf{N}^{n+a}$ is the set of exponents of $F$, and it satisfies Hypothesis 3.4. This polytope is delimited by the hyperplanes $z_i = 0$, $\sum_{i=1}^n z_i = \sum_{i=1}^a d_i z_{n+i}$, and $\sum_{i=1}^a z_{n+i} = 1$. Since the last one is the unique one that does not contain the origin, the weight $w_\Delta(z_1, \ldots, z_{n+a})$ of an element in the cone $C(\Delta)$ is given by $\sum_{i=1}^a z_{n+i}$, and the denominator is $d_\Delta = 1$. Moreover we have $\omega(\Delta) = \boldsymbol{\mu} + a$.

We introduce a notation

Definition 3.11. For $\mathbf{t} = (t_1, \ldots, t_a) \in \mathbf{N}^a$, we set $\mathbf{f}^{[\mathbf{t}]} := \prod_{i=1}^a f_i^{[t_i]}$ and $\widetilde{\mathbf{f}}^{[\mathbf{t}]} := \prod_{i=1}^a \widetilde{f}_i^{[t_i]}$, where $\widetilde{f}$ denotes the Teichmüller lift of $f$.

Applying Propositions 3.5 and 3.9 to this case, we get

Lemma 3.12. *The invariants associated to $D$ and $p$ are independant of $p$; the density is $\delta = \boldsymbol{\mu} + a$, and the minimal support is*

$$\Sigma = \left\{ (\mathbf{s}, \mathbf{t}) \in (\mathbf{N}_{>0})^n \times (\mathbf{N}_{>0})^a, \ \sum_{i=1}^a t_i = \boldsymbol{\mu} + a, \ \sum_{j=1}^n s_j \leq \sum_{i=1}^a d_i t_i \right\}$$

*If we set $\Sigma := \{(\mathbf{s}_k, \mathbf{t}_k), \ 1 \leq k \leq N\}$, then for any $1 \leq k, l \leq N$, the $(k,l)$-coefficient of* $\mathrm{HW}(F)$ *is*

$$m_{kl}(F) = \pi^{(p-1)(a+\boldsymbol{\mu})} \left\{ \widetilde{\mathbf{f}}^{[p\mathbf{t}_l - \mathbf{t}_k]} \right\}_{p\mathbf{s}_l - \mathbf{s}_k}$$

Proof. The assertions on the density and the minimal support come from Proposition 3.5; here the condition on $p$ is empty since we have $d_\Delta = 1$

We determine the Hasse-Witt matrix $\mathrm{HW}(F)$.

We have $F := \sum_{i=1}^a \sum_{\mathbf{d} \in D_i} c_{i\mathbf{d}} \mathbf{x}^{\mathbf{d}} x_{n+i}$, and let $\gamma_{i\mathbf{d}}$ denote the Teichmüller lifting of $c_{i\mathbf{d}}$. If $(\mathbf{s}_k, \mathbf{t}_k)$, $(\mathbf{s}_l, \mathbf{t}_l)$ are elements of $\Sigma$, we deduce from Proposition 3.9 the equality

$$m_{kl}(F) = \pi^{(p-1)(a+\boldsymbol{\mu})} \sum \prod_{i=1}^a \prod_{D_i} \frac{\gamma_{i\mathbf{d}}^{v_{i\mathbf{d}}}}{v_{i\mathbf{d}}!}$$

where the sum is over the set $V((\mathbf{s}_k,\mathbf{t}_k),(\mathbf{s}_l,\mathbf{t}_l))$ consisting of those $(V_i)_{1\leq i\leq a}$, $V_i=(v_{i\mathbf{d}})_{\mathbf{d}\in D_i}$ satisfying $0\leq v_{i\mathbf{d}}\leq p-1$, $\sum_{i=1}^a\sum_{D_i}\mathbf{d}v_{i\mathbf{d}}=p\mathbf{s}_l-\mathbf{s}_k$, $(\sum_{D_1}v_{1\mathbf{d}},\dots,\sum_{D_a}v_{a\mathbf{d}})=p\mathbf{t}_l-\mathbf{t}_k$ from Remark 3.6. Note that the equality $\sum\sum v_{i\mathbf{d}}=\lceil(p-1)\omega(D)\rceil=(p-1)(\boldsymbol{\mu}+a)$ comes by adding the $a$ coordinates in the preceding equation.

The coefficient in the right hand side of the equality can be written

$$\left\{\widetilde{\mathbf{f}}^{[p\mathbf{t}_l-\mathbf{t}_k]}\right\}_{p\mathbf{s}_l-\mathbf{s}_k}=\sum\prod_{i=1}^a\prod_{D_i}\frac{\gamma_{i\mathbf{d}}^{w_{i\mathbf{d}}}}{w_{i\mathbf{d}}!}$$

where the sum is over those $W=(W_1,\dots,W_a)$, $W_i=(w_{i\mathbf{d}})_{\mathbf{d}\in D_i}$ such that $0\leq w_{i\mathbf{d}}\leq p-1$, $(\sum_{D_1}w_{1\mathbf{d}},\dots,\sum_{D_a}w_{a\mathbf{d}})=p\mathbf{t}_l-\mathbf{t}_k$ and $\sum_{i=1}^a\sum_{D_i}\mathbf{d}w_{i\mathbf{d}}=p\mathbf{s}_l-\mathbf{s}_k$. □

In order to give a congruence modulo $p$, we slightly modify the definition of the Hasse-Witt matrix, and define a new matrix over the field $\mathbf{F}_q$. Note that we have $\pi^{p-1}\equiv -p \mod p\pi$ in $\mathbf{Q}_p(\zeta_p)$.

Definition 3.13. The *Hasse-Witt matrix* of the variety $X$ is $\mathrm{HW}(X)\in\mathbf{M}_N(\mathbf{F}_q)$ defined by $\mathrm{HW}(X)\equiv\pi^{-(p-1)(\boldsymbol{\mu}+a)}\,\mathrm{HW}(F) \mod p$, i.e. with coefficients

$$m_{kl}(X)=(-1)^{\boldsymbol{\mu}+a}\left\{\mathbf{f}^{[p\mathbf{t}_l-\mathbf{t}_k]}\right\}_{p\mathbf{s}_l-\mathbf{s}_k}$$

For any $\emptyset\neq J\subset\{1,\dots,n\}$, $\emptyset\neq K\subset\{1,\dots,a\}$ ,we define $\mathrm{HW}_{J,K}(X)$ as the matrix associated to $\mathrm{HW}(F_{J\cup K})$ as above.

Remark 3.14. In the case $a=1$ of an hypersurface, this matrix is the transpose of the matrix $A(\Lambda)$ defined in [3]: our matrix is the matrix of a $\sigma$-linear morphism, whereas the matrix $A(\Lambda)$ is the matrix of a $\sigma^{-1}$-linear morphism. Our choice comes from the fact that usually, the Hasse-Witt matrix is the matrix of a $\sigma$-linear operator, whereas its (twisted) transpose is the matrix of the Cartier-Manin operation, which is $\sigma^{-1}$-linear.

We deduce the congruence for the zeta function $Z(X,T)$ from the calculations above.

Theorem 3. *Let $X\subset\mathbf{A}^n$ denote the affine variety defined over $\mathbf{F}_q$ by the vanishing of the polynomials $f_1,\dots,f_a$ with respective degrees $d_1,\dots,d_a$.*

*For any $\emptyset\neq J\subset\{1,\dots,n\}$, $\emptyset\neq K\subset\{1,\dots,a\}$, let $\boldsymbol{\mu}(J,K)$ denote the least nonnegative integer greater than or equal to*

$$\frac{|J|-\sum_{i\in K}d_i}{\max\{d_i,\ i\in K\}}$$

*and* $\mathrm{HW}_{J,K}(X)$ *the corresponding Hasse-Witt matrix.*

*The zeta function of* $X$ *satisfies*

$$Z(X, q^{-\boldsymbol{\mu}}T)^{(-1)^{n+a+1}} \equiv$$

$$\prod \det\left(\mathbf{I} - \mathrm{HW}_{J,K}(X)\cdots\mathrm{HW}_{J,K}(X)^{\sigma^{m-1}}T\right)^{(-1)^{n+a-|J|-|K|}} \mod p$$

*where the product is over those* $J, K$ *such that* $\boldsymbol{\mu}(J,K) + n - |J| = \boldsymbol{\mu}$.

Proof. We apply Theorem 1 to our situation. From (10), we have $Z(X, q^{-\boldsymbol{\mu}}T) = L(F, q^{-\boldsymbol{\mu}-a}T)$, and this last function is congruent modulo $\mathfrak{I}_1$ to

$$\prod \det\left(\mathbf{I}_{N_I} - q^{n-|I|-\boldsymbol{\mu}}\,\mathrm{HW}_I(F)\cdots\mathrm{HW}_I(F)^{\tau^{m-1}}T\right)^{(-1)^{|I|+1}}$$

where the product is over those $I \subset \{1,\dots,n+a\}$ such that $\delta_I + n - |I| = \boldsymbol{\mu}$. Note that since these functions have their coefficients in $\mathbf{Z}_p$, we actually get a congruence modulo $p$.

It remains to determine all such $I$. First note that when $I \subset \{1,\dots,n\}$, we have $D_I = \{0\}$, and the corresponding factor cannot appear in the congruence. When $I \subset \{n+1,\dots,n+a\}$, $D_I$ consists of the points $\mathbf{u}_i$, $i \in I$, we get $\boldsymbol{\mu}(I) = |I|$, and $\boldsymbol{\mu}(I) + n > n \geq \boldsymbol{\mu}$.

Thus we write $I = J \cup K$ for some non empty $J \subset \{1,\dots,n\}$ and $K \subset \{1,\dots,a\}$. In this case, the density $\delta_I$ is $\boldsymbol{\mu}(J,K) + |K|$. As a consequence, the term coming from $I = (J,K)$ appears in the congruence exactly when $\boldsymbol{\mu}(J,K) + n - |J| = \boldsymbol{\mu}$. For such an $I$ we have the congruence modulo $p$

$$q^{n-|I|-\boldsymbol{\mu}}\,\mathrm{HW}_I(F)\cdots\mathrm{HW}_I(F)^{\tau^{m-1}} \equiv \mathrm{HW}_{J,K}(X)\cdots\mathrm{HW}_{J,K}(X)^{\sigma^{m-1}}$$

and this is the desired result. □

## References


[1] A. Adolphson – S. Sperber, *p-adic estimates for exponential sums and the theorem of Chevalley-Warning,* Ann. Sci. École Norm. Sup. (4) **20** (1987), no. 4, pp. 545–556.

[2] A. Adolphson – S. Sperber, *Hasse invariants and mod p solutions of A-hypergeometric systems,* J. Number Theory **142** (2014), pp. 183–210.

[3] A. Adolphson – S. Sperber, *A generalization of the Hasse-Witt matrix of a hypersurface,* Finite Fields Appl. **47** (2017), pp. 203–221.

[4] J. Ax, *Zeroes of polynomials over finite fields,* Amer. J. Math. **86** (1964), pp. 255–261.

[5] P. Berthelot – A. Ogus, *Notes on crystalline cohomology,* Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1978.

[6] R. Blache – É. Férard, *Newton stratification for polynomials: the open stratum,* J. Number Theory **123** (2007), no. 2, pp. 456–472.

[7] R. Blache, *Valuation of exponential sums and the generic first slope for Artin-Schreier curves,* J. Number Theory **132** (2012), no. 10, pp. 2336–2352.

[8] E. Bombieri, *On exponential sums in finite fields,* Amer. J. Math. **88** (1966), pp. 71–105.

[9] R. M. Crew, *Etale p-covers in characteristic p,* Compositio Math. **52** (1984), no. 1, pp. 31–45.

[10] B. Dwork, *On the zeta function of a hypersurface,* Inst. Hautes Études Sci. Publ. Math. (1962), no. 12, pp. 5–68.

[11] N. Katz, *On a theorem of Ax,* Amer. J. Math. **93** (1971), pp. 485–499.

[12] N. Katz, *Algebraic solutions of differential equations (p-curvature and the Hodge filtration),* Invent. Math. **18** (1972), pp. 1–118.

[13] N. Katz, *Une formule de congruence pour la fonction zêta,* Groupes de monodromie en géométrie algébrique. II, Lecture Notes in Mathematics, Vol. 340, Springer-Verlag, Berlin-New York, 1973, Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 II), Dirigé par P. Deligne et N. Katz, pp. x+438.

[14] N. Katz, *Slope filtration of F-crystals,* Journées de Géométrie Algébrique de Rennes (Rennes, 1978), Vol. I, Astérisque, vol. 63, Soc. Math. France, Paris, 1979, pp. 113–163.

[15] Ju I. Manin, *The Hasse-Witt matrix of an algebraic curve,* Izv. Akad. Nauk SSSR Ser. Mat. **25** (1961), pp. 153–172.

[16] B. Mazur, *Frobenius and the Hodge filtration,* Bull. Amer. Math. Soc. **78** (1972), pp. 653–667.

[17] L. Miller, *The Hasse-Witt-matrix of special projective varieties,* Pacific J. Math. **43** (1972), pp. 443–455.

[18] O. Moreno – K. W. Shum – F. N. Castro – P. V. Kumar, *Tight bounds for Chevalley-Warning-Ax-Katz type estimates, with improved applications,* Proc. London Math. Soc. (3) **88** (2004), pp. 545–564.

[19] N. Nygaard, *On supersingular abelian varieties,* Algebraic geometry (Ann Arbor, Mich., 1981), Lecture Notes in Math. vol. 1008, Springer, Berlin, 1983, pp. 83–101.

[20] F. Oort, *Abelian varieties isogenous to a Jacobian in: Problems from the workshop on automorphisms of curves*, Rend. Sem. Mat. Univ. Padova **113** (2005), pp. 129–177.

[21] P. Robba, *Index of p-adic differential operators. III. Application to twisted exponential sums,* Astérisque, (1984), no. 119-120, 7, pp. 191–266.

[22] J. P. Serre, *Endomorphismes complètement continus des espaces de Banach p-adiques,* Inst. Hautes Études Sci. Publ. Math. (1962), no. 12, pp. 69–85.

[23] J. Scholten – H. J. Zhu, *Families of supersingular curves in characteristic 2,* Math. Res. Lett. **9** (2002), no. 5–6, pp. 639–650.

[24] J. Scholten – H. J. Zhu, *Hyperelliptic curves in characteristic 2,* Int. Math. Res. Not. (2002), no. 17, pp. 905–917.

[25] J. Scholten – H. J. Zhu, *Slope estimates of Artin-Schreier curves,* Compositio Math. **137** (2003), no. 3, pp. 275–292.

[26] S. Sperber, *On the p-adic theory of exponential sums,* Amer. J. Math. **108** (1986), no. 2, pp. 255–296.

[27] D. Wan, *Newton polygons of zeta functions and L functions,* Ann. of Math. (2) **137** (1993), pp. 249–293.

[28] E. Warning, *Bemerkung zur vorstehenden Arbeit von Herrn Chevalley,* Abh. Math. Sem. Univ. Hamburg **11** (1935), pp. 76–83.

[29] H. J. Zhu, *Asymptotic variation of L functions of one-variable exponential sums,* J. Reine Angew. Math. **572** (2004), pp. 219–233.