ACTA ARITHMETICA
118.1 (2005)

A Stickelberger theorem for p-adic Gauss sums

by

Régis Blache (Pointe à Pitre)

0. Introduction. Character sums over finite fields have been widely studied since Gauss. During the last decade, coding theorists initiated the study of a new type of sums, over points with coordinates in a p-adic field. Let $\mathcal{O}_m^{(u)}$ be the ring of integers of $K_m = \mathbb{Q}_p(\zeta_{p^m-1})$, the unramified extension of degree m of the field of p-adic numbers $\mathbb{Q}_p$ obtained by adjoining the (p^m-1)th roots of unity, and $\mathcal{T}_m = \mathcal{T}_m^* \cup \{0\}$ the *Teichmüller* of $\mathcal{O}_m^{(u)}$, where $\mathcal{T}_m^*$ is the multiplicative subgroup of elements of finite order in $\mathcal{O}_m^{(u)*}$. Many character sums over finite fields can be extended to this situation; the first studied was $\sum_{x\in\mathcal{T}_m} \widetilde{\psi}_{l,m}(f(x))$, $\widetilde{\psi}_{l,m}$ an additive character of order p^l over $\mathcal{O}_m^{(u)}$, f a polynomial in $\mathcal{O}_m^{(u)}[X]$, in order to give a generalization of the Weil–Carlitz–Uchiyama bound (cf. [6], and note that for $l = 1$, we get the sums associated to a polynomial and an additive character over the finite field with p^m elements, $\mathbb{F}_{p^m}$).

In this paper we are concerned with certain sums looking as Gauss sums; precisely, if $\widetilde{\psi}_{l,m}$ is as above, and χ is a multiplicative character of order dividing $p^m - 1$, we define the *p-adic Gauss sum of level l* associated with the characters $\widetilde{\psi}_{l,m}$ and χ as

$$G_{\mathcal{T}_m}(\widetilde{\psi}_{l,m}, \chi) = \sum_{x\in\mathcal{T}_m^*} \widetilde{\psi}_{l,m}(x)\chi(x).$$

These sums have already been studied in [11], where a bound is given, and in [8], which has been our starting point.

Here we do not give a bound; we focus on the p-adic valuation of these character sums. Our aim is to generalize the following theorem of Stickelberger on classical Gauss sums to this situation. We first recall some notations: let $\widetilde{\psi}_{1,m}$ be an additive character of order p on $\mathcal{O}_m^{(u)}$, and χ a

2000 *Mathematics Subject Classification*: 11L05, 11L07, 11T24.

Key words and phrases: Gauss sums, Stickelberger theorem, splitting functions, Witt vectors.

multiplicative character of order exactly $p^m - 1$, both taking values in $\mathbb{C}_p$, the (algebraically closed) completion of an algebraic closure of $\mathbb{Q}_p$. If we set $\gamma = \widetilde{\psi}_{1,m}(1) - 1$, then γ is a generator of the maximal ideal of the ring of integers of Ω_1, the ramified extension of degree $p-1$ of $\mathbb{Q}_p$ obtained by adjoining the pth roots of unity. Let $K_{1,m}$ be the compositum of Ω_1 and K_m. In this situation, the Gauss sums of level 1 are exactly the classical Gauss sums over finite fields (cf. [2]), and we have:

Theorem (Stickelberger, [7]). *In $\mathcal{O}_{1,m}$, the ring of integers of $K_{1,m}$, for any $0 \le a \le p^m - 2$, we have*

$$G_{\mathcal{T}_m}(\chi^{-a}, \widetilde{\psi}_{1,m}) \equiv -\frac{\gamma^{s(a)}}{p(a)} \; [\gamma^{s(a)+1}],$$

where if $a = a_0 + pa_1 + \cdots + p^{m-1}a_{m-1}$ is the p-adic expansion of the integer a, we define $s(a) := a_0 + a_1 + \cdots + a_{m-1}$ and $p(a) := a_0! \cdots a_{m-1}!$.

We use ideas close to Dwork's in his proof of the rationality of the zeta functions of varieties over finite fields (cf. [4]); our generalization of this theorem relies on an improvement of his splitting functions. Roughly speaking, a splitting function, in the sense of Dwork, is an analytic representation of an additive character of order p with values in $\mathbb{C}_p^*$; it is a power series Θ with coefficients in Ω_1, converging in the closed disk of center 0 and radius 1, and such that for any $t \in \mathcal{T} := \mathcal{T}_1$, $\Theta(t) = \psi_1(\overline{t})$, where $\overline{t}$ is the image of t in the finite field with p elements $\mathbb{F}_p \simeq \mathbb{Z}_p/p\mathbb{Z}_p$, and ψ_1 is a nontrivial additive character of $\mathbb{F}_p$. Let us give an example of such a function. Consider the series

$$G(X) = \sum_{i \ge 0} \frac{X^{p^i}}{p^i} \in \mathbb{Q}_p[[X]].$$

It has $p-1$ zeroes of valuation $(p-1)^{-1}$, and if γ_1 is one of them, then the series $\theta_1(X) := \exp(G(\gamma_1 X))$ converges in the closed unit disk, and is a splitting function.

The main problem here is to extend this concept to additive characters of order p^l. We shall define *splitting functions of level l*, in order to give an analytic representation of an additive character $\widetilde{\psi}_l$ of $\mathbb{Z}_p$ of order p^l. The first point is to define functions representing the p^lth roots of unity; in order to do this we follow closely the ideas of Dwork, replacing γ_1 as above by γ_l, a zero of G of valuation $(p^{l-1}(p-1))^{-1}$, and defining $\theta_l(X) := \exp(G(\gamma_l X))$. Then we use the Witt vectors representation of the rings $\mathbb{Z}_p/p^l\mathbb{Z}_p$ and $\mathcal{O}_m^{(u)}/p^l\mathcal{O}_m^{(u)}$. Since $\mathbb{Z}_p/p^l\mathbb{Z}_p \simeq \mathbb{Z}/p^l\mathbb{Z} \simeq W_l(\mathbb{F}_p)$, the ring of Witt vectors of length l with coefficients in $\mathbb{F}_p$, we shall require a splitting function Θ_l to satisfy, for any $(t_0, \ldots, t_{l-1})$ in $\mathcal{T}^l$, the condition that $\Theta_l(t_0, \ldots, t_{l-1}) = \psi_l(\overline{t}_0, \ldots, \overline{t}_{l-1})$, where ψ_l is a character of $W_l(\mathbb{F}_p)$ via the above isomorphisms. Once this has been done, the generalization of Stickelberger's theorem is an easy consequence of the description of the coefficients of the splitting function.

The paper is organized as follows: we begin Section 1 by recalling some useful results on p^lth roots of unity in $\mathbb{C}_p$. Then we use the Artin–Hasse exponential and the roots of Artin–Hasse power series to construct power series whose values at the elements of $\mathcal{T}$ are p^lth roots of unity; note that this construction is very close to Dwork's construction of his splitting functions (cf. [4]). In Section 2, after recalling some definitions about rings of Witt vectors, we define splitting functions of level l, and we give an example of such a function relying on the preceding construction; this is Theorem 2.3. The key lemma in its proof is Lemma 2.4. It gives a link between the shape of Artin–Hasse power series and certain polynomials arising from the addition of Witt vectors, and allows us to show that our function represents an additive character. Section 3 is devoted to the proof of Stickelberger's theorem.

Notations. In this paper, $\mathbb{Q}_p$ is the field of p-adic numbers, $\mathbb{Z}_p$ the ring of p-adic integers; let $\mathcal{T} := \{x \in \mathbb{Z}_p;\ x^p = x\} \subset \mathbb{Z}_p$ be the *Teichmüller* of $\mathbb{Z}_p$. Note that $\mathcal{T} = \mathcal{T}^\times \cup \{0\}$, where $\mathcal{T}^\times = \{x \in \mathbb{Z}_p;\ x^{p-1} = 1\}$ is the subgroup of elements of finite order in $\mathbb{Z}_p^\times$. Let also $k := \mathbb{F}_p$ be the residue field of $\mathbb{Z}_p$. Note that $\mathcal{T}$ is the image of a lifting of k to $\mathbb{Z}_p$, called the *Teichmüller lifting.*

We denote by $\mathbb{C}_p$ a completion of the algebraic closure of $\mathbb{Q}_p$, and by v_p the p-adic valuation on $\mathbb{C}_p$, normalized such that $v_p(p) = 1$. Let K_m be the extension of $\mathbb{Q}_p$ generated by the $(p^m - 1)$th roots of unity; it is well known that K_m is an unramified extension of degree m of $\mathbb{Q}_p$. We denote by $\mathcal{O}_m^{(u)}$ its valuation ring, and by $\mathcal{T}_m$ its *Teichmüller*, $\mathcal{T}_m := \{x \in \mathcal{O}_m^{(u)};\ x^{p^m} = x\}$; once again, $\mathcal{T}_m = \mathcal{T}_m^\times \cup \{0\}$, where $\mathcal{T}_m^\times = \{x \in \mathbb{Z}_p;\ x^{p^m-1} = 1\}$ is the subgroup of elements of finite order in $\mathcal{O}_m^{(u)\times}$, and $\mathcal{T}_m$ is the image of the *Teichmüller lifting*, a lifting of $k_m := \mathbb{F}_{p^m}$ to $\mathcal{O}_m^{(u)}$. Recall that any element $x \in K_m$ can be written uniquely as

$$x = p^{-r}t_{-r} + \cdots + t_0 + pt_1 + \cdots$$

for some $t_{-r}, \ldots, t_0, t_1, \ldots$ in $\mathcal{T}_m$.

The extension $K_m/\mathbb{Q}_p$ is Galois, with cyclic Galois group of order m, generated by the *Frobenius* F, whose action on $x = p^{-r}t_{-r} + \cdots + t_0 + pt_1 + \cdots$ is

$$F(x) = p^{-r}t_{-r}^p + \cdots + t_0^p + pt_1^p + \cdots .$$

We can also define a trace from K_m to $\mathbb{Q}_p$ by $\mathrm{Tr}(x) = x + F(x) + \cdots + F^{m-1}(x)$.

Let $l \geq 1$ be an integer. We let $R := R_1$ be the ring $\mathbb{Z}/p^l\mathbb{Z} = \mathbb{Z}_p/p^l\mathbb{Z}_p$, and $R_m = \mathcal{O}_m^{(u)}/p^l\mathcal{O}_m^{(u)}$. Note that the action of Frobenius passes to the quotient; in this way, we can consider the ring R_m as the unramified cyclic extension of R of degree m, adopting the terminology in [9].

1. Analytic representation of p^lth roots of unity. We begin this section by giving properties of p^lth roots of unity, and the extensions of $\mathbb{Q}_p$ they generate, in Subsection 1.1. Then, in Subsection 1.2, we consider series whose values at elements of $\mathcal{T}^\times$ are such roots. Dwork has already shown that the series

$$G(X) = \sum_{i\geq 0} \frac{X^{p^i}}{p^i} \in \mathbb{Q}_p[[X]]$$

has $p-1$ zeroes of valuation $(p-1)^{-1}$, and that given one of these zeroes, say γ_1, the values of the series $\theta_1(X) := \exp(G(\gamma_1 X))$ at elements of $\mathcal{T}^\times$ are pth roots of unity. Here we generalize this remark to p^lth roots of unity, using the roots of G of valuation $(p^{l-1}(p-1))^{-1}$.

1.1. *The fields generated by p^lth roots of unity.* Let $\Omega_l := \mathbb{Q}_p(\zeta_{p^l})$ denote the extension of $\mathbb{Q}_p$ obtained by adjoining a primitive p^lth root of unity ζ_{p^l}, and $\mathcal{O}_l^{(r)}$ its ring of integers.

LEMMA 1.1. *The field Ω_l is a totally ramified extension of $\mathbb{Q}_p$, of degree $p^l - p^{l-1}$; moreover, we have*

$$v_p(\zeta_{p^l} - 1) = (p^l - p^{l-1})^{-1},$$

that is, $\zeta_{p^l} - 1$ is a generator of the maximal ideal $m_l^{(r)}$ of the local ring $\mathcal{O}_l^{(r)}$.

Proof. Clearly a primitive p^lth root of unity is a root of the polynomial

$$(X^{p^l} - 1)/(X^{p^{l-1}} - 1) = X^{(p-1)p^{l-1}} + \cdots + X^{p^{l-1}} + 1.$$

Thus $\zeta_{p^l} - 1$ is a root of $P(X) := (X+1)^{(p-1)p^{l-1}} + \cdots + (X+1)^{p^{l-1}} + 1$. Looking modulo p, we get

$$\begin{aligned} P(X) &\equiv (X^{p^{l-1}} + 1)^{p-1} + \cdots + (X^{p^{l-1}} + 1) + 1 \ [p] \\ &\equiv \sum_{k=1}^{p} \Big(\sum_{i=1}^{k} C_{p-i}^{k-i} \Big) X^{(p-k)p^{l-1}} \ [p]. \end{aligned}$$

Now since $C_{p-i}^{k-i} \equiv (-1)^{k-i} C_{k-1}^{i-1}$ $[p]$, the coefficient of degree k is zero modulo p for $k \geq 2$; we get $P(X) \equiv X^{(p-1)p^{l-1}}$ $[p]$. Since the constant term of P is p, it is an Eisenstein polynomial, thus irreducible, and all its roots are of valuation $(p^{l-1}(p-1))^{-1}$, generating the maximal ideal of $\mathcal{O}_l^{(r)}$.

The following corollary will be useful:

COROLLARY 1.2. *Let ζ and ζ' be two p^lth roots of unity in $\mathbb{C}_p$. If $v_p(\zeta-\zeta') > 1$, then $\zeta = \zeta'$.*

Proof. Since $\zeta - \zeta' = \zeta'(\zeta(\zeta')^{-1} - 1)$, we have $v_p(\zeta(\zeta')^{-1} - 1) > 1$, and $\zeta(\zeta')^{-1}$ is a p^kth root of unity for some $0 \le k \le l$. Thus from Lemma 1.1, we must have $k = 0$, that is, $\zeta = \zeta'$.

1.2. *Analytic representation of p^lth roots of unity.* Let us begin by a quick overview of the theory of Newton polygons (cf. [1, Chapter 4.3], [5, Chapter IV]). If $f(X) := \sum_{n\ge0} a_n X^n$ is a polynomial or a power series in $\mathbb{C}_p[[X]]$, its *Newton polygon* $\mathrm{NP}(f)$ is the convex hull of the set of points with coordinates $(n, v_p(a_n))$, $n \ge 0$. Then we have the following remarkable result (cf. [1, Theorem 4.4.4], [5, p. 106, Corollary to Theorem 14]): if $\mathrm{NP}(f)$ has an edge of (horizontal) length l and slope s, then f has exactly l zeroes of valuation $-s$ in $\mathbb{C}_p$. Applying this result to G, we see that for any $k \ge 1$, $G(X)$ has $p^k - p^{k-1}$ zeroes of valuation $(p^k - p^{k-1})^{-1}$ in $\mathbb{C}_p$.

LEMMA 1.3. *Let γ_l be a zero of G with $v_p(\gamma_l) = (p^l - p^{l-1})^{-1}$, $l \ge 2$. Then there is a unique root γ_{l-1} of G with valuation $(p^{l-1} - p^{l-2})^{-1}$ such that $\gamma_{l-1} \equiv \gamma_l^p\ [p\gamma_l]$.*

Proof. We will consider the Newton polygon of $G_l(X) := G(X + \gamma_l^p)$. Set $G_l(X) := \sum_{k\ge0} f_k X^k$. For $k \ge 1$, a rapid calculation gives

$$f_k = \sum_{i \ge \lceil \log_p(k) \rceil} \frac{C_{p^i}^k}{p^i} \gamma_l^{p(p^i-k)}.$$

Since $v_p(C_{p^i}^k) = i - v_p(k)$, we get $v_p(f_k) \ge -v_p(k)$. Moreover, if $k = p^j$, $j \ge 0$, the term with minimal valuation in f_k is the term $i = j$, which is p^{-j}; we get $v_p(f_{p^j}) = -j$. Finally, the constant term is

$$\sum_{k\ge1} \frac{\gamma_l^{p^k}}{p^{k-1}} = p \sum_{k\ge1} \frac{\gamma_l^{p^k}}{p^k} = p(G(\gamma_l) - \gamma_l) = -p\gamma_l,$$

which is of valuation $1 + (p^l - p^{l-1})^{-1}$. Thus the Newton polygon of G_l has vertices $(0, 1 + (p^l - p^{l-1})^{-1})$ and $(p^k, -k)$, $k \ge 0$. It has an edge of length 1 with slope $-1 - (p^l - p^{l-1})^{-1}$, that is, G_l has a unique zero of valuation $1 + (p^l - p^{l-1})^{-1}$, say α_l, and all other zeroes are of valuation less than or equal to $(p-1)^{-1}$. Finally, G has a unique zero $\gamma_{l-1} := \gamma_l^p + \alpha_l$ such that $\gamma_{l-1} \equiv \gamma_l^p\ [p\gamma_l]$. Any other zero γ satisfies $v_p(\gamma - \gamma_l^p) \le (p-1)^{-1}$.

From the above lemma, we fix once and for all a "compatible" sequence $(\gamma_k)_{0\le k\le l}$ in $\mathbb{C}_p$, that is, γ_l is a fixed root of G of valuation $(p^l - p^{l-1})^{-1}$, for $1 \le k \le l-1$, γ_k is a zero of $G(X)$ of valuation $(p^k - p^{k-1})^{-1}$ such that $\gamma_k \equiv \gamma_{k+1}^p\ [p\gamma_{k+1}]$, and $\gamma_0 := 0$, the trivial zero of G.

Definition 1.4. Let us define the *Artin–Hasse exponential* as $\mathrm{AH}(X) := \exp(G(X))$, and $\theta_k(X) := \mathrm{AH}(\gamma_k X)$, $0 \le k \le l$.

First recall that from Dwork's lemma (cf. [5, IV.2, Lemma 3]), the series $\mathrm{AH}(X)$ is in $1 + X\mathbb{Z}_p[[X]]$. Let us deduce some properties of θ_k from this result.

Proposition 1.5. *Let $1 \le k \le l$. If the development of θ_k in power series in $\mathbb{C}_p[[X]]$ is*

$$\theta_k(X) = \sum_{n\ge 0} \lambda_{n,k} X^n,$$

then its coefficients satisfy

$$v_p(\lambda_{n,k}) \ge \frac{n}{p^k - p^{k-1}}, \quad n \ge 0, \qquad \lambda_{n,k} = \frac{\gamma_k^n}{n!}, \quad 0 \le n \le p-1.$$

In particular the function θ_k converges in the open disk with center 0 *and radius $p^{1/(p^k - p^{k-1})}$.*

Proof. Write $\mathrm{AH}(X) = \sum_{i\ge 0} e_i X^i$. From Dwork's lemma, we know that $e_0 = 1$ and $e_i \in \mathbb{Z}_p$, that is, $v_p(e_i) \ge 0$. Now from the definition of θ_k, we have $\lambda_{n,k} = e_n \gamma_k^n$, and $v_p(\lambda_{n,k}) \ge v_p(\gamma_k^n) = n/(p^k - p^{k-1})$. This shows the first assertion.

Moreover, the first p terms are those of the development of $\exp(\gamma_k X)$ in power series; we get $\lambda_{n,k} = \gamma_k^n/n!$ for $0 \le n \le p-1$.

Now we show that from the compatible system $(\gamma_k)_{0\le k\le l}$ and the functions θ_k, we can define a compatible system of p^lth roots of unity $(\zeta_{p^k})_{0\le k\le l}$ in the following sense:

Definition 1.6. For all $0 \le k \le l$, let ζ_{p^k} be a p^kth root of unity in $\mathbb{C}_p$. We say that the family $(\zeta_{p^k})_{0\le k\le l}$ forms a *compatible system of p^kth roots of unity in* $\mathbb{C}_p$ if the following holds:

(i) ζ_{p^k} is a primitive p^kth root of unity,
(ii) $\zeta_{p^k}^p = \zeta_{p^{k-1}}$ for $1 \le k \le l$.

Proposition 1.7. *The family $(\theta_k(1))_{0\le k\le l}$ forms a compatible system of p^lth roots of unity.*

Proof. Clearly, since $\theta_0(X) = 1$, we have $\theta_0(1) = 1$. Now we show that $\theta_k(1)$ is a primitive p^kth root of unity for $1 \le k \le l$. From the description of θ_k in Proposition 1.5, we have

$$\theta_k(1) = \sum_{n\ge 0} \lambda_{n,k} = 1 + \gamma_k + \cdots$$

(this series converges by Proposition 1.5); this gives in particular

$$v_p(\theta_k(1) - 1) = (p^{k-1}(p-1))^{-1}.$$

Thus from Lemma 1.1 it just remains to show that $\theta_k(1)^{p^k} = 1$.

From the equality of formal power series $\exp(X)^{p^k} = \exp(p^k X)$, we get
$$\mathrm{AH}(X)^{p^k} = \exp(p^k G(X)).$$
Let x be an element of $\mathbb{C}_p$ with $v_p(x) \geq (p^k - p^{k-1})^{-1}$; then
$$v_p\left(p^k \frac{x^{p^i}}{p^i}\right) \geq \frac{p^{i-k+1}}{p-1} - i + k;$$
this quantity is minimal for $i = k-1, k$, and equals then $1 + (p-1)^{-1}$; thus $v_p(p^k G(x)) \geq 1 + (p-1)^{-1}$, and $p^k G(x)$ is in the convergence disk of the exponential. The above equality of formal power series gives $\mathrm{AH}(x)^{p^k} = \exp(p^k G(x))$, and we get
$$\theta_k(1)^{p^k} = \mathrm{AH}(\gamma_k)^{p^k} = \exp(p^k G(\gamma_k)) = \exp(0) = 1.$$
Now we show that $\theta_k(1)^p = \theta_{k-1}(1)$ for $1 \leq k \leq l$. We have
$$\theta_k(1)^p = \Big(\sum_{n\geq 0} \lambda_{n,k}\Big)^p \equiv \sum_{n\geq 0} \lambda_{n,k}^p \ [p\gamma_k],$$
since $\lambda_{n,k} \equiv 0 \ [\gamma_k]$ for $n \geq 1$. Moreover we have $\lambda_{0,k} = \lambda_{0,k-1} = 1$, and $\lambda_{n,k}^p = e_n^p(\gamma_k^p)^n \equiv e_n\gamma_{k-1}^n = \lambda_{n,k-1} \ [p\gamma_k]$ for $n \geq 1$ since $\gamma_k^p \equiv \gamma_{k-1} \ [p\gamma_k]$ by Lemma 1.3 and the e_n are in $\mathbb{Z}_p$. Finally, we get
$$\begin{aligned}\theta_{k-1}(1) = \sum_{n\geq 0} e_n\gamma_{k-1}^n &\equiv \sum_{n\geq 0} e_n\gamma_k^{np} \ [p\gamma_k] \\ &\equiv \sum_{n\geq 0} \lambda_{n,k}^p \ [p\gamma_k] \equiv \theta_k(1)^p \ [p\gamma_k].\end{aligned}$$
Since both sides are p^kth roots of unity, the result now follows from Corollary 1.2.

In the following, we set $\zeta_{p^k} := \theta_k(1)$ for all $0 \leq k \leq l$.

Remark 1.8. (i) If $t \in \mathcal{T}^*$, then $t\gamma_k$ is also a root of G of valuation $(p^{k-1}(p-1))^{-1}$, and the proof of Proposition 1.7 shows that $\theta_k(t) = \mathrm{AH}(t\gamma_k)$ is also a primitive p^kth root of unity.

(ii) We also see that the fields Ω_k and $\mathbb{Q}_p(\gamma_k)$ are equal (they are both totally ramified extensions of degree $p^k - p^{k-1}$ of $\mathbb{Q}_p$, and Proposition 1.7 implies that $\Omega_k \subset \mathbb{Q}_p(\gamma_k)$); thus γ_k and $\zeta_{p^k} - 1$ are both generators of the maximal ideal of Ω_k such that $\zeta_{p^k} - 1 \equiv \gamma_k \ [\gamma_k^2]$.

2. The splitting functions of level l. When proving the rationality of zeta functions of varieties over finite fields, one of the main ideas of Dwork was that of a *splitting function*, i.e. power series over $\mathbb{C}_p$ "representing" additive characters over finite fields. The aim of this section is to extend this concept to the rings R and R_m. In fact, via Witt vectors, any element of these rings can be represented as an l-tuple of elements of their residue fields k and k_m; our strategy is to use coordinatewise Teichmüller lifting of these vectors and the results of Section 1 (in particular Remark 1.8) to construct power series of l variables representing characters of R and R_m.

In 2.1, we recall some facts about rings of Witt vectors, then in 2.2, we give the link between the rings R and R_m and rings of Witt vectors with coordinates in the fields k and k_m. Finally, in 2.3, we give a precise definition of the *splitting functions of level l* and give an example of such a function.

2.1. *Some background on rings of Witt vectors.* We recall here the definitions and some properties of rings of Witt vectors; the reader can find more details in [10] or [3].

The *Witt polynomials* $\Phi_0, \ldots, \Phi_n, \ldots$ are defined in $\mathbb{Z}[(X_i)_{i\in\mathbb{N}}]$ by:

$$\Phi_0(X_0) = X_0, \ \ldots, \ \Phi_n(X_0, \ldots, X_n) = X_0^{p^n} + pX_1^{p^{n-1}} + \cdots + p^n X_n, \ \ldots$$

There exists two families of elements $(S_i)_{i\in\mathbb{N}}$, $(P_i)_{i\in\mathbb{N}}$ in $\mathbb{Z}[(X_i, Y_i)_{i\in\mathbb{N}}]$ such that, for all $n \geq 0$,

$$\Phi_n(X_0, \ldots, X_n) + \Phi_n(Y_0, \ldots, Y_n) = \Phi_n(S_0, \ldots, S_n),$$
$$\Phi_n(X_0, \ldots, X_n)\Phi_n(Y_0, \ldots, Y_n) = \Phi_n(P_0, \ldots, P_n).$$

Note that if we assign the weight p^j to the variables X_j, Y_j, then S_i is isobarous of weight p^i, and P_i is isobarous of weight $2p^i$.

We are now ready to define rings of Witt vectors.

Definition 2.1. Let A be a (commutative) ring. The *ring of Witt vectors of length l, with coefficients in A*, $W_l(A)$, is the set A^l, with addition $\oplus$ and multiplication $\otimes$ defined by

$$(a_0, \ldots, a_{l-1}) \oplus (b_0, \ldots, b_{l-1}) := (S_0(a_0, b_0), \ldots, S_{l-1}(a_0, \ldots, b_{l-1})),$$
$$(a_0, \ldots, a_{l-1}) \otimes (b_0, \ldots, b_{l-1}) := (P_0(a_0, b_0), \ldots, P_{l-1}(a_0, \ldots, b_{l-1})).$$

Note that for $0 \leq i \leq l-1$, the map Φ_i from $W_l(A)$ to A is a ring homomorphism; the image of a vector in $W_l(A)$ by Φ_i is often called its *ith ghost component.*

As usual,

$$V : W_l(A) \to W_l(A), \qquad V(a_0, \ldots, a_{l-1}) = (0, a_0, \ldots, a_{l-2}),$$

denotes the *Verschiebung*; it is a group endomorphism (for the additive structure of $W_l(A)$), but not a ring endomorphism. Note that for any vector $(a_0, \ldots, a_{l-1})$ in $W_l(A)$, we have the equality of Witt vectors

$$(a_0, \ldots, a_{l-1}) = \bigoplus_{i=0}^{l-1} V^i(a_i, 0, \ldots, 0).$$

Finally, if $\phi : A \to B$ is a ring homomorphism, then $W_l(\phi)$, the map from $W_l(A)$ to $W_l(B)$ sending $(a_0, \ldots, a_{l-1})$ to $(\phi(a_0), \ldots, \phi(a_{l-1}))$, is again a ring homomorphism. In particular, if A is a ring of characteristic p, the Frobenius of A, sending an element to its pth power, induces a homomorphism of $W_l(A)$, sending $(a_0, \dots, a_{l-1})$ to $(a_0^p, \dots, a_{l-1}^p)$. We shall denote this morphism by F, and call it the *Frobenius of* $W_l(A)$.

2.2. *The ring* $\mathbb{Z}/p^l\mathbb{Z}$ *and its unramified extensions.* In this section, we recall results about the ring $\mathbb{Z}/p^l\mathbb{Z}$ and its unramified extensions; the proofs and more details can be found in [9]. The image of $\mathcal{T}_m$ under reduction modulo p^l is a subset of R_m, which is the image of a section τ of reduction modulo p from R_m to k_m; moreover, every element b in R_m can be written in a unique way as $b_0 + \dots + p^{l-1}b_{l-1}$, with $b_0, \dots, b_{l-1}$ in the image of $\mathcal{T}_m$.

The Galois group of the extension R_m/R is cyclic of order m, generated by the Frobenius F sending $b = b_0 + \dots + p^{l-1}b_{l-1}$ to $F(b) = b_0^p + \dots + p^{l-1}b_{l-1}^p$. We also define a *trace from* R_m *to* R by

$$\mathrm{Tr}_{R_m/R}(b) = b + F(b) + \dots + F^{m-1}(b).$$

With the help of the trace, we can describe the additive characters of the rings R_m, $m \geq 1$. Let ψ_l be a primitive additive character of R, i.e. sending the class of 1 to a primitive p^lth root of unity; then every character of R_m can be written as $y \mapsto \psi_l(\mathrm{Tr}_{R_m/R}(xy))$ for some x in R_m.

For any $m \geq 1$, we fix an isomorphism $w_m : W_l(k_m) \to R_m$ defined by:

$$w_m(a_0, \dots, a_{l-1}) = \tau(a_0) + pF^{-1}\tau(a_1) + \dots + p^{l-1}F^{-(l-1)}\tau(a_{l-1}).$$

Note that via w_m, the Frobenius F on R_m corresponds to the Frobenius F of $W_l(k_m)$ defined in 2.1. Moreover the trace from R_m to R corresponds to the trace from $W_l(k_m)$ to $W_l(k)$ defined by

$$\mathrm{Tr}_{W_l(k_m)/W_l(k)}(a_0, \dots, a_{l-1}) = \bigoplus_{i=0}^{m-1} F^i(a_0, \dots, a_{l-1}) = \bigoplus_{i=0}^{m-1} (a_0^{p^i}, \dots, a_{l-1}^{p^i}).$$

2.3. *The splitting functions.* Recall the concept of a splitting function, as introduced by Dwork (cf. [4]). A *splitting function* Θ is a power series in one variable over Ω_1 that converges in a disk of radius strictly greater than 1 and has the following two properties:

(i) For x in k, denote by $\widetilde{x} \in \mathcal{T}$ its *Teichmüller representative*, the unique element of $\mathcal{T}$ that reduces to x modulo p. Then the function $x \mapsto \Theta(\widetilde{x})$ is a nontrivial additive character ψ of k, with values in Ω_1.

(ii) For each $m \geq 1$, the additive character ψ_m of k_m obtained by composing ψ with the trace from k_m to k can be represented as follows: for x in k_m, denote by $\widetilde{x} \in \mathcal{T}_m$ its Teichmüller representative; then we have

$$\psi_m(x) = \prod_{i=0}^{m-1} \Theta(\widetilde{x}^{p^i}).$$

We shall generalize this concept in order to represent additive characters of order p^l, i.e. additive characters of the rings R_m. We first need to give an equivalent of the Teichmüller lifting. For this we will use Witt vectors. From the isomorphisms w_m, we can define an equivalent of the Teichmüller representative and generalize the notion of splitting function.

Let $x \in R_m$ whose image under w_m^{-1} is $(x_0, \dots, x_{l-1})$. We define the *lift* of x as $\widehat{x} := (\widetilde{x}_0, \dots, \widetilde{x}_{l-1})$, the element of $\mathcal{T}_m^l \subset \mathbb{C}_p^l$ obtained by replacing each component of the Witt vector corresponding to x by its Teichmüller representative. We also define, for any $i \geq 0$,

$$F^i \widehat{x} = (\widetilde{x}_0^{p^i}, \dots, \widetilde{x}_{l-1}^{p^i});$$

note that it is the lift of $F^i x$.

We are now ready to define the splitting functions of level l:

Definition 2.2. A *splitting function of level l, Θ_l*, is a power series in l variables over Ω_l that converges in an open subset of $\mathbb{C}_p^l$ of the form $D(0, r_1) \times \dots \times D(0, r_l)$, with $r_1, \dots, r_l > 1$, and has the following two properties:

(i) The function from R to $\mathbb{C}_p$ defined by $x \mapsto \Theta_l(\widehat{x})$ is an additive character ψ_l of order p^l of R, with values in Ω_l.

(ii) For each $m \geq 1$, the additive character $\psi_{l,m}$ of R_m obtained by composing ψ_l with the trace from R_m to R can be represented as

$$\psi_{l,m}(x) = \prod_{i=0}^{m-1} \Theta_l(F^i \widehat{x}).$$

The aim of this section is to construct a splitting function of level l from the functions θ_i of Section 1. Let

$$\Theta_l : \prod_{i=1}^{l} D(0, p^{(p^{i-1}(p-1))^{-1}}) \to \mathbb{C}_p,$$
$$(X_0, \dots, X_{l-1}) \mapsto \theta_l(X_0) \cdots \theta_1(X_{l-1}).$$

Then we have

Theorem 2.3. *The function Θ_l is a splitting function of level l.*

We show this theorem in several steps. Remark first that Θ_l is a power series in l variables over Ω_l that converges in a suitable open subset of $\mathbb{C}_p^l$ by Proposition 1.5. It remains to show properties (i) and (ii). We begin with an equality of formal power series relating the series F and polynomials arising from addition of Witt vectors; this equality will be the cornerstone of the proof of the theorem.

Lemma 2.4. (i) *We have the following equality of formal power series in* $\mathbb{Z}_p[[X,Y]]$:

$$\mathrm{AH}(X)\mathrm{AH}(Y) = \prod_{k\geq 0} \mathrm{AH}(T_k(X,Y)),$$

where, for any $k \geq 0$, T_k *is a homogeneous polynomial of degree* p^k *in* $\mathbb{Z}[X,Y]$.

(ii) *Let* $x_0,\dots,x_{l-1},y_0,\dots,y_{l-1} \in k_m$, *and let* $\widetilde{x}_0,\dots,\widetilde{y}_{l-1} \in \mathcal{T}_m$ *be their Teichmüller representatives. If we let*

$$(z_0,\dots,z_{l-1}) = (x_0,\dots,x_{l-1}) \oplus (y_0,\dots,y_{l-1})$$

in $W_l(k_m)$, *we have the following congruence in* $\mathbb{C}_p$:

$$\Theta_l(\widetilde{x}_0,\dots,\widetilde{x}_{l-1})\Theta_l(\widetilde{y}_0,\dots,\widetilde{y}_{l-1}) \equiv \Theta_l(\widetilde{z}_0,\dots,\widetilde{z}_{l-1})\ [p\gamma_l].$$

Proof. (i) Let $T_k(X,Y) := S_k(X,0,\dots,0,Y,0,\dots,0)$. Since S_k is isobarous of weight p^k, we see that T_k is homogeneous of degree p^k. Consider, for any $l \geq 0$, the following equality of Witt vectors in $W_{l+1}(\mathbb{Z}_p[[X,Y]])$:

$$\begin{aligned}(X,\dots,X)\oplus(Y,\dots,Y) &= \bigoplus_{k=0}^{l}(V^k(X,0,\dots,0)\oplus V^k(Y,0,\dots,0))\\ &= \bigoplus_{k=0}^{l} V^k(T_0(X,Y),\dots,T_l(X,Y)) = \bigoplus_{k=0}^{l}\bigoplus_{i=0}^{l} V^{k+i}(T_i(X,Y),0,\dots,0)\\ &= \bigoplus_{i=0}^{l} V^i\Big(\bigoplus_{k=0}^{l} V^k(T_i(X,Y),0,\dots,0)\Big) = \bigoplus_{i=0}^{l} V^i(T_i(X,Y),\dots,T_i(X,Y)).\end{aligned}$$

Now the image under Φ_l of the vector $V^i(T_i(X,Y),\dots,T_i(X,Y))$ in $W_{l+1}(\mathbb{Q}_p[[X,Y]])$ is

$$p^iT_i(X,Y)^{p^{l-i}} + \dots + p^lT_i(X,Y) = p^l\sum_{j=0}^{l-i}\frac{T_i(X,Y)^{p^j}}{p^j}.$$

Thus, taking the images under Φ_l (the lth ghost components) of both sides of the above equality of Witt vectors, and dividing by p^l, we obtain the following congruence in $\mathbb{Q}_p[[X,Y]]$:

$$G(X)+G(Y) \equiv G(T_0(X,Y)) + \dots + G(T_l(X,Y)) \bmod (X,Y)^{p^{l+1}}.$$

Finally, letting l grow to infinity, we get in $\mathbb{Q}_p[[X,Y]]$:

$$G(X)+G(Y) = \sum_{k\geq 0} G(T_k(X,Y)).$$

Applying exp to this last equality gives the desired result.

(ii) We show the congruence by induction on l. First note that the equality of formal power series above is valid whenever the two sides converge, that is, for any $x, y \in \mathbb{C}_p$ with $|x|, |y| < 1$. Let us show the case $l = 1$. If x, y are in k_m, we have

$$\varTheta_1(\widetilde{x})\varTheta_1(\widetilde{y}) = \theta_1(\widetilde{x})\theta_1(\widetilde{y}) = \mathrm{AH}(\gamma_1\widetilde{x})\mathrm{AH}(\gamma_1\widetilde{y}) = \prod_{k\geq 0} \mathrm{AH}(T_k(\gamma_1\widetilde{x}, \gamma_1\widetilde{y})).$$

Now it is well known that $T_0(X, Y) = S_0(X, Y) = X + Y$, and we get

$$\mathrm{AH}(T_0(\gamma_1\widetilde{x}, \gamma_1\widetilde{y})) = \mathrm{AH}(\gamma_1(\widetilde{x} + \widetilde{y})) \equiv \mathrm{AH}(\gamma_1(\widetilde{x+y})) = \varTheta_1(\widetilde{x+y}) \ [p\gamma_1],$$

since $\widetilde{x} + \widetilde{y} \equiv \widetilde{x+y}$ $[p]$, and the coefficients of the series AH are in $\mathbb{Z}_p$. On the other hand, if $k \geq 1$, since T_k is homogeneous of degree p^k, we have

$$\mathrm{AH}(T_k(\gamma_1\widetilde{x}, \gamma_1\widetilde{y})) = \mathrm{AH}(\gamma_1^{p^k} T_k(\widetilde{x}, \widetilde{y})) \equiv 1 \ [p\gamma_1],$$

since $v_p(\gamma_1^{p^k}) = p^k/(p-1) \geq 1 + 1/(p-1)$, that is, $\gamma_1^{p^k} \equiv 0$ $[p\gamma_1]$, and $\mathrm{AH}(X) \in 1 + X\mathbb{Z}_p[[X]]$. Thus we have $\varTheta_1(\widetilde{x})\varTheta_1(\widetilde{y}) \equiv \varTheta_1(\widetilde{x+y})$ $[p\gamma_1]$, and since both sides of the congruence are pth roots of unity, this proves the case $l = 1$ with the help of Corollary 1.2.

Assume we have shown the result for $l - 1$. Then

$$\begin{aligned}&\varTheta_l(\widetilde{x}_0, \ldots, \widetilde{x}_{l-1})\varTheta_l(\widetilde{y}_0, \ldots, \widetilde{y}_{l-1}) \\ &\qquad = \theta_l(\widetilde{x}_0)\varTheta_{l-1}(\widetilde{x}_1, \ldots, \widetilde{x}_{l-1})\theta_l(\widetilde{y}_0)\varTheta_{l-1}(\widetilde{y}_1, \ldots, \widetilde{y}_{l-1}).\end{aligned}$$

From the equality in (i), and since T_k is homogeneous of degree p^k, we have

$$\theta_l(\widetilde{x}_0)\theta_l(\widetilde{y}_0) = \mathrm{AH}(\gamma_l\widetilde{x}_0)\mathrm{AH}(\gamma_l\widetilde{y}_0) = \prod_{k\geq 0} \mathrm{AH}(\gamma_l^{p^k} T_k(\widetilde{x}_0, \widetilde{y}_0)),$$

and we obtain as above the following congruences (note that from Lemma 1.3, we have $\gamma_l^{p^i} \equiv \gamma_{l-i}$ $[p\gamma_l]$):

$$\begin{aligned}\mathrm{AH}(\gamma_l^{p^i} T_i(\widetilde{x}_0, \widetilde{y}_0)) &\equiv \mathrm{AH}(\gamma_{l-i}\widetilde{\overline{T}_i(x_0, y_0)}) \\ &= \theta_{l-i}(\widetilde{\overline{T}_i(x_0, y_0)}) \ [p\gamma_l] \quad \text{for } i \leq l-1,\end{aligned}$$

where $\overline{T}_i$ stands for the reduction modulo p of T_i, and

$$\mathrm{AH}(\gamma_l^{p^i} T_i(\widetilde{x}_0, \widetilde{y}_0)) \equiv \mathrm{AH}(0) = 1 \ [p\gamma_l] \quad \text{for } i \geq l.$$

Consequently, we obtain

$$\begin{aligned}\theta_l(\widetilde{x}_0)\theta_l(\widetilde{y}_0) &\equiv \theta_l(\widetilde{x_0 + y_0})\theta_{l-1}(\widetilde{\overline{T}_1(x_0, y_0)}) \cdots \theta_1(\widetilde{\overline{T}_{l-1}(x_0, y_0)}) \ [p\gamma_l] \\ &\equiv \theta_l(\widetilde{x_0 + y_0})\varTheta_{l-1}(\widetilde{\overline{T}_1(x_0, y_0)}, \ldots, \widetilde{\overline{T}_{l-1}(x_0, y_0)}) \ [p\gamma_l].\end{aligned}$$

Now the result comes from the induction hypothesis, the following equality in $W_{l-1}(k_m)$:

$$(z_1,\dots,z_{l-1}) = (\overline{T}_1(x_0,y_0),\dots,\overline{T}_{l-1}(x_0,y_0))\oplus(x_1,\dots,x_{l-1})\oplus(y_1,\dots,y_{l-1}),$$

and the fact that $z_0 = x_0 + y_0$.

We are now ready to prove Theorem 2.3.

Proof of Theorem 2.3. Property (i): From Remark 1.8, and since for $x \in R$ we have $\widehat{x} \in \mathcal{T}^l$, it is clear that $\Theta_l(\widehat{x}) = \Theta_l(\widetilde{x}_0,\dots,\widetilde{x}_{l-1})$ is a p^lth root of unity. Moreover, $\Theta_l(\widehat{1}) = \Theta_l(1,0,\dots,0) = \theta_l(1) = \zeta_{p^l}$ is a primitive p^lth root of unity. On the other hand, from Lemma 2.4(ii), for $x, y \in R$ we have

$$\begin{aligned}\Theta_l(\widehat{x})\Theta_l(\widehat{y}) &= \Theta_l(\widetilde{x}_0,\dots,\widetilde{x}_{l-1})\Theta_l(\widetilde{y}_0,\dots,\widetilde{y}_{l-1})\\ &\equiv \Theta_l(\widetilde{z}_0,\dots,\widetilde{z}_{l-1})\ [p\gamma_l] \equiv \Theta_l(\widehat{x+y})\ [p\gamma_l].\end{aligned}$$

Now since both sides are p^lth roots of unity, Corollary 1.2 ensures that the above congruence is in fact an equality. Summing up, we have shown that the map $x \mapsto \Theta_l(\widehat{x})$ is an additive character of order p^l of R, say ψ_l.

Property (ii): We first show that for $(t_0,\dots,t_{l-1})$ in $\mathcal{T}_m^l$, the product $\prod_{i=0}^{m-1}\Theta_l(t_0^{p^i},\dots,t_{l-1}^{p^i})$ is a p^lth root of unity. Actually it is sufficient to show that $\theta_l(t_0)\theta_l(t_0^p)\cdots\theta_l(t_0^{p^{m-1}})$ is a p^lth root of unity for any l. Since $t_0^{p^m} = t_0$, we have

$$\begin{aligned}(\theta_l(t_0)\theta_l(t_0^p)\cdots\theta_l(t_0^{p^{m-1}}))^{p^l} &= \prod_{i=0}^{m-1}\exp\left(p^l\left(\gamma_l t_0^{p^i} + \cdots + \frac{(\gamma_l t_0^{p^i})^{p^l}}{p^l} + \cdots\right)\right)\\ &= \exp((p^l\gamma_l + \cdots + \gamma_l^{p^l} + \cdots)(t_0 + \cdots + t_0^{p^{m-1}})).\end{aligned}$$

Note that we can write these equalities since all the terms occurring are in the convergence disk of the exponential (cf. proof of Proposition 1.7); since γ_l is a zero of G, the last term is 1, and we are done.

From Lemma 2.4(ii), for any $x_0,\dots,x_{l-1} \in k_m$ we have

$$\prod_{i=0}^{m-1}\Theta_l(\widetilde{x}_0^{p^i},\dots,\widetilde{x}_{l-1}^{p^i}) \equiv \Theta_l(\widetilde{y}_0,\dots,\widetilde{y}_{l-1})\ [p\gamma_l],$$

where we have set, in $W_l(k_m)$,

$$(y_0,\dots,y_{l-1}) = \bigoplus_{i=0}^{m-1}(x_0^{p^i},\dots,x_{l-1}^{p^i}) = \mathrm{Tr}_{W_l(k_m)/W_l(k)}(x_0,\dots,x_{l-1}).$$

Thus the y_i are actually in k, and both sides of the congruence are p^lth roots of unity; once more, Corollary 1.2 shows that the congruence is an equality; finally we get, for any $x \in R_m$,

$$\begin{aligned}\prod_{i=0}^{m-1} \Theta_l(F^i\widehat{x}) = \prod_{i=0}^{m-1} \Theta_l(\widetilde{x}_0^{p^i}, \ldots, \widetilde{x}_{l-1}^{p^i}) &= \Theta_l(\widetilde{y}_0, \ldots, \widetilde{y}_{l-1}) \\ &= \psi_l \circ w_m(y_0, \ldots, y_{l-1}) \\ &= \psi_l \circ w_m(\mathrm{Tr}_{W_l(k_m)/W_l(k)}(x_0, \ldots, x_{l-1})) \\ &= \psi_l(\mathrm{Tr}_{R_m/R}(x)) = \psi_{l,m}(x),\end{aligned}$$

and this ends the proof of Theorem 2.3.

3. A Stickelberger theorem for p-adic Gauss sums. Let ζ_{p^l} be as above, and $\widetilde{\psi}_{l,m} = \widetilde{\psi}_l \circ \mathrm{Tr}_{K_m/\mathbb{Q}_p}$ be an additive character of order p^l of $\mathcal{O}_m^{(u)}$, where $\widetilde{\psi}_l$ is the additive character of $\mathbb{Z}_p$ sending 1 to ζ_{p^l}. Let ζ be a primitive (p^m-1)th root of unity, i.e. a generator of $\mathcal{T}_m^\times := \mathcal{T}_m \setminus \{0\}$, and χ be the multiplicative character from $\mathcal{T}_m^\times$ to $\mathbb{C}_p^\times$, of order p^m-1, sending ζ to ζ. For any integer $0 \le a \le p^m-2$ we define the following Gauss sums:

$$G_{\mathcal{T}_m}(\chi^{-a}, \widetilde{\psi}_{l,m}) = \sum_{x \in \mathcal{T}_m^*} \chi^{-a}(x)\widetilde{\psi}_{l,m}(x).$$

Note that for $l=1$ these sums coincide with classical Gauss sums over finite fields. They are the same sums as in [8], where they are called *incomplete Gauss sums.*

These sums lie in the ring of integers $\mathcal{O}_{l,m}$ of $K_{l,m}$, the compositum of Ω_l and K_m. Notice that γ_l is a generator of the maximal ideal of $\mathcal{O}_{l,m}$. Our aim is to show

THEOREM 3.1. *Let a be an integer such that $0 \le a \le p^m-2$, and $a = a_0 + pa_1 + \cdots + p^{m-1}a_{m-1}$ be its p-adic expansion $(0 \le a_i \le p-1)$. Set $s(a) := a_0 + a_1 + \cdots + a_{m-1}$ and $p(a) := a_0! \cdots a_{m-1}!$. Then we have the following congruence in $\mathcal{O}_{l,m}$:*

$$G_{\mathcal{T}_m}(\chi^{-a}, \widetilde{\psi}_{l,m}) \equiv -\frac{\gamma_l^{s(a)}}{p(a)}\ [\gamma_l^{s(a)+1}].$$

REMARK 3.2. Note that by the Remark 1.8(ii) we can replace γ_l by $\zeta_{p^l}-1$ in the preceding congruence.

Proof of Theorem 3.1. We first rewrite the Gauss sum. The character $\widetilde{\psi}_{l,m}$ factors to the character $\psi_{l,m} : \mathcal{O}_m^{(u)}/p^l\mathcal{O}_m^{(u)} = R_m \to \mathbb{C}_p^*$, obtained by composing $\psi_l : R \to \mathbb{C}_p$, the character sending 1 to ζ_{p^l}, with the trace from R_m to R. Since an element x of $\mathcal{T}_m$ is sent via w_m^{-1} to the element $(\overline{x}, 0, \ldots, 0)$ of $W_l(k_m)$, we get

$$\widetilde{\psi}_{l,m}(x) = \Theta_l(x, 0, \ldots, 0) \cdots \Theta_l(x^{p^{m-1}}, 0, \ldots, 0) = \theta_l(x) \cdots \theta_l(x^{p^{m-1}});$$

thus we can write, in $\mathbb{C}_p$ (actually in $\mathcal{O}_{l,m}$),

$$\begin{aligned} G_{\mathcal{T}_m}(\chi^{-a},\widetilde{\psi}_{l,m}) &= \sum_{x\in\mathcal{T}_m^*} x^{-a_0-pa_1-\cdots-p^{m-1}a_{m-1}}\theta_l(x)\cdots\theta_l(x^{p^{m-1}}) \\ &= \sum_{x\in\mathcal{T}_m^*}\Big(\sum_{n\geq 0}\lambda_{n,l}x^{n-a_0}\Big)\cdots\Big(\sum_{n\geq 0}\lambda_{n,l}(x^{p^{m-1}})^{n-a_{m-1}}\Big) \\ &= \sum_{n_0,\dots,n_{m-1}\geq 0}\lambda_{n_0,l}\cdots\lambda_{n_{m-1},l}\sum_{x\in\mathcal{T}_m^*}x^{n_0-a_0+\cdots+p^{m-1}(n_{m-1}-a_{m-1})} \\ &= \sum_{n_0,\dots,n_{m-1}\geq 0}\lambda_{n_0,l}\cdots\lambda_{n_{m-1},l}\sum_{x\in\mathcal{T}_m^*}x^{n_0+\cdots+p^{m-1}n_{m-1}-a} \\ &= (p^m-1)\sum_{\substack{n_0,\dots,n_{m-1}\geq 0\\ n_0+\cdots+p^{m-1}n_{m-1}\equiv a\ [p^m-1]}}\lambda_{n_0,l}\cdots\lambda_{n_{m-1},l} \end{aligned}$$

(notice that the sum $\sum_{x\in\mathcal{T}_m^*}x^n$ is p^m-1 if $n\equiv 0\ [p^m-1]$ and zero otherwise). Now $v_p(\lambda_{n_0,l}\cdots\lambda_{n_{m-1},l})\geq (n_0+\cdots+n_{m-1})/(p^{l-1}(p-1))$, and

$$\lambda_{a_0,l}\cdots\lambda_{a_{m-1},l}=\frac{\gamma_l^{s(a)}}{p(a)}$$

by the description of the coefficients $\lambda_{n,l}$ for $n\leq p-1$ in Proposition 1.5; thus the theorem comes from the following lemma.

LEMMA 3.3. *Let $0\leq a\leq p^m-2$ and $n_0,\dots,n_{m-1}$ be $m+1$ nonnegative integers such that*

$$n_0+\cdots+p^{m-1}n_{m-1}\equiv a\ [p^m-1].$$

If $a=a_0+pa_1+\cdots+p^{m-1}a_{m-1}$ is the p-adic expansion of the integer a, then

$$n_0+\cdots+n_{m-1}\geq s(a)=a_0+\cdots+a_{m-1},$$

and equality occurs if and only if $n_0=a_0,\dots,n_{m-1}=a_{m-1}$.

Proof. Set $n_0+\cdots+p^{m-1}n_{m-1}=a_0+pa_1+\cdots+p^{m-1}a_{m-1}+k(p^m-1)$. We must have $k\geq 0$ since $0\leq a\leq p^m-2$. We rewrite this as

$$\begin{aligned} &n_0+\cdots+p^{m-1}n_{m-1} \\ &\quad= a_0+k(p-1)+p(a_1+k(p-1))+\cdots+p^{m-1}(a_{m-1}+k(p-1)). \end{aligned}$$

Reducing this last equality modulo p, we get $n_0\equiv a_0-k\ [p]$, and there exists an integer k_1 such that $n_0=a_0-k+k_1p$. Moreover k_1 is a nonnegative integer since $0\leq a_0\leq p-1$, and $k,n_0\geq 0$. We can rewrite the first equality of this proof as

$$p(n_1+k_1)+\cdots+p^{m-1}n_{m-1}=p(a_1+kp)+\cdots+p^{m-1}(a_{m-1}+k(p^m-1)).$$

Dividing both sides by p and reducing modulo p yields $n_1 + k_1 = a_1 + pk_2$ with k_2 an integer, nonnegative since $k_1 \geq 0$ and $0 \leq a_1 \leq p - 1$. We can repeat this process to get nonnegative integers $k_3, \ldots, k_{m-1}$ such that $n_i + k_i = a_i + pk_{i+1}$ for $1 \leq i \leq m - 2$, and $n_{m-1} + k_{m-1} = a_{m-1} + kp$. Summing all these equalities, we get

$$n_0 + \cdots + n_{m-1} + k_1 + \cdots + k_{m-1} = a_0 - k + k_1 p + a_1 + k_2 p + \cdots + a_{m-1} + kp,$$

$$n_0 + \cdots + n_{m-1} = a_0 + a_1 + \cdots + a_{m-1} + (k + k_1 + \cdots + k_{m-1})(p - 1).$$

Since k and the k_i are nonnegative integers, this last equality proves the lemma.

Remark. Note that for $l = 1$, we obtain the classical Stickelberger theorem (cf. [2], [7]).

References

[1] Y. Amice, *Les nombres p-adiques*, Presses Univ. France, Paris, 1975.

[2] B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi Sums*, Wiley, New York, 1998.

[3] N. Bourbaki, *Algèbre Commutative IX*, Hermann, Paris, 1962.

[4] B. M. Dwork, *On the zeta function of an hypersurface*, Inst. Hautes Études Sci. Publ. Math. 12 (1962), 5–68.

[5] N. Koblitz, *p-adic Numbers, p-adic Analysis and Zeta-Functions*, Grad. Texts in Math. 58, Springer, New York, 1977.

[6] P. V. Kumar, T. Helleseth and A. R. Calderbank, *An upper bound for Weil exponential sums over Galois rings and applications*, IEEE Trans. Inform. Theory 41 (1995), 456–468.

[7] S. Lang, *Algebraic Number Theory*, Grad. Texts in Math. 110, Springer, 1994.

[8] P. Langevin and P. Solé, *Gauss sums over quasi-Frobenius rings*, in: Finite Fields and Applications, Springer, 2001, 329–340.

[9] B. R. MacDonald, *Finite Rings with Identity*, Dekker, 1974.

[10] J.-P. Serre, *Corps locaux*, Hermann, Paris, 1963.

[11] A. G. Shanbag, P. V. Kumar and T. Helleseth, *An upper bound for a hybrid sum over Galois rings with applications to aperiodic correlation for some q-ary sequences*, IEEE Trans. Inform. Theory 42 (1996), 250–254.

Équipe "Algèbre Arithmétique et Applications"
Université Antilles Guyane
Campus de Fouillole
97159 Pointe à Pitre Cedex - FWI
E-mail: rblache@univ-ag.fr

Received on 5.1.2004
and in revised form on 15.9.2004 (4689)