Invent. math. 94, 105–112 (1988)

Inventiones mathematicae

Gauss sums for $\mathbf{F}_q[T]$

Dinesh S. Thakur*
School of Mathematics, The Institute for Advanced Study, Princeton, NJ 08540, USA

The purpose of this paper is to define 'Gauss sums' taking values in function fields of one variable over a finite field and to prove analogues of various classical and recent results. These results include Stickelberger's theorem, the Hasse-Davenport theorem, Weil's theorem on 'Jacobi sums as Hecke characters' and the Gross-Koblitz theorem. For comparison, the reader may consult [G-K] and references given there.

In this paper we deal only with the simplest case, where the base ring A is the polynomial ring $\mathbf{F}_q[T]$ and where we use the Carlitz module; i.e., the simplest rank one Drinfeld module. (See section I). The general case, which has a quite different flavour, will be presented elsewhere. These results formed a part of the author's thesis, 'Gamma functions and Gauss sums for function fields and periods of Drinfeld modules' (Harvard 1987). But the new presentation here is due to a suggestion by Professor Tate. It is my pleasure to thank him.

I. Carlitz' theory

Let us briefly recall the relevant portions of Carlitz' theory (see [Ca2] or [Ha]). Let $\mathbf{F}_q$ be a finite field of characteristic p. Put $A=\mathbf{F}_q[T]$ and $K=\mathbf{F}_q(T)$. Let $\bar{K}$ be an algebraic closure of K. ($\bar{K}$ will be our universe). Let $\bar{K}^+$ be its underlying additive group and $\mathrm{End}(\bar{K}^+)$ be its ring of endomorphisms. Let C (the Carlitz module) be the homomorphism $C\colon A\to\mathrm{End}(\bar{K}^+)\,(a\mapsto C_a)$ determined by $C_T(u)=Tu+u^q$ and $C_\theta(u)=\theta u$ for $\theta\in\mathbf{F}_q$ and $u\in\bar{K}$. For $a\in A$, put $\Lambda_a=\{u\in\bar{K}: C_a(u)=0\}$. Then Λ_a is an A-module under C.

Let $\wp$ be a monic irreducible polynomial of degree $h>0$ in A.

Theorem 0 (Carlitz-Hayes): (1) *$C_\wp(u)/u$ is an Eisenstein polynomial at $\wp$ and as A-modules, $\Lambda_\wp$ is (non-canonically) isomorphic to $A/\wp$.*

(2) *$K(\Lambda_\wp)$ is a Galois extension of K with Galois group $(A/\wp)^*$, under the natural action on the $\wp$-division points.*

* Supported in part by NSF grant DMS 8610730C2

(3) *The extension $K(\Lambda_\wp)$ over K is unramified at all finite places except $\wp$, and is totally ramified at $\wp$. At the infinite place, the inertia group = the decomposition group = $\mathbf{F}_q^* = A^* \hookrightarrow (A/\wp)^*$.*

These results should be compared with the cyclotomic theory over $\mathbf{Q}$, where for p a prime in $\mathbf{Z}$, the $\mathbf{Z}$-module μ_p of p-th roots of unity, is an analogue of $\Lambda_\wp$. The Gauss sums introduced in the next section arise when one combines Carlitz' cyclotomic theory and the usual cyclotomic theory obtained by adjoining roots of unity to K.

II. Gauss sums

Classically, a Gauss sum is defined to be

$$-\sum_{x\in\mathbf{F}_{p^m}^*} \chi(x)\,\psi(\operatorname{Tr} x),$$

where χ is a non-trivial multiplicative character $\chi\colon \mathbf{F}_{p^m}^* \to \mathbf{C}^*$, ψ is a non-trivial additive character $\psi\colon \mathbf{F}_p \to \mathbf{C}^*$ and Tr is the trace from $\mathbf{F}_{p^m}$ to $\mathbf{F}_p$.

Our key idea in making Gauss sums for function fields is to view ψ rather as an isomorphism of $\mathbf{Z}$-modules, $\psi\colon \mathbf{Z}/p \to \mu_p$ and to replace it by an isomorphism of A-modules, $\psi\colon A/\wp \to \Lambda_\wp$. Also we restrict the class of multiplicative characters. The reason for this restriction will be apparent in the remark following proposition I.

Let k be a finite field of 'characteristic $\wp$', i.e., a finite extension of $A/\wp$. Let ϕ be a $\mathbf{F}_q$-algebra homomorphism, $\phi\colon k \to L$, where L is a field containing $K(\Lambda_\wp)$. Then a basic Gauss sum is just

$$g(\phi) = -\sum_{x\in k^*} \phi(x^{-1})\,\psi(\operatorname{Tr} x) \tag{1}$$

where the trace is from k to $A/\wp$.

Lemma I. *If h is a function on $\mathbf{F}_{q^f}$ with values in a ring containing $\mathbf{F}_{q^f}$ and with $h(0)=0$, then*

$$\sum_{x\in\mathbf{F}_{q^f}^*} x^{-q^j} h(\operatorname{Tr} x) = \sum_{y\in\mathbf{F}_q^*} y^{-q^j} h(y).$$

Proof. The result will follow if we establish the equality $\sum_{\operatorname{Tr} x = y} x^{-q^j} = y^{-q^j}$.

To see this equality, put $a_{j,f} = \sum x^{-q^j}$, for $y=1$. Then

$$\sum_{\operatorname{Tr} x=y} x^{-q^j} = y^{-q^j} \sum_{\operatorname{Tr} x=1} x^{-q^j} = y^{-q^j} a_{j,f}$$

$$-1 = \sum x^{-q^j}(\operatorname{Tr} x) = \sum_y{}' \sum_{\operatorname{Tr} x=y} x^{-q^j} y$$

$$= a_{j,f} \sum{}' y^{1-q^j} = -a_{j,f}$$

implies that $a_{j,f}=1$. This proves the lemma.

In other words, there are h basic Gauss sums, say $g_j (j \bmod h)$, with $\phi = \chi_j$ being $\mathbf{F}_q$-homomorphisms $A/\wp \to L$, indexed so that $\chi_j^q = \chi_{j+1} (j \bmod h)$. Then we have $g_j = -\sum_{z \in (A/\wp)^*} \chi_j(z^{-1}) \psi(z)$.

In fact, Professor Tate observed that the Fourier expansion of $\psi(z)$ in terms of all characters of $(A/\wp)^*$ is just given by

Proposition I.

$$\psi(z) = \sum g_j \chi_j(z) \tag{2}$$

Proof. The coefficient of $\chi(z)$ is zero for $\chi \neq \chi_j$, because of $\mathbf{F}_q$-linearity of ψ and is g_j for $\chi = \chi_j$, by Fourier inversion. This establishes the result. (This should be compared with the classical situation $\psi(z) = \sum g_\chi \chi(z)$ with the obvious notation.)

Remark. Notice that the proposition shows that $g(\phi)$ defined by (1), is zero, unless the multiplicative character ϕ is restricted as in the definition of the basic Gauss sums.

Clearly g_j belongs to $K(\mu_{q^h-1})(\Lambda_\wp)$. Let L be this compositum of the extensions $K(\mu_{q^h-1})$ and $K(\Lambda_\wp)$ of K, which are linearly disjoint by simple ramification considerations. Hence, the Galois group of L over K is canonically isomorphic to the product of the Galois groups of these extensions over K. So the powers of Frobenius (q-th power) σ for the extension $K(\mu_{q^h-1})$ over K and elements $\mu \in (A/\wp)^* = \mathrm{Gal}(K(\Lambda_\wp)/K)$ can be thought of as elements of $\mathrm{Gal}(L/K)$. We will denote the image of $l \in L$ under g in the $\mathrm{Gal}(L/K)$ as l^g.

Theorem I. (1) $g_j^\sigma = g_{j+1} (j \bmod h)$.
(2) $g_j^\mu = \chi_j(\mu) g_j$.
(3) $g_j \neq 0$, *for all* j.

Proof. (1) follows from $\chi_j^q = \chi_{j+1}$ and (2) follows by straightforward manipulation involving change of variable. Since ψ is non-zero, we find that some g_j is also non-zero. Then (3) follows from (1) and the result is established.

Set $\wp_j = T - \chi_{1-j}(T) (j \bmod h)$. These are monic representatives of primes above $\wp$ in $\mathbf{F}_{q^h}[T]$. Observe that χ_{1-j} is then the Teichmüller character of $\wp_j$ and $\wp_j^\sigma = \wp_{j-1}$.

Theorem II.

$$\prod_{j \bmod h} g_j^{q-1} = (-1)^h \wp.$$

In particular, g_j *lie above* $\wp$.

Proof. Since $\psi(Tz) = T\psi(z) + \psi(z)^q$, we have $g_j \chi_j(T) = g_j T + g_{j-1}^q$. As $g_j \neq 0$, we get

$$g_{j-1}^q / g_j = -(T - \chi_j(T)) = -\wp_{1-j} (j \bmod h) \tag{3}$$

Multiplying all these equations together, we get the theorem.

Let $\bar{\wp}_j$ be the unique prime above $\wp_j$ in the integral closure of A in L. Put $\bar{\wp}=\bar{\wp}_1$.

I am grateful to Professor Tate for the proof of the next result.

Lemma II. *There exists a unique $\lambda \in K_{\wp}(\psi(1)) \subset L_{\bar{\wp}}$ such that $\lambda^{\mathbf{N}\wp-1}=-\wp$ and $\lambda \equiv \psi(1) \bmod \psi(1)^2$.*

Proof. Uniqueness is obvious. By theorem 0, $C_{\wp}(u)/u$ is an Eisenstein polynomial $u^{\mathbf{N}\wp-1}+\ldots+\wp$, so its root $\psi(1)$ generates totally tamely ramified abelian extension of $K_{\wp}$ of degree $\mathbf{N}\wp-1$, but any $\mathbf{N}\wp-1$-th root λ also generates such an extension. By local class field theory such extensions are obtained by adjoining $\mathbf{N}\wp-1$-th root of prime elements, so we have $K_{\wp}(\psi(1))=K_{\wp}((-\tilde{\wp})^{1/(\mathbf{N}\wp-1)})$ for some prime element $\tilde{\wp}$. Now, from the equations satiesfied by these generating elements, we see that $\wp$ and $\tilde{\wp}$ are norms from this extension. Thus their ratio is a one-unit and hence $\mathbf{N}\wp-1$-th power. So the extension is the same as $K_{\wp}(\lambda)$. This proves the lemma.

Theorem III (Analogue of Stickelberger's theorem). $g_j/\lambda^{q^j} \equiv \dfrac{1}{d_j} \bmod \bar{\wp}$ *for* $0 \leqq j < h$, *where* $d_0=1$, $d_j=-\wp_{1-j}\, d_{j-1}^q$.

Proof. By lemma II,

$$\psi(\mathrm{Tr}(x))=C_{\mathrm{Tr}(x)}(\psi(1)) \equiv \mathrm{Tr}(x)\,\psi(1) \equiv \mathrm{Tr}(x)\,\lambda \bmod \psi(1)^2$$

As $\chi_0(y) \equiv y \bmod \bar{\wp}$, it follows that,

$$g_0 \equiv -\lambda \sum \chi_0(x^{-1})\,\mathrm{Tr}(x) \equiv \lambda \bmod \bar{\wp}^2, \tag{4}$$

Theorem then immediately follows from (3) and (4).

Theorem IV. (1) $(g_j)=\bar{\wp}_{1-j}\,\bar{\wp}_{2-j}^q \ldots \bar{\wp}_{h-j}^{q^{h-1}}$.

(2) *The valuation (normalised in the usual fashion, so that the valuation of T is -1) of g_j at any infinite place of L is* $-\dfrac{1}{q-1}$.

Proof. (1) follows immediately from theorem III. Raising both sides of (1) to the q^h-1-th power, it is easy to see that (2) follows from the fact (part (3) of theorem 0) that q^h-1-th power of $\bar{\wp}_j$ is $\wp_j=T-\chi_{1-j}(T)$, since $\dfrac{1+q+\ldots+q^{h-1}}{q^h-1}=\dfrac{1}{q-1}$. The result is thus proved.

Observe that part (2) of the theorem is the analogue of the wellknown result on the infinite absolute values of the usual Gauss sums.

III. Analogue of the Gross-Koblitz theorem

Carlitz [Ca1] defined a factorial function for $\mathbf{F}_q[T]$ as follows. Define $[i]$ and D_i for nonnegative integers i, by

$$[i]=T^{q^i}-T, \qquad D_0=1, \qquad D_i=[i]\,D_{i-1}^q.$$

For $z \in \mathbf{N}$, $z = \sum z_i q^i$, $0 \leqq z_i \leqq q-1$, define the factorial function by

$$\Pi(z) = \prod D_i^{z_i} \in \mathbf{F}_p[T].$$

David Goss [Go] made a Morita-style $\wp$-adic factorial $\Pi_\wp$: $\mathbf{Z}_p \to A_\wp$ as follows. By [Ca 1], pa. 514, D_i is the product of all monic elements of degree i in $\mathbf{F}_q[T]$. Let $\tilde{D}_i$ be the product of all monic elements of degree i, which are relatively prime to $\wp$. Goss shows that $-\tilde{D}_i \to 1$, $\wp$-adically, as $i \to \infty$. (In fact the proof also shows that $-\tilde{D}_j \equiv 1 \bmod \wp$, if $j \geqq h$.) Thus we set

$$\Pi_\wp(z) = \prod (-\tilde{D}_i)^{z_i}.$$

It is easily seen that $\Pi_\wp$ is a continuous function.

Put $\Gamma_\wp(z) = \Pi_\wp(z-1)$. (Notice that $\Pi_\wp$ here is denoted by $\Gamma_\wp$ in [Go].)

Theorem V. $\Pi_\wp\left(\frac{q^r}{1-q^h}\right)^{q^h-1} = (-1)^{h-1} \wp_1^{e_r}$ *for* $0 \leqq r \leqq h-1$, *with* $e_r = \sum_{i=0}^{h-1} (q^r - q^i)\, \sigma^{r-i}$ *and* $\Pi_\wp\left(\frac{q^r}{1-q^h}\right) \equiv -D_r \bmod \wp$.

Proof. For $0 \leqq r \leqq h-1$, let

$$M_r = \Pi_\wp\left(\frac{q^r}{1-q^h}\right) = (-\tilde{D}_r)(-\tilde{D}_{r+h})(-\tilde{D}_{r+2h}) \ldots$$

Now $\tilde{D}_a = D_a/(D_{a-h}\, \wp^l)$, where l is such that $\tilde{D}_a$ is unit at $\wp$. Hence

$$\tilde{D}_r \ldots \tilde{D}_{r+mh} = \frac{D_r \ldots D_{r+mh}}{D_r \ldots D_{r+(m-1)h}\, \wp^w} = \frac{D_{r+mh}}{\wp^w}$$

($w = \operatorname{ord}_\wp D_{r+mh}$.) Call the quantity on the preceding line T_{r+mh}. Then $M_r = \lim (-1)^{m+1} T_{r+mh}$. Since $D_i = [i]\, D_{i-1}^q$,

$$T_{r+mh} = [r+mh]\, [r-1+mh]^q \ldots \frac{[mh]^{q^r}}{\wp^{q^r}} \ldots [r+1+(m-1)h]^{q^{h-1}}\, T_{r+(m-1)h}^{q^h},$$

because $[l]$ is the product of all monic primes of degree dividing l, so that $\wp$ divides $[l]$ (and then divides it only to the first power) if and only if h divides l. Now $[l+mh] = T^{q^{mh+l}} - T$. We may assume that $P \neq T$ since we can always make the substitution $T+1$ for T. Let $T = au$ be the decomposition in the completion $K_\wp$, of T, a unit at $\wp$, as product of its 'Teichmüller representative' a and its one unit part u. As $a^{q^{mh}} = a$ and $u^{q^t} \to 1$ as $t \to \infty$, we have, as $m \to \infty$,

$$[l+mh] = ((au)^{q^{mh+l}} - T) \to (a^{q^l} - T).$$

Let $\mathbf{F}_{q^h} = \mathbf{F}_q(a)$. Then we have the inclusion $\mathbf{F}_{q^h}[T] \subset K_\wp$. We may assume that χ_0 is the Teichmüller character. In other words, $\wp_1 = T - a$ and $a^{q^l} - T =$

$-\wp_{1-l}(l \bmod h)$. It follows that $\lim [l+mh] = -\wp_{1-l}$. Passing to the limit as m tends to infinity, in the recursion formula for T_{r+mh} then shows that

$$M_r^{1-q^h} = -\frac{(-\wp_{1-r})(-\wp_{2-r})^q \ldots (-\wp_{-r})^{q^{h-1}}}{\wp^{q^r}}.$$

Also, as we have noted, $-\tilde{D}_j \equiv 1 \bmod \wp$ if $j \geqq h$, so $M_r \equiv -\tilde{D}_r = -D_r \bmod \wp$. Thus the theorem is established.

Corollary. *If N divides $\mathbf{N}\wp - 1$, then $\Gamma_\wp(i/N)$ is algebraic for any integer i.*

Proof. This is an immediate consequence of the theorem and the defintion of $\Pi_\wp$, if $0 \leqq i < q^h - 1$. In particular, $\Gamma_\wp(0)$ is algebraic. Then it is easy to see from the definition of $\Pi_\wp$ that $\Pi_\wp(z+1)/\Pi_\wp(z)$ is algebraic. Induction then establishes the corollary.

Theorem VI (Analogue of the Gross-Koblitz theorem). *For $0 \leqq j < h$,*

$$g_j = -\lambda^{q^j}/\Pi_\wp\left(\frac{q^j}{1-q^h}\right).$$

Proof. Factorizations of both sides given by the theorem V and theorem IV are same and hence they are easily seen to be equal up to a $q^h - 1$-th root of unity. Hence it boils down to prove

$$g_j/\lambda^{q^h} \equiv \frac{-1}{\Pi_\wp(q^j/1-q^h)} \equiv \frac{1}{D_j} \bmod \wp.$$

Now the theorem III shows that the left hand side is congruent to the reciprocal of $(-\wp_{h-j+1})(-\wp_{h-j+2})^q \ldots (-\wp_h)^{q^{j-1}}$. Since T is congruent to a, $-\wp_k$ is congruent to $-a + a^{q^{h-k+1}} \equiv [h-k+1]$ and hence the desired congruence and the theorem follows.

Remark. Minus sign in the theorem is due to different normalizations of signs used in Morita's and Goss' definitions.

IV. Jacobi sums and analogue of the theorem of Weil

Let $F = \mathbf{F}_{q^r}(T)$ and let P be a prime of $\mathbf{F}_{q^r}[T]$ above $\wp$, with relative residue class degree f. Choose a prime $\tilde{P}$ above P in $\mathbf{F}_{q^{hf}}[T]$. We may assume that the prime of $\mathbf{F}_{q^h}[T]$ below $\tilde{P}$ is $\wp_1$. That is to say, we may assume that χ_0 is Teichmüller character for $\tilde{P}$. This fixes g_j's.

For an element of the form

$$\underset{\sim}{a} = \oplus\, m_j \cdot \left(\frac{q^j}{q^r - 1}\right)$$

in the free abelian group with basis $\frac{1}{q^r-1}\mathbf{Z}/\mathbf{Z}$, put

$$g(\underline{a}, P)=\prod_j (g_j g_{j+r} \cdots g_{j+hf-r})^{m_j}.$$

Also, put (for $k \geqq 0$)

$$\underline{a}^{(q^k)}=\oplus\, m_j \cdot \left(\frac{q^{j+k}}{q^r-1}\right)$$

and

$$n(\underline{a})=\sum m_j \left\langle \frac{q^j}{q^r-1} \right\rangle$$

where $\langle x \rangle$ is representative of $x \bmod \mathbf{Z}$ such that $0 \leqq \langle x \rangle < 1$.

Remark. Let $j \geqq 0$. Then the basic sum g_j is just $g(\langle q^j/(q^{hf}-1)\rangle, \tilde{P})$ and since

$$\frac{q^j}{q^r-1}=\frac{q^j+q^{j+r}+\ldots+q^{j+hf-r}}{q^{hf}-1}$$

we see that $g(\langle q^j/(q^r-1)\rangle, P)=g_j g_{j+r} \cdots g_{j+hf-r}$. This, of course, is the intention of the defintion.

It is easy to see that (use obvious modifications of σ, μ actions).

Theorem VII. (1) *$g(\underline{a}, P)$ is independent of the choice of $\tilde{P}$.*

(2) *$g(\underline{a}, P)$ belongs to $F(\Lambda_\wp)$.*

(3) *If $n(\underline{a})$ is an integer, then the 'Jacobi sum' $g(\underline{a}, P)$ belongs to F.*

(4) *$g(\underline{a}, P)$ depends on the choice of ψ only up to multiplication by q^h-1-th root of unity, and is independent of ψ if $n(\underline{a})$ is an integer.*

(5) *$g(\underline{a}^{(q^h)}, P)=g(\underline{a}, P)$.*

Theorem VIII (Analogue of the Hasse-Davenport theorem). *If P' is a prime (in $\mathbf{F}_{q^{rt}}[T]$ for some t) of relative residue class degree s over P, then*

$$g(\underline{a}, P')=g(\underline{a}, P)^s.$$

Proof. It is easy to see that this follows from lemma I, (5) of theorem VII and

$$\frac{q^j}{q^h-1}=q^j(1+q^h+\ldots+q^{h(s-1)})/(q^{hs}-1).$$

Remark. In contrast with the classical situation, the 'Jacobi sum $g(\underline{a}, P)$' (i.e., when $n(\underline{a})$ is an integer) is not a character sum built out of multiplicative characters; since the multiplicative characters take values in a finite field. Nonetheless, we have

Theorem IX. *If $n(\underline{a})$ is an integer, then the Jacobi sums $g(\underline{a}, P)$ extended multiplicatively to a function on ideals, give an algebraic Hecke character χ of F of conductor 1 with the algebraic part $\theta=\sum n(\underline{a}^{(q^j)})\,\sigma^{-j}$ where the sum runs over j in the*

Galois group $\mathbf{Z}/(r)$. *More precisely, for principal ideal* (α) *of* $\mathbf{F}_{q^r}[T]$, α *monic, we have* $\chi((\alpha))=\alpha^\theta b^{\deg\alpha}$, *where*

$$b=(-1)^s \qquad s=\sum_{i=0}^{r-1} n(\underline{a}^{(q^i)}).$$

Proof. (3) shows that $g_j=\eta_{1-j}\eta_{2-j}^q\dots\eta_{hf-j}^{q^{hf-1}}$ for some choice $\eta_i=(-\wp_i)^{1/(q^{hf}-1)}$. Put

$$\beta_i=(\eta_i\,\eta_{i+r}\dots\eta_{i+hf-r})^{(q^{hf}-1)/(q^r-1)}(i \bmod r).$$

Then

$$g\left(\frac{q^j}{q^r-1}, P\right)=\beta_{1-j}\beta_{2-j}^q\dots\beta_{r-j}^{q^{r-1}}.$$

The hypothesis implies that there are integers t_i (i from 0 to $r-1$) such that $\sum t_i q^i=n(\underline{a})(q^r-1)$ and

$$\begin{aligned}\chi((\wp))&=\prod g\left(\frac{q^j}{q^f-1}, P\right)^{t_j}\\ &=(\beta_1\beta_2^q\dots\beta_r^{q^{r-1}})^{t_0}(\beta_r\dots)^{t_1}\dots(\beta_2\dots\beta_1^{q^{r-1}})^{t_{r-1}}\\ &=\beta_1^{n(\underline{a})(q^r-1)}\beta_2^{n(\underline{a}^{(q)})(q^r-1)}\dots\\ &=(-1)^{hf(n(\underline{a})+\dots+n(\underline{a}^{(q^{r-1})}))/r}\wp_1^{n(\underline{a})}\dots\wp_r^{n(\underline{a}^{(q^{r-1})})}.\end{aligned}$$

This proves the theorem.

References

[Ca 1] Carlitz, L.: An analogue of the von Staudt-Clausen theorem. Duke Math. J. **3**, 503–517 (1937)

[Ca 2] Carlitz, L.: A class of polynomials. Trans. Am. Math. Soc. **43**, 167–182 (1938)

[Go] Goss, D.: Modular forms for $\mathbf{F}_r[T]$. J. Reine Angew. Math. **317**, 16–39 (1980)

[G-K] Gross, B.H., Koblitz, N.: Gauss sums and the p-adic Γ-function. Ann. Math. **109**, 569–581 (1979)

[Ha] Hayes, D.: Explicit class field theory for rational function fields. Trans. Am. Math. Soc. **189**, 77–91 (1974)

Oblatum 26-I-1988 & 15-III-1988