By (52) and (53)

$$\mathscr{I}(s_1) = \varepsilon_1 c \sum_a \chi(a)\left(\frac{Na}{D}\right)^{-s_1} \psi\left(s_1, \frac{Na}{D}\right).$$

Hence, by (50),

$$(56)\quad \frac{1}{2}\varepsilon_1 \xi(s_1, \chi) = \operatorname{re}\mathscr{I}(s_1) = \frac{1}{2}\{\mathscr{I}(s_1) + \overline{\mathscr{I}(s_1)}\}$$
$$= \frac{\varepsilon_1 c}{2} D^{s_1} \sum_a \frac{\chi(a)}{Na^{s_1}} \psi\left(s_1, \frac{Na}{D}\right) + \frac{\bar{\varepsilon}_1 c}{2} D^{1-s_1} \sum_a \frac{\bar{\chi}(a)}{Na^{1-s_1}} \overline{\psi\left(s_1, \frac{Na}{D}\right)}.$$

Now we use (51) and divide (56) through by $\frac{1}{2}c\varepsilon_1 D^{s_1} G(s_1)$. Using (55) (with $y = Na/D$, $E = y^{1/2}$) and considering that $1/G(s_1) \ll 1$ (since $t_1 \ll 1$) we can prove that the remainders of the infinite series with $Na > X_1$ are in modulus $\ll l^{-1}$. Thus we get (48) with

$$c_a = \psi\left(s_1, \frac{Na}{D}\right)\Big/ G(s_1), \qquad c_a' = \overline{\psi\left(s_1, \frac{Na}{D}\right)}\Big/ G(s_1)$$

which are $\ll 1$, by (54), (55).

References

[1] E. Bombieri, *On the large sieve*, Mathematika 12 (1965), pp. 201–225.
[2] E. Fogels, *On the zeros of Hecke's L-functions I*, Acta Arith. 7 (1962), pp. 87–106.
[3] — *On the abstract theory of primes III*, ibid. 11 (1966), pp. 293–331.
[4] — *Большое решето*, Latvijas PSR Zinātņu Akad. Vēstis 4 (1969), pp. 1–12.
[5] E. Landau, *Einführung in die elementare und analytische Theorie der algebraischen Zahlen und der Ideale*, Leipzig und Berlin 1927.
[6] — *Über Ideale und Primideale in Idealklassen*, Math. Zeitschr. 2 (1918), pp. 52–154.
[7] — *Vorlesungen über Zahlentheorie III*, Leipzig 1927.
[8] Лаврик, *Функциональное уравнение для L-функций Дирихле и задача делителей в арифметических прогрессиях*, Известия АН СССР, сер. мат. 30 (1966), pp. 433–448.
[9] — *Приближенное функциональное уравнение дзета-функции Гекке мнимого квадратичного поля*, Мат. заметки 2 (1965), pp. 475–482.
[10] Ю. В. Линник, *Все большие числа-суммы простого и двух квадратов (О проблеме Гарди–Литтлвуда) II*, Мат. Сборник 53 (95), (1961), pp. 3–38.
[11] K. Prachar, *Primzahlverteilung*, Berlin 1957.
[12] E. C. Titchmarsh, *The theory of functions*, Oxford 1932.
[13] — *The theory of Riemann zeta-function*, Oxford 1951.
[14] G. N. Watson, *A treatise on the theory of Bessel functions*, Cambridge 1944.

Reçu par la Rédaction le 7. 2. 1969

ACTA ARITHMETICA
XVI (1969)

Kloosterman sums and finite field extensions*

by

L. Carlitz (Durham, North Carolina)

1. Introduction. Let $q = p^f$, where p is prime and $f \geqslant 1$. Put $F = \mathrm{GF}(q)$, the finite field of order q. For arbitrary $a \in F$ define

$$t(a) = a + a^p + \ldots + a^{p^{f-1}},$$

so that $a \in \mathrm{GF}(p)$. Put

$$e(a) = e^{2\pi i t(a)/p}.$$

We now define the Kloosterman sum for F:

$$(1.1)\qquad S(a) = \sum_{\substack{x \in F \\ x \neq 0}} e(ax + x'),$$

where $xx' = 1$. It is easily seen that $S(a)$ is real for all $a \in F$.

In addition to F we consider also the finite field $F_n = \mathrm{GF}(q^n)$ of order q^n, where $n \geqslant 1$ and define the Kloosterman sum for F_n. We denote this sum by $S^{(n)}(a)$, where a is an arbitrary element of F_n. Clearly $S^{(1)}(a) = S(a)$.

It follows at once from the definition that

$$S^{(n)}(0) = -1 \qquad (n = 1, 2, 3, \ldots).$$

We may accordingly assume that $a \neq 0$. For arbitrary $a \in F$ we investigate the relationship of $S^{(n)}(a)$ to $S(a)$. We shall show that

$$(1.2)\qquad \sum_{n=1}^{\infty} \frac{1}{nq^{ns}} S^{(n)}(a) = \log\{1 + q^{-s}S(a) + q^{1-2s}\} \qquad (s > 1).$$

By means of (1.2) we can express $S^{(n)}(a)$ explicitly in terms of $S(a)$. In particular we show that

$$(1.3)\qquad S^{(n)}(a) = (-1)^{n-1} 2^{1-n} \sum_{2r \leqslant n} \binom{n}{2r} \{S(a)\}^{n-2r} \{\{S(a)\}^2 - 4q\}^r$$

* Supported in part by NSF grant GP-7855.

and

$$S^{(n)}(a) = -\sum_{2t\leqslant n}(-1)^{n-t}\frac{n}{n-t}\binom{n-t}{t}q^t\big(S(a)\big)^{n-2t}. \tag{1.4}$$

Another simple explicit formula is

$$S^{(n)}(a) = -(\alpha^n+\beta^n), \tag{1.5}$$

where α, β are the roots of

$$z^2+S(a)z+q = 0.$$

If we assume that

$$|S(a)| \leqslant 2q^{1/2} \tag{1.6}$$

for some q and some $a\in F$, then it follows from (1.5) that

$$|S^{(n)}(a)| \leqslant 2q^{n/2} \qquad (n = 1, 2, 3, \ldots) \tag{1.7}$$

for the fixed a. It is indeed known [1], [7] that (1.6) holds generally but the proof depends on the Riemann hypothesis for a function field. The proof of (1.7), on the other hand, is elementary.

In the final sections of the paper we evaluate $S(a)$ for small values of q and verify that (1.6) holds in all cases considered. It then follows, for example when $q = 2$, that

$$S^{(n_k)}(1) = o(2^{n_k/2})$$

for some infinite sequence $\{n_k\}$ and that

$$S^{(n'_k)}(1) \sim 2\cdot 2^{n'_k/2}$$

sor some infinite sequence $\{n'_k\}$. This result is proved in several other fpecial cases and it seems plausible that for any q and any $a\in\mathrm{GF}(q)$,

$$S^{(n_k)}(a) = o(q^{n_k/2})$$

for some infinite sequence n_k and that

$$S^{(n'_k)}(a) \sim 2\cdot q^{n'_k/2}$$

for some infinite sequence $\{n'_k\}$.

For $p > 2$ let $a_1, a_2, \ldots, a_{2t}$ denote nonzero numbers of F and $a, \lambda_1, \ldots, \lambda_{2t}$ denote arbitrary numbers of F. Put

$$T = \sum e(2\lambda_1\xi_1+\ldots+2\lambda_{2t}\xi_{2t}),$$

where the summation is over all $\xi_1, \ldots, \xi_{2t}\in F$ such that

$$a_1\xi_1^2+\ldots+a_{2t}\xi_{2t}^2 = a. \tag{1.8}$$

Then (see [3]) we have

$$T = q^{t-1}\psi\big((-1)^t\delta\big)S(a\omega), \tag{1.9}$$

where not all $\lambda_j = 0$, $\psi\big((-1)^t\delta\big)$ is the quadratic character,

$$\delta = a_1a_2\ldots a_{2t}, \qquad \omega = \frac{\lambda_1^2}{a_1}+\ldots+\frac{\lambda_{2t}^2}{a_{2t}} \neq 0.$$

(The corresponding weighted sum T when the number of squares is odd is evaluated explicitly.) Thus by (1.9) our results for $S^{(n)}(a)$ can be restated in terms of the weighted sum

$$T^{(n)} = \sum e(2\lambda_1\xi_1+\ldots+2\lambda_{2t}\xi_{2t}),$$

where now the summation is over all $\xi_1, \ldots, \xi_{2t}\in F_n$ that satisfy (1.8).

We remark that the recent work of the Lehmers [4], [5] on Kloosterman sums is in a different direction.

2. Preliminaries. As above we put

$$t(a) = a+a^p+\ldots+a^{p^{f-1}} \tag{2.1}$$

and

$$e(a) = e^{2\pi it(a)/p} \tag{2.2}$$

for arbitrary $a\in F$. It follows at once from (2.1) that

$$t(a+b) = t(a)+t(b), \qquad t(ka) = kt(a) \qquad (k\in\mathrm{GF}(p)),$$

so that

$$e(a+b) = e(a)e(b), \qquad e(ka) = \big(e(a)\big)^k \qquad (k\in\mathrm{GF}(p)). \tag{2.3}$$

It is also evident that

$$t(a) = t(a^p), \qquad e(a) = e(a^p). \tag{2.4}$$

We shall make frequent use of the familiar formula

$$\sum_{b\in F} e(ab) = \begin{cases} q & (a = 0),\\ 0 & (a\neq 0).\end{cases} \tag{2.5}$$

In particular it follows from (2.5) that

$$S(0) = -1, \tag{2.6}$$

where $S(a)$ is defined by (1.1). Also it is evident from (2.4) that

$$S(a^p) = \sum_{\substack{x\in F\\ x\neq 0}} e(a^px+x') = \sum_{\substack{x\in F\\ x\neq 0}} e(a^px^p+x'^p) = \sum_{\substack{x\in F\\ x\neq 0}} e(ax+x'),$$

so that

$$S(a^p) = S(a) \quad (a \in F).$$

Hence

$$S(a) = S(a^p) = \ldots = S(a^{p^{l-1}}). \tag{2.7}$$

The definition of $S^{(n)}(a)$, the Kloosterman sum for $F_n = \mathrm{GF}(q^n)$ is of course included in (1.1). However for the application it will be necessary to introduce some additional notation. For $a \in F_n$ we put

$$S^{(n)}(a) = \sum_{\substack{\xi \in F_n \\ \xi \neq 0}} e_n(a\xi + \xi'), \tag{2.8}$$

where $e_n(\xi)$ is defined by

$$e_n(\xi) = e\big(\tau_n(\xi)\big) \tag{2.9}$$

and

$$\tau_n(\xi) = \xi + \xi^q + \ldots + \xi^{q^{n-1}}. \tag{2.10}$$

Note that $\tau_n(\xi) \in F$, so that $e_n(\xi)$ is well-defined. We note also that by (2.10)

$$\tau_n(\xi + \eta) = \tau_n(\xi) + \tau_n(\eta) \quad (\xi, \eta \in F_n), \tag{2.11}$$

$$\tau_n(a\xi) = a\tau_n(\xi) \quad (a \in F, \ \xi \in F_n). \tag{2.12}$$

Hence by (2.8), (2.9), (2.11) and (2.12), we have

$$S^{(n)}(a) = \sum_{\substack{\xi \in F_n \\ \xi \neq 0}} e\big(a\tau_n(\xi) + \tau_n(\xi')\big) \quad (a \in F). \tag{2.13}$$

This may be rewritten in the form

$$S^{(n)}(a) = \sum_{u, v \in F} e(au + v) h_n(u, v), \tag{2.14}$$

where

$$h_n(u, v) = \sum_{\substack{\xi \in F_n, \xi \neq 0 \\ \tau_n(\xi) = u, \tau_n(\xi') = v}} 1. \tag{2.15}$$

3. Characters. In order to evaluate $h_n(u, v)$ we consider the distribution of monic irreducible polynomials in $F[x]$ subject to certain restrictions.

Let A be a monic polynomial in $F[x]$ with non-vanishing constant term:

$$A = x^m + a_1 x^{m-1} + \ldots + a_m \quad (a_j \in F, \ a_m \neq 0). \tag{3.1}$$

The set of such polynomials will be denoted by Φ; clearly Φ is closed under multiplication. Next define $\lambda_{j,k}(1) = 1$ and, for $m \geqslant 1$,

$$\lambda_{j,k}(A) = e(ja_1 + ka_{m-1}a'_m) \quad (j, k \in F), \tag{3.2}$$

where $a_m a'_m = 1$. It is easily verified that

$$\lambda_{j,k}(AB) = \lambda_{j,k}(A)\lambda_{j,k}(B), \tag{3.3}$$

where A, B are arbitrary polynomials in Φ.

In particular it follows from (3.2) that

$$\lambda_{j,k}(x + a) = e(ja + ka') \tag{3.4}$$

and

$$\lambda_{j,k}(x^2 + ax + b) = e(ja + kab'). \tag{3.5}$$

Also by (3.2)

$$\sum_{\substack{A \in \Phi \\ \deg A = m}} \lambda_{j,k}(A) = \sum_{\substack{a_1, \ldots, a_m \in F \\ a_m \neq 0}} e(ja_1 + ka_{m-1}a'_m)$$

and therefore by (2.5)

$$\sum_{\substack{A \in \Phi \\ \deg A = m}} \lambda_{j,k}(A) = 0 \quad (m \geqslant 3), \tag{3.6}$$

provided j, k do not vanish simultaneously.

By (3.5) we have

$$\sum_{\substack{A \in \Phi \\ \deg A = 2}} \lambda_{j,0}(A) = 0 \quad (j \neq 0), \tag{3.7}$$

$$\sum_{\substack{A \in \Phi \\ \deg A = 2}} \lambda_{0,k}(A) = 0 \quad (k \neq 0). \tag{3.8}$$

If neither j nor k is equal to 0, we have

$$\sum_{\substack{A \in \Phi \\ \deg A = 2}} \lambda_{j,k}(A) = \sum_{\substack{a, b \in F \\ b \neq 0}} e(ja + kab') = \sum_{b \neq 0} \sum_{a} e\big((j + kb')a\big).$$

By (2.5) the inner sum vanishes unless $j + kb' = 0$; hence for fixed $j, k \neq 0$ there is just one such value of b and therefore

$$\sum_{\substack{A \in \Phi \\ \deg A = 2}} \lambda_{j,k}(A) = q \quad (jk \neq 0). \tag{3.9}$$

For $m = 1$ it is evident that

$$\sum_{\substack{A \in \Phi \\ \deg A = 1}} \lambda_{j,0}(A) = \sum_{a \neq 0} e(ja) = -1 \quad (j \neq 0), \tag{3.10}$$

and

$$\sum_{\substack{A\in\Phi\\ \deg A=1}} \lambda_{0,k}(A) = \sum_{a\neq 0} e(ka') = -1 \qquad (k\neq 0). \tag{3.11}$$

If neither j nor $k=0$ we get

$$\sum_{\substack{A\in\Phi\\ \deg A=1}} \lambda_{j,k}(A) = \sum_{a\neq 0} e(ja+ka') = S(jk). \tag{3.12}$$

If we put

$$\sigma_m(j,k) = \sum_{\substack{A\in\Phi\\ \deg A=m}} \lambda_{j,k}(A) \qquad (j,k\in F) \tag{3.13}$$

then

$$\sigma_0(j,k) = 1 \qquad (j,k\in F). \tag{3.14}$$

By (3.6), (3.7), (3.8), (3.9), (3.10), (3.11), (3.12) we have

$$\sigma_m(j,k) = 0 \qquad (m\geqslant 3;\ j,k \text{ not both } =0), \tag{3.15}$$

$$\sigma_2(j,0) = \sigma_2(0,k) = 0 \qquad (j\neq 0,\ k\neq 0), \tag{3.16}$$

$$\sigma_2(j,k) = q \qquad (jk\neq 0), \tag{3.17}$$

$$\sigma_1(j,0) = \sigma_1(0,k) = -1 \qquad (j\neq 0,\ k\neq 0), \tag{3.18}$$

$$\sigma_1(j,k) = S(jk) \qquad (jk\neq 0). \tag{3.19}$$

If both $j,k=0$ it is evident from (3.2) that

$$\sigma_m(0,0) = (q-1)q^{m-1} \qquad (m\geqslant 1). \tag{3.20}$$

We now define

$$L_{j,k}(s) = \sum_{A\in\Phi} \frac{\lambda_{j,k}(A)}{|A|^s} \qquad (s>1), \tag{3.21}$$

where

$$|A| = q^m \qquad (m=\deg A).$$

In view of (3.13) we have

$$L_{j,k}(s) = \sum_{m=0}^{\infty} q^{-ms}\sigma_m(j,k). \tag{3.22}$$

Therefore, by (3.15), (3.16), (3.17), (3.18), (3.19) we have

$$L_{j,0}(s) = 1-q^{-s} \qquad (j\neq 0), \tag{3.23}$$

$$L_{0,k}(s) = 1-q^{-s} \qquad (k\neq 0), \tag{3.24}$$

$$L_{j,k}(s) = 1+q^{-s}S(jk)+q^{1-2s} \qquad (jk\neq 0). \tag{3.25}$$

As for $L_{0,0}(s)$, it follows at once from (3.20) that

$$L_{0,0}(s) = (1-q^{-s})(1-q^{1-s})^{-1}. \tag{3.26}$$

4. The main result. It follows from (3.3) and (3.21) that

$$L_{j,k}(s) = \prod_{P\in\Phi}\left\{1-\frac{\lambda_{j,k}(P)}{|P|^s}\right\}^{-1} \tag{4.1}$$

where the product is over all monic irreducibles in Φ. The only irreducible in $F[x]$ that is excluded is $P=x$, so that (4.1) may be replaced by

$$L_{j,k}(s) = \prod_{P\neq x}\left\{1-\frac{\lambda_{j,k}(P)}{|P|^s}\right\}^{-1}. \tag{4.2}$$

Taking logarithms (4.2) becomes

$$\log L_{j,k}(s) = \sum_{P\neq x}\sum_{t=1}^{\infty}\frac{1}{t}\cdot\frac{\lambda_{j,k}(P^t)}{|P|^{ts}} \tag{4.3}$$

$$= \sum_{m=1}^{\infty}\frac{1}{m}q^{-ms}\sum_{rt=m} r \sum_{\deg P=r}\lambda_{j,k}(P^t),$$

where it is understood, on the extreme right, that $P=x$ is excluded.

Let P denote a monic irreducible of degree r, so that

$$P(x) = (x-\xi)(x-\xi^q)\dots(x-\xi^{q^{r-1}}), \tag{4.4}$$

where ξ is a primitive number of $\mathrm{GF}(q^m)$, that is,

$$\xi\in\mathrm{GF}(q^m), \qquad \xi\notin\mathrm{GF}(q^t) \qquad (1\leqslant t<m).$$

If we put

$$P(x) = x^r+a_1x^{r-1}+\dots+a_r \qquad (a_j\in F,\ a_r\neq 0)$$

then clearly

$$\begin{aligned} -a_1 &= \xi+\xi^q+\dots+\xi^{q^{r-1}},\\ -a_{r-1}a_r' &= \xi'+\xi'^q+\dots+\xi'^{q^{r-1}}, \end{aligned} \tag{4.5}$$

where $\xi\xi'=1$. Since

$$P^t(x) = x^{tr}+ta_1x^{r-1}+\dots+ta_{r-1}a_r^{t-1}x+a_r^t,$$

it follows from (2.10) and (4.5) that

$$\tau_{tr}(\xi) = -ta_1, \qquad \tau_{tr}(\xi') = -ta_{r-1}a_r'. \tag{4.6}$$

Put $n=tr$. Then by (2.9) and (4.6)

$$e_n(\xi) = e\big(\tau_n(\xi)\big) = e(-ta_1), \qquad e_n(\xi') = e\big(\tau_n(\xi')\big) = e(-ta_{r-1}a_r'),$$

so that by (3.2)

$$\lambda_{j,k}(P^i) = e(-jta_1 - kta_{r-1}a'_r) = e\big(j\tau_n(\xi)+k\tau_n(\xi')\big). \tag{4.7}$$

To each irreducible P of degree r it is clear from (4.4) that there correspond r values of ξ, namely

$$\xi,\ \xi^q,\ \ldots,\ \xi^{q^{r-1}}.$$

Hence

$$\sum_{ri=n} r \sum_{\deg P=r} \lambda_{j,k}(P^i) = \sum_{b,c\in F} e(jb+kc) \sum_{\substack{\xi\in F_n,\ \xi\neq 0\\ \tau_n(\xi)=b,\ \tau_n(\xi')=c}} 1 = \sum_{b,c\in F} e(jb+kc)h_n(b,c),$$

by (2.15). Thus (4.3) becomes

$$\log L_{j,k}(s) = \sum_{n=1}^{\infty} \frac{1}{n} q^{-ns} \sum_{b,c\in F} e(jb+kc)h_n(b,c). \tag{4.8}$$

For arbitrary $u, v \in F$ we have by (4.8)

$$\sum_{j,k\in F} e(-ju-kv)\log L_{j,k}(s)$$

$$= \sum_{n=1}^{\infty} \frac{1}{n} q^{-ns} \sum_{j,k\in F} e(-ju-kv) \sum_{b,c\in F} e(jb+kc)h_n(b,c)$$

$$= \sum_{n=1}^{\infty} \frac{1}{n} q^{-ns} \sum_{b,c\in F} h_n(b,c) \sum_{j,k\in F} e\big(j(b-u)+k(c-v)\big).$$

Since

$$\sum_{j,k\in F} e\big(j(b-u)+k(c-v)\big) = \begin{cases} q^2 & (b=u,\ c=v),\\ 0 & (\text{otherwise}), \end{cases} \tag{4.9}$$

it follows that

$$\sum_{j,k\in F} e(-ju-kv)\log L_{j,k}(s) = q^2 \sum_{n=1}^{\infty} \frac{1}{n} q^{-ns} h_n(u,v), \tag{4.10}$$

where u, v are arbitrary elements of F.

We now return to (2.14). It is clear from (2.14) that

$$\sum_{n=1}^{\infty} \frac{1}{n} q^{-ns} S^{(n)}(a) = \sum_{u,v\in F} e(au+v) \sum_{n=1}^{\infty} \frac{1}{n} q^{-ns} h_n(u,v).$$

Combining this with (4.10) we get

$$q^2 \sum_{n=1}^{\infty} \frac{1}{n} q^{-ns} S^{(n)}(a) = \sum_{u,v\in F} e(au+v) \sum_{j,k\in F} e(-ju-kv)\log L_{j,k}(s)$$

$$= \sum_{j,k\in F} \log L_{j,k}(s) \sum_{u,v\in F} e\big((a-j)u+(1-k)v\big).$$

Again applying (4.9), it follows at once that

$$\sum_{n=1}^{\infty} \frac{1}{n} q^{-ns} S^{(n)}(a) = \log L_{a,1}(s). \tag{4.11}$$

Therefore, by (3.25), we have our principal result:

THEOREM 1. *If $S(a)$ denotes the Kloosterman sum for $F = \mathrm{GF}(q)$ and $S^{(n)}(a)$ the corresponding sum for $F_n = \mathrm{GF}(q^n)$, then for $a \in F$,*

$$\sum_{n=1}^{\infty} \frac{1}{n} q^{-ns} S^{(n)}(a) = \log\{1+q^{-s}S(a)+q^{1-2s}\} \qquad (s>1). \tag{4.12}$$

5. Explicit formulas. Clearly by means of (4.12), $S^{(n)}(a)$ is expressed in terms of $S(a)$ where a is an arbitrary element of F. We shall now obtain explicit formulas for $S^{(n)}(a)$.

It is convenient to put

$$1+S(a)z+qz^2 = (1-\alpha z)(1-\beta z), \tag{5.1}$$

where

$$\alpha+\beta = -S(a), \qquad \alpha\beta = q. \tag{5.2}$$

Thus α, β are roots of

$$x^2+S(a)x+q = 0, \tag{5.3}$$

so that

$$\alpha, \beta = \tfrac{1}{2}\big\{-S(a) \pm \big[(S(a))^2-4q\big]^{1/2}\big\}. \tag{5.4}$$

Now by (5.1)

$$\log\{1+S(a)z+qz^2\} = \log(1-\alpha z)(1-\beta z) = -\sum_{n=1}^{\infty} \frac{1}{n}(\alpha^n+\beta^n)z^n.$$

Comparing this with (4.12) we get

$$S^{(n)}(a) = -(\alpha^n+\beta^n) \tag{5.5}$$

and therefore

$$S^{(n)}(a) = -2^{-n}\Big\{\Big[-S(a)+\big((S(a))^2-4q\big)^{1/2}\Big]^n + \Big[-S(a)-\big((S(a))^2-4q\big)^{1/2}\Big]^n\Big\}. \tag{5.6}$$

Also it is clear from (5.3) and (5.4) that $S^{(n)}(a)$ satisfies the recurrence

$$S^{(n+2)}(a)+S(a)S^{(n+1)}(a)+qS^{(n)}(a)=0 \quad (n\geqslant 0) \tag{5.7}$$

provided we put

$$S^{(0)}(a)=-2.$$

In the next place, by (5.1),

$$\frac{2+S(a)z}{1+S(a)z+qz^2}=\frac{1}{1-\alpha z}+\frac{1}{1-\beta z}=\sum_{n=0}^{\infty}(\alpha^n+\beta^n)z^n.$$

But since

$$\begin{aligned}\frac{2+S(a)z}{1+S(a)z+qz^2}&=\frac{2+S(a)z}{[1+\frac{1}{2}S(a)z]^2-\frac{1}{4}[(S(a))^2-4q]z^2}\\&=2\sum_{r=0}^{\infty}4^{-r}z^{2r}\frac{[(S(a))^2-4q]^r}{[1+\frac{1}{2}S(a)z]^{2r+1}}\\&=2\sum_{r=0}^{\infty}4^{-r}z^{2r}[(S(a))^2-4q]^r\sum_{t=0}^{\infty}(-1)^t\binom{2r+t}{t}(\tfrac{1}{2}S(a)z)^t\\&=2\sum_{n=0}^{\infty}(-1)^n2^{-n}z^n\sum_{2r\leqslant n}\binom{n}{2r}(S(a))^{n-2r}[(S(a))^2-4q]^r;\end{aligned}$$

it follows from (5.5) that

$$S^{(n)}(a)=(-1)^{n-1}2^{1-n}\sum_{2r\leqslant n}\binom{n}{2r}(S(a))^{n-2r}[(S(a))^2-4q]^r. \tag{5.8}$$

Since

$$(S(a))^2-4q=(\alpha-\beta)^2,$$

we may replace (5.8) by

$$S^{(n)}(a)=(-1)^{n-1}2^{1-n}\sum_{2r\leqslant n}\binom{n}{2r}(\alpha-\beta)^{2r}(S(a))^{n-2r}. \tag{5.9}$$

Again, since

$$\frac{1}{\alpha-\beta}\left(\frac{\alpha}{1-\alpha z}-\frac{\beta}{1-\beta z}\right)=\frac{1}{(-\alpha z)(1-\beta z)}=\frac{1}{1+S(a)z+qz^2}$$

and

$$\begin{aligned}\{1+S(a)z+qz^2\}^{-1}&=\sum_{r=0}^{\infty}(-1)^rz^r(S(a)+qz)^r\\&=\sum_{r=0}^{\infty}(-1)^rz^r\sum_{t=0}^{r}\binom{r}{t}(S(a))^{r-t}(qz)^t\\&=\sum_{n=0}^{\infty}z^n\sum_{2t\leqslant n}(-1)^{n-t}\binom{n-t}{t}q^t(S(a))^{n-2t},\end{aligned}$$

it follows that

$$\frac{\alpha^{n+1}-\beta^{n+1}}{\alpha-\beta}=\sum_{2t\leqslant n}(-1)^{n-t}\binom{n-t}{t}q^t(S(a))^{n-2t}.$$

Hence making use of the identity

$$\alpha^n+\beta^n=\frac{\alpha^{n+1}-\beta^{n+1}}{\alpha-\beta}-\alpha\beta\frac{\alpha^{n-1}-\beta^{n-1}}{\alpha-\beta},$$

we get after a little manipulation

$$S^{(n)}(a)=-\sum_{2t\leqslant n}(-1)^{n-t}\frac{n}{n-t}\binom{n-t}{t}q^t(S(a))^{n-2t}. \tag{5.10}$$

By means of (5.10) $S^{(n)}(a)$ is exhibited as a polynomial in $S(a)$ with integral coefficients. For example we have

$$\begin{aligned}S^{(2)}(a)&=-(S(a))^2+2q,\\S^{(3)}(a)&=(S(a))^3-3qS(a),\\S^{(4)}(a)&=-(S(a))^4+4q(S(a))^2-2q^2,\\S^{(5)}(a)&=(S(a))^5-5q(S(a))^3+5q^2S(a).\end{aligned}$$

It is easily verified that these values satisfy the recurrence (5.7).

It is known that ([1], [7])

$$|S(a)|\leqslant 2q^{1/2} \tag{5.11}$$

for all q and all $a\in\mathrm{GF}(q)$. It follows from (5.11) and (5.4) that

$$|\alpha|=|\beta|=q^{1/2}; \tag{5.12}$$

indeed α, β are complex conjugates. If we only assume (5.11) for some fixed q and some fixed $a\in\mathrm{GF}(q)$, (5.12) remains true.

Consequently, by (5.5),

$$|S^{(n)}(a)|\leqslant 2q^{n/2} \tag{5.13}$$

for all n.

This proves

THEOREM 2. *If $S(a)$ satisfies (5.11) for some q and some $a\in\mathrm{GF}(q)$, then $S^{(n)}(a)$ satisfies (5.13) for all n and the same value of a.*

6. Some special cases. It has been remarked in the Introduction that when $q=2^f, f\geqslant 1$, $S(a)$ is an odd integer for all $a\in\mathrm{GF}(q)$. We consider first the case $q=2$, $a=1$. Then we have

$$S(1)=1 \quad (q=2). \tag{6.1}$$

Thus (4.12) becomes

$$\sum_{n=1}^{\infty}\frac{1}{n}2^{-ns}S^{(n)}(1)=\log(1+2^{-s}+2^{1-2s}). \tag{6.2}$$

By (5.4) we now have

$$\alpha,\beta=\tfrac{1}{2}(-1\pm\sqrt{-7}), \tag{6.3}$$

so that

$$|\alpha|=|\beta|=\sqrt{2}. \tag{6.4}$$

Hence we have

$$|S^{(n)}(1)|\leqslant 2\cdot 2^{n/2}\quad(n=1,2,3,\ldots). \tag{6.5}$$

An equivalent statement is that

$$|S(1)|\leqslant 2q^{1/2} \tag{6.6}$$

for $q=2^n$, $n\geqslant 1$. We have therefore proved (5.11) in this special case.

We remark also that $S^{(n)}(1)$ satisfies

$$S^{(n+2)}(1)+S^{(n+1)}(1)+2S^{(n)}(1)=0\quad(n\geqslant 0) \tag{6.7}$$

with $S^{(0)}(1)=-2$. Using the recurrence it is easily verified that

$$\begin{aligned}&S^{(2)}(1)=3,\quad S^{(3)}(1)=-5,\quad S^{(4)}(1)=-1,\\ &S^{(5)}(1)=11,\quad S^{(6)}(1)=-9,\quad S^{(7)}(1)=-13,\\ &S^{(8)}(1)=31,\quad S^{(9)}(1)=-5,\quad S^{(10)}(1)=-57.\end{aligned}$$

The explicit formulas (5.9), (5.10) now become

$$S^{(n)}(1)=(-1)^{n-1}2^{1-n}\sum_{2r\leqslant n}(-1)^r\binom{n}{2r}7^r, \tag{6.8}$$

$$S^{(n)}(1)=-\sum_{2t\leqslant n}(-1)^{n-t}\frac{n}{n-t}\binom{n-t}{t}2^t, \tag{6.9}$$

respectively.

By means of (6.9) we can compute the residue (mod 8) of $S^{(n)}(1)$. Indeed we have, for $n\geqslant 2$,

$$S^{(n)}(1)\equiv(-1)^{n-1}\left\{1-\frac{2n}{n-1}\binom{n-1}{1}+\frac{4n}{n-2}\binom{n-2}{2}\right\}\pmod 8.$$

The quantity inside the braces is equal to

$$1-2n+2n(n-3)\equiv 1+2n^2\pmod 8.$$

Hence we get

$$S^{(n)}(1)\equiv\begin{cases}-1\pmod 8 & (n\text{ even}),\\ 3\pmod 8 & (n\text{ odd}).\end{cases} \tag{6.10}$$

The special values $S^{(4)}(1)=-1$, $S^{(9)}(1)=-5$ suggest that $S^{(n)}(1)$ is sometimes considerably smaller than $2\cdot 2^{n/2}$. Put

$$\alpha=\sqrt{2}(\cos\varphi+i\sin\varphi),\quad \beta=\sqrt{2}(\cos\varphi-i\sin\varphi), \tag{6.11}$$

so that

$$\cos\varphi=\frac{1}{-2\sqrt{2}},\quad \sin\varphi=\frac{\sqrt{7}}{2\sqrt{2}},\quad \cos 2\varphi=-\frac{3}{4}.$$

Since $\cos 2\varphi=-3/4$, it follows (for proof see [2], [6]) that φ is an *irrational* multiple of π.

By (6.11)

$$S^{(n)}(1)=-(\alpha^n+\beta^n)=-2\cdot 2^{n/2}\cos n\varphi.$$

We may therefore state

THEOREM 3. *For $q=2$ there exists an infinite sequence $N=\{n_1,n_2,n_3,\ldots\}$ such that*

$$S^{(n)}(1)=o(2^{n/2})\quad(n\in N). \tag{6.12}$$

There also exists an infinite sequence $N'=\{n_1',n_2',n_3',\ldots\}$ such that

$$S^{(n)}(1)\sim 2\cdot 2^{n/2}\quad(n\in N'). \tag{6.13}$$

It is not clear to what extent (6.12) can be sharpened. In particular it seems unlikely that

$$S^{(n)}(1)=O(1)\quad(n\in N'') \tag{6.14}$$

for any infinite sequence N''.

7. Other special cases. When $q=4$ we define the GF (4) by means of $\theta^2+\theta+1=0$. It is easily verified that

$$S(\theta)=-1. \tag{7.1}$$

We have therefore

$$\sum_{n=1}^{\infty}\frac{1}{n\cdot 4^{ns}}S^n(\theta)=\log(1-4^{-s}+4^{1-2s}). \tag{7.2}$$

In the present case α,β are roots of

$$x^2-x+4=0,$$

so that

$$\alpha,\beta=\tfrac{1}{2}(1\pm\sqrt{-15}). \tag{7.3}$$

Clearly $S^{(n)}(\theta)$ satisfies the recurrence

$$S^{(n+2)}(\theta)-S^{(n+1)}(\theta)+4S^{(n)}(\theta)=0 \tag{7.4}$$

with $S^{(0)}(\theta)=-2$, $S^{(1)}(\theta)=-1$. The first few values of $S^{(n)}(\theta)$ are

$$S^{(2)}(\theta)=7, \quad S^{(3)}(\theta)=11, \quad S^{(4)}(\theta)=-17,$$
$$S^{(5)}(\theta)=-61, \quad S^{(6)}(\theta)=7, \quad S^{(7)}(\theta)=231.$$

Formulas (5.9), (5.10) now reduce to

$$S^{(n)}(\theta)=-2^{1-n}\sum_{2r\leqslant n}(-1)^r\binom{n}{2r}15^r, \tag{7.5}$$

$$S^{(n)}(\theta)=-\sum_{2t\leqslant n}(-1)^t\frac{n}{n-t}\binom{n-t}{t}4^t. \tag{7.6}$$

It follows from (7.6) that

$$S^{(n)}(\theta)\equiv 4n-1 \pmod{16}. \tag{7.7}$$

Since, by (7.3),

$$|\alpha|=|\beta|=2,$$

it follows that

$$|S^{(n)}(\theta)|\leqslant 2\cdot 4^{n/2}, \tag{7.8}$$

so that we have proved (5.11) in this special case also.

If we put

$$\alpha=2(\cos\varphi+i\sin\varphi), \quad \beta=2(\cos\varphi+i\sin\varphi), \tag{7.9}$$

so that

$$\cos\varphi=\tfrac{1}{4}, \quad \sin\varphi=\tfrac{1}{4}\sqrt{15},$$

then exactly as above we can assert that *there exists an infinite sequence N such that*

$$S^{(n)}(\theta)=o(4^{n/2}) \quad (n\in N) \tag{7.10}$$

and an infinite sequence N' such that

$$S^{(n)}(\theta)\sim 2\cdot 4^{n/2} \quad (n\in N'). \tag{7.11}$$

We remark that by (2.7)

$$S^{(n)}(\theta)=S^{(n)}(\theta^2). \tag{7.12}$$

For $q=16$ we may define the GF(16) by means of $\varepsilon^4+\varepsilon+1=0$. We find, after some computation, the following results:

$$\begin{gathered} S(1)=-1, \quad S(\varepsilon^2+\varepsilon)=7, \\ S(\varepsilon)=-1, \quad S(\varepsilon^3)=3, \quad S(\varepsilon^3+1)=-5. \end{gathered} \tag{7.13}$$

Note that $\theta=\varepsilon^2+\varepsilon$ satisfies $\theta^2+\theta+1=0$ so that $S(\varepsilon^2+\varepsilon)=7$ is in agreement with the result obtained for $q=4$. Also $S(1)$ is in agreement with a previous result.

The numbers ε, ε^3, ε^3+1 are *primitive* elements of GF(16), that is, they do not belong to any smaller field. Moreover by (2.7)

$$\begin{gathered} S(\varepsilon)=S(\varepsilon^2)=S(\varepsilon+1)=S(\varepsilon^2+1), \\ S(\varepsilon^3)=S(\varepsilon^3+\varepsilon^2)=S(\varepsilon^3+\varepsilon^2+\varepsilon+1)=S(\varepsilon^3+\varepsilon), \\ S(\varepsilon^3+1)=S(\varepsilon^3+\varepsilon^2+1)=S(\varepsilon^3+\varepsilon^2+\varepsilon)=S(\varepsilon^3+\varepsilon+1). \end{gathered}$$

Also by (7.13) it is clear that

$$|S(a)|<2\cdot q^{1/2}=8, \tag{7.14}$$

so that

$$|S^{(n)}(a)|\leqslant 2\cdot 16^{n/2} \tag{7.15}$$

for all $a\in$GF(16).

We shall not take the space to state various explicit formulas for $S^{(n)}(a)$.

Finally we remark that for $q=3$ we have

$$S(1)=-1, \quad S(-1)=2,$$

so that here also

$$|S^{(n)}(a)|\leqslant 2\cdot 3^{n/2} \quad (q=3,\ a=\pm 1). \tag{7.16}$$

For $q=5$ we find that

$$\begin{gathered} S(1)=\tfrac{1}{2}(3-\sqrt{5}), \quad S(4)=\tfrac{1}{2}(3+\sqrt{5}), \\ S(2)=-1-\sqrt{5}, \quad S(3)=-1+\sqrt{5}. \end{gathered}$$

Once again it follows that

$$|S^{(n)}(a)|\leqslant 2\cdot 5^{n/2} \quad (q=5;\ a=1,2,3,4). \tag{7.17}$$

References

[1] L. Carlitz and S. Uchiyama, *Bounds for exponential sums*, Duke Math. Journ. 24 (1957), pp. 37–42.

[2] L. Carlitz and J. M. Thomas, *Rational tabulated values of trigonometric functions*, Amer. Math. Monthly 69 (1962), pp. 789–793.

[3] L. Carlitz, *Weighted quadratic partitions over a finite field*, Canadian Journ. Math. 5 (1953), pp. 317–323.

[4] D. H. and Emma Lehmer, *The cyclotomy of Kloosterman sums*, Acta Arith. 12 (1967), pp. 385–407.

[5] D. H. and Emma Lehmer, *The cyclotomy of hyper-Kloosterman sums*, Acta Arith. 14 (1968), pp. 89–111.

[6] J. M. H. Olmsted, *Rational values of trigonometric functions*, Amer. Math. Monthly 52 (1945), pp. 507–508.

[7] A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. USA 34 (1948), pp. 204–207.

Reçu par la Rédaction le 12. 2. 1969

ACTA ARITHMETICA
XVI (1969)

Sur certaines fonctions additives à valeurs entières

par

HUBERT DELANGE (Paris)

1. Introduction. Kubilius a établi le résultat suivant (1):

Soit f une fonction arithmétique additive à valeurs entières. On suppose que $f(p) = 0$ pour tout p premier (2).

Alors, pour chaque entier q, l'ensemble des entiers positifs n pour lesquels $f(n) = q$ possède une densité d_q.

Plus precisèment, si $\nu_q(x)$ est le nombre des $n \leqslant x$ tels que $f(n) = q$, on a pour x infini

$$\nu_q(x) = d_q x + O\left[\frac{x \log\log x}{\log x}\right].$$

Nous nous proposons ici d'améliorer le résultat de Kubilius en montrant que *l'on a en fait*

$$\nu_q(x) = d_q x + O[x^{1/2}].$$

On peut même préciser *qu'il existe une constante absolue C telle que, quelle que soit la fonction f considérée et quel que soit l'entier q, on a pour* $x \geqslant 1$

$$|\nu_q(x) - d_q x| \leqslant C x^{1/2}. \tag{1}$$

2. Rappels.

2.1. Soit $\mathscr{A}$ l'ensemble des fonctions arithmétiques, c'est-à-dire des fonctions réelles ou complexes définies sur l'ensemble N^* des entiers $\geqslant 1$.

Il est usuel de définir une convolution dans $\mathscr{A}$ par la formule

$$(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right).$$

(1) Cf. J. Kubilius, *Probabilistic Methods in the Theory of Numbers* (Translations of mathematical Monographs, vol. 11, theorem 4.9, p. 88).

(2) Tout au long de cet article, la lettre p désigne un nombre premier. Les lettres m, n, r désignent des entiers $\geqslant 1$.