ON CHARACTER SUMS IN FINITE FIELDS.

By

H. DAVENPORT
of MANCHESTER.

1. Introduction.

Let $q = p^e$ be a power of a prime p, and let $[q]$ denote the finite field (or "Galois field") of q elements. Let $f_1(x), \ldots, f_r(x)$ be polynomials over $[q]$, and let $\chi_1, \ldots, \chi_r$ be multiplicative characters of $[q]$ with the convention $\chi(0) = 0$. A character sum is an expression of the form

$$S(f, \chi) = \sum_{x \text{ in } [q]} \chi_1(f_1(x)) \ \ldots \ \chi_r(f_r(x)). \tag{1}$$

We shall make the (trivial) simplification of supposing that $\chi_1, \ldots, \chi_r$ are non-principal characters, and that $f_1(x), \ldots, f_r(x)$ are different normalised[1] polynomials, each irreducible over $[q]$. Let $k_1, \ldots, k_r$ denote the degrees of these polynomials, and let $K = k_1 + \cdots + k_r$.

In connection with any such character sum we define a function $L(f, \chi; s)$ of the complex variable $s = \sigma + it$ which is in fact a polynomial in q^{-s} of degree $K - 1$. These L-functions are essentially the same as those obtained by Hasse[2] as factors of the congruence zeta-function of an algebraic function-field generated by an equation of the form $y^n = f(x)$. The object of this paper is to give a more direct and elementary account of these L-functions.

The definition is as follows. Let (f, g) denote the resultant of two normalised polynomials $f(x)$, $g(x)$ over $[q]$.[3] Let

---

[1] A normalised polynomial is one in which the coefficient of the highest power of x is 1.

[2] Journal für Math. (Crelle), 172 (1934), 37—54.

[3] $(f, g) = \prod_{\Phi} f(\Phi)$, where Φ runs through the roots of $g(x) = 0$.

(2) $$\sigma_\nu = \sum_g \chi_1((f_1, g)) \ldots \chi_r((f_r, g)),$$

where the summation is extended over all normalised polynomials $g(x)$ over $[q]$ of degree ν.[1] Then

(3) $$L(f, \chi; s) = \sum_{\nu=0}^{\infty} \sigma_\nu q^{-\nu s}.$$

The results which will be proved fall under three heads.

(I). If h is any positive integer, the field $[q^h]$ is an extension-field of $[q]$, and any character χ in $[q]$ induces a character $\chi^{(h)}$ in $[q^h]$. This character is defined by $\chi^{(h)}(\xi) = \chi(N\xi)$, where $N\xi$ denotes the norm relative to $[q]$ of an element ξ of $[q^h]$. Let

(4) $$S^{(h)}(f, \chi) = \sum_{\xi \text{ in } [q^h]} \chi_1^{(h)}(f_1(\xi)) \ldots \chi_r^{(h)}(f_r(\xi)).$$

Let $s_1, \ldots, s_{K-1}$ denote the different zeros of $L(f, \chi; s)$, ignoring the period $\frac{2\pi}{\log q}$ in t. Then

(5) $$-S^{(h)}(f, \chi) = q^{h s_1} + \cdots + q^{h s_{K-1}}.$$

In particular,

(6) $$-S(f, \chi) = q^{s_1} + \cdots + q^{s_{K-1}}.$$

(II). If $\chi_1^{k_1} \ldots \chi_r^{k_r} \neq \chi_0$ (the principal character), $L(f, \chi; s)$ satisfies the functional equation[2]

(7) $$q^{\frac{1}{2}(K-1)s} L(f, \chi; s) = \varepsilon(f, \chi) q^{\frac{1}{2}(K-1)(1-s)} L(f, \bar{\chi}; 1-s),$$

where

(8) $$\varepsilon(f, \chi) = q^{-\frac{1}{2}(K-1)} \sigma_{K-1}, \qquad |\varepsilon(f, \chi)| = 1.$$

σ_{K-1} will be evaluated explicitly in terms of Gaussian sums and of the characters of certain resultants of the polynomials $f_1, \ldots, f_r$.

If $\chi_1^{k_1} \ldots \chi_r^{k_r} = \chi_0$, $L(f, \chi; s)$ has the factor $1 - q^{-s}$. Writing

---

[1] For $\nu = 0$, there is only one polynomial g, namely 1. Also $(f_i, 1) = 1$. Hence $\sigma_0 = 1$.

[2] This was conjectured by Hasse (loc. cit., 52). A proof different from that in the present paper has been given (in an unpublished MS) by Witt.

$$(9) \qquad L_1(f, \chi; s) = \frac{L(f, \chi; s)}{1 - q^{-s}} = \sigma'_0 + \sigma'_1 q^{-s} + \cdots + \sigma'_{K-2} q^{-(K-2)s},$$

$L_1(f, \chi; s)$ satisfies (7) and (8) with $K-2$ in place of $K-1$ and σ'_{K-2} in place of σ_{K-1}. σ'_{K-2} will be evaluated explicitly.

(III). It is conjectured that the zeros of $L(f, \chi; s)$ (apart from the possible zero $s = 0$) all have real part $\frac{1}{2}$. If $K = 2$, and $\chi_1^{k_1} \ldots \chi_r^{k_r} \neq \chi_0$, then

$$L(f, \chi; s) = 1 + \sigma_1 q^{-s},$$

and $|\sigma_1| = q^{\frac{1}{2}}$, by (8). If $K = 3$ and $\chi_1^{k_1} \ldots \chi_r^{k_r} = \chi_0$, then

$$L(f, \chi; s) = (1 - q^{-s})(1 + \sigma'_1 q^{-s}),$$

and $|\sigma'_1| = q^{\frac{1}{2}}$. Hence, in these two cases, the conjecture is true.

It is a deep theorem of Hasse[1] that the conjecture is true for $K = 3$ when each of the characters is the quadratic character.

It will be proved that, in the general case, the real part of any zero (except $s = 0$) satisfies

$$(10) \qquad \theta_K \leqq \sigma \leqq 1 - \theta_K,$$

where

$$(11) \qquad \theta_3 = \frac{1}{4}, \quad \theta_K = \frac{3}{2(K+4)} \qquad (K \geqq 4).$$

If $\chi_1^{k_1} \ldots \chi_r^{k_r} = \chi_0$, (10) can be improved to

$$(12) \qquad \theta_{K-1} \leqq \sigma \leqq 1 - \theta_{K-1}.$$

Combining (10) with (6), we have

$$(13) \qquad |S(f, \chi)| \leqq (K-1) q^{1-\theta_K},$$

where θ_K can be replaced by θ_{K-1} if $\chi_1^{k_1} \ldots \chi_r^{k_r} = \chi_0$.[2]

The inequality (13) has several applications. The most obvious of these is to the distribution of power-residues (mod p). This is discussed in § 9.

---

[1] Hamburg Abh. 10 (1934), 325—348.

[2] For $K > 3$, all previously known inequalities for $S(f, \chi)$ dealt only with the case in which all the characters are quadratic. For an account of them, see Davenport, Journal London Math. Soc. 8 (1933), 46—52. They are all weaker than (13) above.

Another application is to a result of Bilharz on the distribution of the irreducible polynomials (mod p) with respect to which a fixed polynomial is a primitive root.[1] In the proof of this, the hypothesis[2] is made that the zeros of $L(f, \chi; s)$ satisfy an inequality of the type (10), where θ_K is independent of the characters $\chi_1, \ldots, \chi_r$. This, as we see, is the case.

2. Proof of (5).

In this section we shall take for granted the result (which will be proved in § 4, § 5) that $L(f, \chi; s)$ is a polynomial in q^{-s} of degree $K - 1$, and shall show how (5) follows from the definition of $L(f, \chi; s)$.

We observe first that the definition (3) of $L(f, \chi; s)$ can be written in a product form, analogous to the Euler product for Dirichlet's L-functions. Write, for brevity,

$$X(g) = \chi_1((f_1, g)) \ldots \chi_r((f_r, g)),$$

then $X(g_1 g_2) = X(g_1) X(g_2)$ for any two normalised polynomials g_1, g_2. Write also $|g| = q^\nu$ for any normalised polynomial g of degree ν. We have

$$L(f, \chi; s) = \sum_g X(g) |g|^{-s},$$

where the summation is extended over all normalised polynomials g over $[q]$. Since every such polynomial is representable uniquely as a product of normalised irreducible polynomials, and since $X(g)$, $|g|$ are multiplicative, we have (for $\Re s > 1$)

$$L(f, \chi; s) = \prod_G (1 - X(G) |G|^{-s})^{-1}, \tag{14}$$

where the product is extended over all normalised irreducible polynomials G over $[q]$.

It follows from (14) that

$$\log L(f, \chi; s) = \sum_G \sum_{\nu=1}^{\infty} \frac{1}{\nu} X(G^\nu) |G^\nu|^{-s}.$$

On the other hand, if $L(f, \chi; s)$ is a polynomial in q^{-s} with zeros $s_1, \ldots, s_{K-1}$, we have

[1] Math. Annalen 114 (1937), 476—492.

[2] loc. cit. (20).

$$\log L(f, \chi;\ s) = -\sum_{h=1}^{\infty} \frac{1}{h} \left(\sum_{i=1}^{K-1} q^{h s_i} \right) q^{-hs}.$$

Comparing the coefficients of q^{-hs} in the two expressions, we obtain

(15)
$$-\sum_{i=1}^{K-1} q^{h s_i} = h \sum_{\substack{G,\ \nu \\ |G^\nu| = q^h}} \frac{1}{\nu} X(G^\nu) = \sum_{h' | h} h' \sum_{G} X\left(G^{\frac{h}{h'}}\right),$$

where, in the last sum, G runs through all normalised irreducible polynomials of degree h'.

We now recall that the elements of $[q^h]$ consist precisely of all roots ξ of all normalised irreducible polynomials G over $[q]$ whose degree h' divides h. The conjugates of such an element ξ consist of all the roots of G, each counted $\frac{h}{h'}$ times. Hence

$$\chi_i^{(h)}(f_i(\xi)) = \chi_i(N f_i(\xi)) = \chi_i\left(\left(f_i,\ G^{\frac{h}{h'}}\right)\right).$$

Thus

$$\chi_1^{(h)}(f_1(\xi)) \ \ldots\ \chi_r^{(h)}(f_r(\xi)) = X\left(G^{\frac{h}{h'}}\right).$$

Summation over all elements ξ of $[q^h]$ is equivalent to summation over h' and G under the same conditions as in (15), and each polynomial G arises from h' different elements ξ. Hence the sum (15) is equal to $S^{(h)}(f, \chi)$ and (5) is proved.

3. Preliminaries.

Gaussian sums. Denote by $\mathfrak{S} x$ the absolute trace (Spur) of an element x of $[q]$, i. e. its trace relative to $[p]$. Corresponding to any non-principal character χ of $[q]$ there exists a Gaussian sum defined by

(16)
$$\tau(\chi) = \sum_{x \text{ in } [q]} \chi(x)\, e(\mathfrak{S} x),$$

where $e(u)$ is an abbreviation for $e^{\frac{2\pi i u}{p}}$. It is well known that

$$|\tau(\chi)| = \sqrt{q}. \tag{17}$$

If, in (16), we replace x by ax, where $a \neq 0$ is an element of $[q]$, and change χ into the conjugate complex character $\bar{\chi}$, we obtain the useful formula

$$\chi(a) = \frac{1}{\tau(\bar{\chi})} \sum_{x \text{ in } [q]} \bar{\chi}(x)\, e(\mathfrak{S}(ax)). \tag{18}$$

This formula is obviously also valid for $a = 0$.

Let h be any positive integer, and let $\chi^{(h)}$, as before, denote the character induced by χ in $[q^h]$. Let

$$\tau^{(h)}(\chi) = \sum_{\xi \text{ in } [q^h]} \chi^{(h)}(\xi)\, e(\mathfrak{S}\xi), \tag{19}$$

where $\mathfrak{S}\xi$ again denotes the absolute trace of ξ. It was proved by Davenport and Hasse[1] that

$$\tau^{(h)}(\chi) = (-1)^{h-1} (\tau(\chi))^h. \tag{20}$$

A more elementary proof has been given by H. L. Schmid.[2]

Basis for a finite field. Let ϑ be any generating element of $[q^k]$ relative to $[q]$, so that $1, \vartheta, \ldots, \vartheta^{k-1}$ form a basis for $[q^k]$ relative to $[q]$, i. e. every element ξ of $[q^k]$ is representable uniquely as

$$\xi = x_0 + x_1 \vartheta + \cdots + x_{k-1} \vartheta^{k-1}$$

with $x_0, \ldots, x_{k-1}$ in $[q]$.

There exists an element λ of $[q^k]$ such that

$$\begin{cases} sp\,\lambda = sp\,\lambda\vartheta = \cdots = sp\,\lambda\vartheta^{k-2} = 0, \\ \qquad sp\,\lambda\vartheta^{k-1} = 1, \end{cases} \tag{21}$$

where sp denotes the trace of an element of $[q^k]$ relative to $[q]$. For the equations (21) are k linear equations for λ and its conjugates, and are easily seen to have the solution

$$\lambda = \prod_{\vartheta'} (\vartheta - \vartheta')^{-1},$$

where ϑ' runs through the conjugates of ϑ other than ϑ itself.

---

[1] Journal für Math. (Crelle), 172 (1934), 151—182. The Gaussian sums are defined there with a negative sign prefixed.

[2] Journal für Math. (Crelle), 176 (1937), 189—191.

If an element ξ of $[q^k]$ has the form

$$\xi = u_0 + u_1 \vartheta + \cdots + u_{\nu-1} \vartheta^{\nu-1} + \vartheta^\nu \qquad (u_0, \ldots \text{ in } [q]), \tag{22}$$

where $0 \leqq \nu \leqq k - 1$, the equations (22) show that[1]

$$\begin{cases} sp\,\lambda\,\xi = sp\,\lambda\,\vartheta\,\xi = \cdots = sp\,\lambda\,\vartheta^{k-2-\nu}\,\xi = 0, \\ \qquad\qquad sp\,\lambda\,\vartheta^{k-1-\nu}\,\xi = 1. \end{cases} \tag{23}$$

It is plain that as $u_0, \ldots, u_{\nu-1}$ run through all elements of $[q]$, ξ runs through all elements of $[q^k]$ which satisfy (23).

Simultaneous basis for several finite fields. Let $k_1, \ldots, k_r$ be positive integers (not necessarily different), and let $K = k_1 + \cdots + k_r$. Sets

$$\alpha_{11}, \ldots, \alpha_{K1}; \quad \alpha_{12}, \ldots, \alpha_{K2}; \quad \ldots; \quad \alpha_{1r}, \ldots, \alpha_{Kr}$$

of elements of $[q^{k_1}], \ldots, [q^{k_r}]$ respectively will be called a simultaneous basis for these fields relative to $[q]$ if every set $\xi_1, \ldots, \xi_r$ of elements of $[q^{k_1}], \ldots, [q^{k_r}]$ respectively is representable uniquely as

$$\xi_i = x_1 \alpha_{1i} + \cdots + x_K \alpha_{Ki} \qquad (i = 1, \ldots, r),$$

where $x_1, \ldots, x_K$ are elements of $[q]$.

Let $\vartheta_1, \ldots, \vartheta_r$ be generating elements of $[q^{k_1}], \ldots, [q^{k_r}]$ respectively, relative to $[q]$, and suppose also that no two of the ϑ's are equal or conjugate. Then

$$1, \vartheta_1, \ldots, \vartheta_1^{K-1}; \quad \ldots; \quad 1, \vartheta_r, \ldots, \vartheta_r^{K-1}$$

form a simultaneous basis for the fields. For, as $x_0, \ldots, x_{K-1}$ run through $[q]$, the elements $\xi_1, \ldots, \xi_r$ defined by

$$\xi_i = x_0 + x_1 \vartheta_i + \cdots + x_{K-1} \vartheta_i^{K-1}$$

run through $q^K = q^{k_1 + \cdots + k_r}$ sets of elements of $[q^{k_1}], \ldots, [q^{k_r}]$. Thus it suffices to show that these sets are all different, i. e. that there is no non-zero set of x's for which

$$x_0 + x_1 \vartheta_i + \cdots + x_{K-1} \vartheta_i^{K-1} = 0$$

for $i = 1, \ldots, r$. This is so, since the determinant of the K linear equations formed by these equations and their conjugates is not zero.

[1] If $\nu = k - 1$, the first line of (23) is empty.

Let $\vartheta_1, \ldots, \vartheta_r$ be a set of generating elements, as above. There exist elements $\lambda_1, \ldots, \lambda_r$ in $[q^{k_1}], \ldots, [q^{k_r}]$ respectively, such that

$$(24)\quad \left\{\begin{array}{l} \sum_{i=1}^{r} sp\,\lambda_i = \sum_{i=1}^{r} sp\,\lambda_i\vartheta_i = \cdots = \sum_{i=1}^{r} sp\,\lambda_i\vartheta_i^{K-2} = 0, \\ \sum_{i=1}^{r} sp\,\lambda_i\vartheta_i^{K-1} = 1, \end{array}\right.$$

where $sp\,\lambda_i\vartheta_i^\nu$ denotes the trace of $\lambda_i\vartheta_i^\nu$, considered as an element of $[q^{k_i}]$, relative to $[q]$. For, denoting by $\lambda_i^{(1)} = \lambda_i, \lambda_i^{(2)}, \ldots, \lambda_i^{(k_i)}$ the conjugates of λ_i relative to $[q]$, the equations (24) are K linear equations in the K unknowns $\lambda_1^{(1)}, \ldots, \lambda_r^{(k_r)}$. Their solution is easily seen to be

$$(25)\quad \lambda_i = \prod_{\vartheta'} (\vartheta_i - \vartheta')^{-1},$$

where ϑ' runs through all of $\vartheta_1, \ldots, \vartheta_r$ and their conjugates, except ϑ_i itself.

We observe that if a set $\xi_1, \ldots, \xi_r$ of elements of $[q^{k_1}], \ldots, [q^{k_r}]$ has the form

$$(26)\quad \xi_i = u_0 + u_1\vartheta_i + \cdots + u_{\nu-1}\vartheta_i^{\nu-1} + \vartheta_i^\nu \qquad (u_0, \ldots, u_{\nu-1} \text{ in } [q]),$$

where $0 \leqq \nu \leqq K-1$, then (24) show that[1]

$$(27)\quad \left\{\begin{array}{l} \sum_{i=1}^{r} sp\,\lambda_i\xi_i = \sum_{i=1}^{r} sp\,\lambda_i\vartheta_i\xi_i = \cdots = \sum_{i=1}^{r} sp\,\lambda_i\vartheta_i^{K-2-\nu}\xi_i = 0, \\ \sum_{i=1}^{r} sp\,\lambda_i\vartheta_i^{K-1-\nu}\xi_i = 1. \end{array}\right.$$

It is also plain that if $u_0, \ldots, u_{\nu-1}$ run through all elements of $[q]$, then $\xi_1, \ldots, \xi_r$, defined by (26), run through all sets which satisfy (27).

4. Theorem 1.

Let ϑ_i be a root of $f_i(x) = 0$ $(i = 1, \ldots, r)$. Since $f_1(x), \ldots, f_r(x)$ are different normalised irreducible polynomials, no two ϑ's are equal or conjugate.

---

[1] If $\nu = K-1$, the first line of (27) is empty.

Thus they form a set of generating elements of $[q^{k_1}], \ldots, [q^{k_r}]$ of the kind considered in § 3.

Let $\psi_i = \chi_i^{(k_i)}$ be the character induced by χ_i in $[q^{k_i}]$. Let

$$\varepsilon = \chi_1^{k_1} \ldots \chi_r^{k_r}(-1).$$

Theorem 1. *For* $\nu \geqq K$, $\sigma_\nu = 0$. *For* $0 \leqq \nu \leqq K - 1$,

$$\sigma_\nu = \varepsilon^\nu \sum_{\substack{\xi_1, \ldots, \xi_r \\ (27)}} \psi_1(\xi_1) \ldots \psi_r(\xi_r),$$

where $\xi_1, \ldots, \xi_r$ *run through all elements of* $[q^{k_1}], \ldots, [q^{k_r}]$ *respectively which satisfy* (27).

Proof. If $g(x)$ is a normalised polynomial of degree ν, we have, by the definition of the resultant,

$$(f_i, g) = (-1)^{k_i \nu}(g, f_i) = (-1)^{k_i \nu} N g(\vartheta_i),$$

where $Ng(\vartheta_i)$ denotes the norm of $g(\vartheta_i)$, considered as an element of $[q^{k_i}]$, relative to $[q]$. Hence

$$\chi_i((f_i, g)) = \chi_i(-1)^{k_i \nu} \psi_i(g(\vartheta_i)).$$

Let $g(x) = x^\nu + u_{\nu-1} x^{\nu-1} + \cdots + u_0$. By definition,

$$\sigma_\nu = \sum_{\substack{u_0, \ldots, u_{\nu-1} \\ \text{in } [q]}} \chi_1((f_1, g)) \ldots \chi_r((f_r, g))$$

(28) $$= \varepsilon^\nu \sum_{\substack{u_0, \ldots, u_{\nu-1} \\ \text{in } [q]}} \psi_1(g(\vartheta_1)) \ldots \psi_r(g(\vartheta_r)).$$

In view of the remark made at the end of § 3, this establishes the second result.

Since

$$1, \vartheta_1, \ldots, \vartheta_1^{K-1}; \quad \ldots; \quad 1, \vartheta_r, \ldots, \vartheta_r^{K-1}$$

forms a simultaneous basis for $[q^{k_1}], \ldots, [q^{k_r}]$ it follows that, if $\nu \geqq K$, $g(\vartheta_1), \ldots, g(\vartheta_r)$ run through all elements of these fields as $u_0, \ldots, u_{K-1}$ run through $[q]$, for fixed $u_K, \ldots, u_{\nu-1}$. Hence, if $\nu \geqq K$,

$$\sigma_\nu = \varepsilon^\nu q^{\nu-K} \sum_{\xi_1 \text{ in } [q^{k_1}]} \cdots \sum_{\xi_r \text{ in } [q^{k_r}]} \psi_1(\xi_1) \ldots \psi_r(\xi_r) = 0.$$

This completes the proof of Theorem 1.

5. The Functional Equation, and the Value of σ_{K-1}.

Let $f'_i(x)$ denote the derived polynomial of $f_i(x)$, and let

$$A_i = (f'_i, f_i) \prod_{\substack{j=1 \\ j \neq i}}^{r} (f_j, f_i) \tag{29}$$

for $i = 1, \ldots, r$. Since $f_1(x), \ldots, f_r(x)$ are different normalised irreducible polynomials, $A_i \neq 0$.

Theorem 2 (a). *If* $\chi_1^{k_1} \ldots \chi_r^{k_r} \neq \chi_0$,

$$\sigma_{K-1} = \varepsilon^{K-1} \frac{\tau(\chi_1)^{k_1} \ldots \tau(\chi_r)^{k_r}}{\tau\left(\chi_1^{k_1} \ldots \chi_r^{k_r}\right)} \prod_{i=1}^{r} (-1)^{k_i - 1} \chi_i(A_i). \tag{30}$$

Also, for $\nu = 0, 1, \ldots, K-1$,

$$\frac{\sigma_\nu}{q^{\frac{1}{2}\nu}} = \frac{\sigma_{K-1}}{q^{\frac{1}{2}(K-1)}} \frac{\sigma_{K-1-\nu}}{q^{\frac{1}{2}(K-1-\nu)}}. \tag{31}$$

Proof. If a is any element of $[q]$, we have

$$\sum_{t \text{ in } [q]} e(\mathfrak{S}(t a)) = \begin{cases} 0 \text{ if } a \neq 0, \\ q \text{ if } a = 0. \end{cases}$$

Suppose that $0 \leqq \nu \leqq K-1$, and let $t_0, t_1, \ldots, t_{K-1-\nu}$ be any elements of $[q]$. Let $t(x) = t_0 + \cdots + t_{K-1-\nu} x^{K-1-\nu}$. The value of the sum

$$\sum_{\substack{t_0, \ldots, t_{K-1-\nu} \\ \text{in } [q]}} e\left(\mathfrak{S}\left(\sum_{i=1}^{r} sp\, \lambda_i \xi_i t(\vartheta_i) - t_{K-1-\nu}\right)\right)$$

is zero unless $\xi_1, \ldots, \xi_r$ satisfy (27), in which case it is $q^{K-\nu}$. Hence, by Theorem 1,

$$\sigma_\nu = \frac{\varepsilon^\nu}{q^{K-\nu}} \sum_{\substack{t_0, \ldots, t_{K-1-\nu} \\ \text{in } [q]}} \sum_{\xi_1 \text{ in } [q^{k_1}]} \cdots \sum_{\xi_r \text{ in } [q^{k_r}]} \psi_1(\xi_1) \ldots \psi_r(\xi_r) \times$$
$$\times\, e\left(\mathfrak{S}\left(\sum_{i=1}^{r} sp\, \lambda_i \xi_i t(\vartheta_i) - t_{K-1-\nu}\right)\right).$$

By (18),

$$\sum_{\xi_i \text{ in } [q^{k_i}]} \psi_i(\xi_i) e\left(\mathfrak{S}(sp\, \lambda_i\, \xi_i\, t(\vartheta_i))\right)$$

$$= \psi_i(\lambda_i t(\vartheta_i)) \tau(\psi_i).$$

Since, in the notation of § 3, $\psi_i = \chi_i^{(k_i)}$, we have

$$\psi_i(\lambda_i) = \bar{\chi}_i(N\lambda_i),$$

and, by (20),

$$\tau(\psi_i) = (-1)^{k_i - 1}(\tau(\chi_i))^{k_i}.$$

By (25),

$$\lambda_i^{-1} = \prod_{\vartheta'} (\vartheta_i - \vartheta')$$

$$= f_i'(\vartheta_i) \prod_{\substack{j=1 \\ j \neq i}}^{r} f_j(\vartheta_i),$$

hence

$$N\lambda_i^{-1} = (f_i', f_i) \prod_{\substack{j=1 \\ j \neq i}}^{r} (f_j, f_i) = A_i.$$

We have, therefore,

$$\sigma_\nu = \frac{\varepsilon^\nu}{q^{K-\nu}} \prod_{i=1}^{r} (-1)^{k_i - 1} \chi_i(A_i) \tau(\chi_i)^{k_i} \sum_{t_0, \ldots, t_{K-1-\nu}} \psi_1(t(\vartheta_1)) \ldots \psi_r(t(\vartheta_r)) e(-\mathfrak{S}\, t_{K-1-\nu}).$$

In the sum over the t's, we consider first all terms for which $t_{K-1-\nu} = 0$. With any set $t_0, \ldots, t_{K-2-\nu}$ (not all zero) occur also all sets $u\, t_0, \ldots, u\, t_{K-2-\nu}$ for any $u \neq 0$ of $[q]$. The contributions of these two sets differ by the factor

$$\psi_1(u) \ldots \psi_r(u) = \bar{\chi}_1^{k_1} \ldots \bar{\chi}_r^{k_r}(u).$$

Since

$$\sum_{\substack{u \text{ in } [q] \\ u \neq 0}} \bar{\chi}_1^{k_1} \ldots \bar{\chi}_r^{k_r}(u) = 0,$$

the total contribution of the terms under consideration vanishes.

In the terms for which $t_{K-1-\nu} \neq 0$, we write

$$t_j = t_{K-1-\nu}\, u_j,$$

$$g(x) = u_0 + u_1 x + \cdots + u_{K-2-\nu} x^{K-2-\nu} + x^{K-1-\nu}.$$

Then the sum over $t_0, \ldots, t_{K-1-\nu}$ becomes

$$\sum_{\substack{u_0, \ldots, u_{K-2-\nu} \\ \text{in } [q]}} \psi_1(g(\vartheta_1)) \ldots \psi_r(g(\vartheta_r)) \sum_{\substack{t_{K-1-\nu} \text{ in } [q] \\ t_{K-1-\nu} \neq 0}} \psi_1 \ldots \psi_r(t_{K-1-\nu})\, e(-\mathfrak{S}\, t_{K-1-\nu}).$$

The value of the sum over $t_{K-1-\nu}$ (in which the condition $t_{K-1-\nu} \neq 0$ may now be omitted) is

$$\sum_t \bar{\chi}_1^{k_1} \ldots \bar{\chi}_r^{k_r}(t)\, e(-\mathfrak{S}\, t) = \tau\left(\overline{\chi_1^{k_1} \ldots \chi_r^{k_r}}\right).$$

The sum over the u's gives

$$\varepsilon^{K-1-\nu}\, \sigma_{K-1-\nu},$$

by (28).

Hence

$$\sigma_\nu = \frac{\varepsilon^\nu}{q^{K-\nu}} \left(\prod_{i=1}^{r} (-1)^{k_i-1}\, \tau(\chi_i)^{k_i} \chi_i(A_i)\right) \tau\left(\overline{\chi^{k_1} \ldots \chi_r^{k_r}}\right) \varepsilon^{K-1-\nu}\, \sigma_{K-1-\nu}$$

(32)
$$= \frac{\varepsilon^{K-1}}{q^{K-1-\nu}} \frac{\tau(\chi_1)^{k_1} \ldots \tau(\chi_r)^{k_r}}{\tau\left(\chi_1^{k_1} \ldots \chi_r^{k_r}\right)} \left(\prod_{i=1}^{r} (-1)^{k_i-1} \chi_i(A_i)\right) \sigma_{K-1-\nu},$$

using (17). Taking $\nu = K - 1$, we obtain (30) (since $\sigma_0 = 1$). Finally, (31) follows from (32) and (30).

The relations (31) are equivalent to the functional equation (7), and (8) follows from (30) and (17).

Theorem 2 (b). *If* $\chi_1^{k_1} \ldots \chi_r^{k_r} = \chi_0$, $\sigma_0 + \sigma_1 + \cdots + \sigma_{K-1} = 0$. *If* $\sigma'_\nu = \sigma_0 + \cdots + \sigma_\nu$, *then*

(33)
$$-\sigma_{K-1} = \sigma'_{K-2} = \frac{1}{q} \tau(\chi_1)^{k_1} \ldots \tau(\chi_r)^{k_r} \prod_{i=1}^{r} (-1)^{k_i-1} \chi_i(A_i).$$

Also, for $\nu = 0, 1, \ldots, K-2$,

(34)
$$\frac{\sigma'_\nu}{q^{\frac{1}{2}\nu}} = \frac{\sigma'_{K-2}}{q^{\frac{1}{2}(K-2)}} \frac{\bar{\sigma}'_{K-2-\nu}}{q^{\frac{1}{2}(K-2-\nu)}}.$$

Proof. We note first that $\varepsilon = \chi_1^{k_1} \ldots \chi_r^{k_r}(-1) = 1$.

If $\xi_1, \ldots, \xi_r$ run through all sets satisfying (27), and a runs through all elements of $[q]$ except 0, then $\eta_1 = a\,\xi_1, \ldots, \eta_r = a\,\xi_r$ run through all sets satisfying

(35 a) $$\sum_{i=1}^{r} sp\,\lambda_i \eta_i = \sum_{i=1}^{r} sp\,\lambda_i \vartheta_i \eta_i = \cdots = \sum_{i=1}^{r} sp\,\lambda_i\, \vartheta_i^{K-2-\nu} \eta_i = 0,$$

(35 b) $$\sum_{i=1}^{r} sp\,\lambda_i\, \vartheta_i^{K-1-\nu} \eta_i \neq 0.$$

Hence

$$(q-1)\sigma_\nu = \sum_{\substack{\eta_1, \ldots, \eta_r \\ (35\,a),\ (35\,b)}} \psi_1(\eta_1) \ldots \psi_r(\eta_r).$$

It follows that

(36) $$(q-1)(\sigma_0 + \sigma_1 + \cdots + \sigma_\nu) = \sum_{\substack{\eta_1, \ldots, \eta_r \\ (35\,a)}} \psi_1(\eta_1) \ldots \psi_r(\eta_r).$$

Taking $\nu = K-1$, the conditions (35 a) disappear, and we obtain

$$(q-1)(\sigma_0 + \cdots + \sigma_{K-1}) = 0.$$

Replacing the conditions (35 a) by summations over variables $t_0, \ldots, t_{K-2-\nu}$ as in the proof of Theorem 2 (a), we have

$$(q-1)\sigma'_\nu = \frac{1}{q^{K-1-\nu}} \sum_{\substack{t_0, \ldots, t_{K-2-\nu} \\ \text{in } [q]}} \sum_{\eta_1 \text{ in } [q^{k_1}]} \cdots \sum_{\eta_r \text{ in } [q^{k_r}]} \psi_1(\eta_1) \ldots \psi_r(\eta_r) \times$$
$$\times\, e\left(\mathfrak{S}\left(\sum_{i=1}^{r} sp\,\lambda_i \xi_i\, t(\vartheta_i)\right)\right)$$
$$= \frac{1}{q^{K-1-\nu}} \prod_{i=1}^{r} (-1)^{k_i-1} \chi_i(A_i)\, \tau(\chi_i)^{k_i} \sum_{\substack{t_0, \ldots, t_{K-2-\nu} \\ \text{in } [q]}} \psi_1(t(\vartheta_1)) \ldots \psi_r(t(\vartheta_r)).$$

As $t_0, \ldots, t_{K-2-\nu}$ run through all elements of $[q]$, $t(\vartheta_1), \ldots, t(\vartheta_r)$ run through all sets $\eta_1, \ldots, \eta_r$ of elements of $[q^{k_1}], \ldots, [q^{k_r}]$ which satisfy (35 a) with ν replaced by $K-2-\nu$. Hence

(37) $$(q-1)\sigma'_\nu = \frac{1}{q^{K-1-\nu}} \left(\prod_{i=1}^{r} (-1)^{k_i-1} \chi_i(A_i)\, \tau(\chi_i)^{k_i}\right) (q-1)\, \sigma'_{K-2-\nu}.$$

Taking $\nu = K-2$, we obtain (33) (since $\sigma'_0 = 1$). Finally, (34) follows from (33) and (37).

The relations (34) are equivalent to the functional equation (7) for $L_1(f, \chi; s)$ with $K-2$ in place of $K-1$, and the modified form of (8) follows from (33) and (17).

6. Inequalities for the Zeros.

In this and the following sections, the constants implied by the symbol O depend only on K.

Lemma 1. *If*

$$S^{(h)}(f, \chi) = O(q^{(1-\theta)h}) \qquad \left(0 < \theta \leqq \frac{1}{2}\right) \tag{38}$$

as h tends to infinity through all multiples of a fixed positive integer k, then all zeros of $L(f, \chi; s)$ (except $s = 0$) satisfy

$$\theta \leqq \sigma \leqq 1 - \theta.$$

Proof. By (5), the hypothesis is equivalent to

$$q^{h s_1} + \cdots + q^{h s_{K-1}} = O(q^{(1-\theta)h})$$

as $h \to \infty$, $k|h$. Let σ be the maximum real part of any of $s_1, \ldots, s_{K-1}$, attained, say, for $s'_1, \ldots, s'_L$. Let ϱ be the maximum real part of any zero other than $s'_1, \ldots, s'_L$. By Dirichlet's theorem on Diophantine approximation, there exist, for any $\varepsilon > 0$, infinitely many h, all multiples of k, such that

$$|q^{it'_l h} - 1| < \varepsilon$$

for $l = 1, \ldots, L$. For such values of h,

$$|q^{h s_1} + \cdots + q^{h s_{K-1}}| > (1 - \varepsilon) L q^{h\sigma} - (K - 1 - L) q^{h\varrho}.$$

Hence

$$q^{\sigma h} = O(q^{(1-\theta)h}) + O(q^{\varrho h}).$$

Since $\varrho < \sigma$, this implies $\sigma \leqq 1 - \theta$. Finally, by the functional equation (7), if $s \neq 0$ is a zero of $L(f, \chi; s)$ then $1 - s$ is a zero of $L(f, \bar{\chi}; s)$.

It is an interesting consequence of Lemma 1 that any inequality of the form (38) automatically implies a more precise inequality. If

$$S^{(h)}(f, \chi) = O(q^{(1-\theta+\varepsilon)h})$$

for any $\varepsilon > 0$, as $h \to \infty$ through multiples of a fixed integer k, then, by Lemma 1 and (5),

$$|S^{(h)}(f, \chi)| \leqq (K - 1) q^{(1-\theta)h}$$

for all h. Such a state of affairs is familiar in connection with the Riemann zeta-function.

Let k denote the least common multiple of $k_1, \ldots, k_r$. Let $\alpha_1, \ldots, \alpha_K$ denote $\vartheta_1, \ldots, \vartheta_r$ and their conjugates. $\alpha_1, \ldots, \alpha_K$ are all elements of $[q^k]$, and are all different. If $k|h$, $f_i(x)$ splits up into a product of linear factors in $[q^h]$, and we can write

$$(39)\qquad S^{(h)}(f, \chi) = \sum_{\xi \text{ in } [q^h]} \Psi_1(\xi - \alpha_1) \ldots \Psi_K(\xi - \alpha_K),$$

where $\Psi_1, \ldots, \Psi_K$ are characters of $[q^h]$, k_i of them being equal to $\chi_i^{(h)}$ $(i = 1, \ldots, r)$.

From now onwards we consider the sum

$$(40)\qquad S = S(\alpha_1, \ldots, \alpha_K;\ \Psi_1, \ldots, \Psi_K) = \sum_{\xi \text{ in } [Q]} \Psi_1(\xi + \alpha_1) \ldots \Psi_K(\xi + \alpha_K),$$

where $\alpha_1, \ldots, \alpha_K$ are any elements and $\Psi_1, \ldots, \Psi_K$ any characters of an arbitrary finite field $[Q]$. It will be proved in the next two sections that if $\alpha_1, \ldots, \alpha_K$ are all different, and $\Psi_1, \ldots, \Psi_K$ are non-principal, then

$$(41)\qquad S = O(Q^{1-\theta_K})$$

as $Q \to \infty$, where θ_K has the value given in (11).

Suppose for a moment that $\Psi_1 \ldots \Psi_K$ is the principal character and that $\alpha_1, \ldots, \alpha_K$ are different. The change of variable $\xi = -\alpha_K + \frac{1}{\eta}$ in (40) gives

$$(42)\qquad S(\alpha_1, \ldots, \alpha_K;\ \Psi_1, \ldots, \Psi_K) = \varepsilon S(\beta_1, \ldots, \beta_{K-1};\ \Psi_1, \ldots, \Psi_{K-1}) + O(1),$$

where $|\varepsilon| = 1$ and

$$(43)\qquad \beta_i = \frac{1}{\alpha_i - \alpha_K} \qquad (i = 1, \ldots, K-1).$$

Hence any inequality of the form (41) which is valid for all sums with K factors for which $\Psi_1 \ldots \Psi_K$ is the principal character is also valid for all sums with $K - 1$ factors without any such restriction, and conversely.

7. The case $K = 3$.

In this section and the following one, all variables of summation run through $[Q]$, subject to any restrictions explicitly imposed.

We note here for convenience of reference two formulae resulting from linear transformation of the variable. Firstly, from the transformation $\xi = -\alpha_1 + (\alpha_2 - \alpha_1)\eta$ we obtain

(44) $$|S(\alpha_1, \alpha_2, \alpha_3; \Psi_1, \Psi_2, \Psi_3)| = |S(0, 1, \alpha; \Psi_1, \Psi_2, \Psi_3)| + O(1),$$

where

(45) $$\alpha = \frac{\alpha_3 - \alpha_1}{\alpha_2 - \alpha_1}.$$

Secondly, if $\Psi_1 \Psi_2 \Psi_3 \Psi_4$ is the principal character, successive application of (42), (43) and (44), (45) gives

(46) $$|S(\alpha_1, \ldots, \alpha_4; \Psi_1, \ldots, \Psi_4)| = |S(0, 1, \alpha; \Psi_1, \Psi_2, \Psi_3)| + O(1),$$

where

(47) $$\alpha = \frac{(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_4)}{(\alpha_1 - \alpha_2)(\alpha_3 - \alpha_4)}.$$

Lemma 2. *If $\alpha_1, \alpha_2, \alpha_3$ are different elements of $[Q]$, and Ψ_1, Ψ_2, Ψ_3 are non-principal characters of $[Q]$, then*

$$S(\alpha_1, \alpha_2, \alpha_3; \Psi_1, \Psi_2, \Psi_3) = O\left(Q^{\frac{3}{4}}\right).$$

Proof.[1] By (44) it is sufficient to consider $S = S(0, 1, \alpha; \Psi_1, \Psi_2, \Psi_3)$, where $\alpha \neq 0, 1$. We have

$$|S|^2 = \sum_{\xi} \sum_{\eta} \Psi_1(\xi) \overline{\Psi}_1(\eta) \Psi_2(\xi + 1) \overline{\Psi}_2(\eta + 1) \Psi_3(\xi + \alpha) \overline{\Psi}_3(\eta + \alpha).$$

This is unaltered if we impose the condition $\eta \neq 0$. Writing $\xi = \eta \zeta$, we obtain

$$|S|^2 = \sum_{\zeta} \Psi_1(\zeta) \sum_{\eta \neq 0} \Psi_2(\eta \zeta + 1) \overline{\Psi}_2(\eta + 1) \Psi_3(\eta \zeta + \alpha) \overline{\Psi}_3(\eta + \alpha)$$

$$\leq \sum_{\zeta \neq 0} \left| S\left(\frac{1}{\zeta}, 1, \frac{\alpha}{\zeta}, \alpha; \Psi_2, \overline{\Psi}_2, \Psi_3, \overline{\Psi}_3\right) \right| + O(Q).$$

If we impose the condition $\zeta \neq 1, \alpha, \frac{1}{\alpha}$, the elements $\frac{1}{\zeta}, 1, \frac{\alpha}{\zeta}, \alpha$ are all different. Hence, by (46), (47),

$$|S|^2 \leq \sum_{\zeta \neq 0, 1, \alpha, \frac{1}{\alpha}} |S(0, 1, \gamma(\zeta); \Psi_2, \overline{\Psi}_2, \Psi_3)| + O(Q),$$

where

[1] This proof is essentially the same as one given in a previous paper (Journal London Math. Soc. 7 (1932), 117—121).

$$\gamma(\zeta) = \frac{(1-\alpha)^2 \zeta}{\alpha (1-\zeta)^2}.$$

The number of solutions of $\gamma(\zeta) = \gamma$ for given γ is at most 2. Hence

$$|S|^2 \leqq 2 \sum_{\gamma} |S(0, 1, \gamma; \Psi_2, \Psi_2, \Psi_3)| + O(Q)$$

$$\text{(48)} \qquad \leqq 2 \sqrt{Q \sum_{\gamma} |S(0, 1, \gamma; \Psi_2, \overline{\Psi}_2, \Psi_3)|^2} + O(Q),$$

by Cauchy's inequality.

Now

$$\sum_{\gamma} |S(0, 1, \gamma; \Psi_2, \Psi_2, \Psi_3)|^2$$
$$= \sum_{\xi} \sum_{\eta} \Psi_2(\xi) \overline{\Psi}_2(\xi + 1) \Psi_2(\eta) \overline{\Psi}_2(\eta + 1) \sum_{\gamma} \Psi_3(\xi + \gamma) \overline{\Psi}_3(\eta + \gamma).$$

Also, writing $\gamma' = \dfrac{1}{\eta + \gamma}$,

$$\sum_{\gamma} \Psi_3(\xi + \gamma) \overline{\Psi}_3(\eta + \gamma) = \sum_{\gamma' \neq 0} \Psi_3(1 + (\xi - \eta)\gamma').$$

The last sum has the value $Q - 1$ if $\xi = \eta$, and -1 otherwise. Hence

$$\sum_{\gamma} |S(0, 1, \gamma; \Psi_2, \Psi_2, \Psi_3)|^2 = O(Q^2).$$

Substituting in (48) we obtain the result enunciated.

Theorem 3. *If (a) $K = 3$, or (b) $K = 4$ and $\chi_1^{k_1} \dots \chi_r^{k_r} = \chi_0$, the zeros of $L(f, \chi; s)$ (except $s = 0$) satisfy*

$$\frac{1}{4} \leqq \sigma \leqq \frac{3}{4}.$$

This follows from Lemma 2, in virtue of Lemma 1 and the remarks made in § 6.

8. The case $K > 3$.

The proof of (41) in the case $K > 3$ uses quite different ideas from the proof for $K = 3$ just given.[1]

[1] The proof is a refinement and extension of a method previously used in connection with a special case of the problem (see Quarterly Journal of Math. 8 (1937), 308—312).

Let R be any positive integer. For any $\zeta_1, \ldots, \zeta_R$ of $[Q]$ we define

$$T(\zeta_1, \ldots, \zeta_R) = \sum_{\xi_1, \ldots, \xi_R} e(\mathfrak{S}(\zeta_1 \Sigma_1 + \cdots + \zeta_R \Sigma_R)),$$

where $\Sigma_1 = \xi_1 + \cdots + \xi_R, \ldots, \Sigma_R = \xi_1 \ldots \xi_R$ denote the elementary symmetric functions of $\xi_1, \ldots, \xi_R$, and $\mathfrak{S}$ denotes the absolute trace of an element of $[Q]$.

Lemma 3. $\sum_{\zeta_1, \ldots, \zeta_R} | T(\zeta_1, \ldots, \zeta_R)|^2 \leqq R!\, Q^{2R}$.

Proof. The sum is

$$\sum_{\xi_1, \ldots, \xi_R} \sum_{\xi'_1, \ldots, \xi'_R} \sum_{\zeta_1, \ldots, \zeta_R} e\Big(\mathfrak{S}(\zeta_1(\Sigma_1 - \Sigma'_1) + \cdots + \zeta_R(\Sigma_R - \Sigma'_R))\Big),$$

where $\Sigma'_1, \ldots, \Sigma'_R$ denote the elementary symmetric functions of $\xi'_1, \ldots, \xi'_R$. The sum over the ζ's is zero unless $\Sigma_1 = \Sigma'_1, \ldots, \Sigma_R = \Sigma'_R$, i. e. unless $\xi'_1, \ldots, \xi'_R$ are a permutation of $\xi_1, \ldots, \xi_R$. Hence the result.

Lemma 4. *Let $\alpha_1, \ldots, \alpha_K$ be different elements of $[Q]$ and $\Psi_1, \ldots, \Psi_K$ be non-principal characters of $[Q]$, and let S be the sum* (40). *Then*

$$|S|^R \leqq Q^{-\frac{1}{2}K} \sum_{\substack{\eta_1, \ldots, \eta_K \\ \eta_1 \neq 0, \ldots, \eta_K \neq 0}} \left| T\left(\sum_{i=1}^{K} \eta_i \alpha_i^{R-1}, \sum_{i=1}^{K} \eta_i \alpha_i^{R-2}, \ldots, \sum_{i=1}^{K} \eta_i\right)\right|.$$

Proof. We have

$$S^R = \sum_{\xi_1, \ldots, \xi_R} \Psi_1((\xi_1 + \alpha_1) \ldots (\xi_R + \alpha_1)) \ldots \Psi_K((\xi_1 + \alpha_K) \ldots (\xi_R + \alpha_K)).$$

Hence, by (18),

$$S^R = \frac{1}{\tau(\overline{\Psi}_1) \ldots \tau(\overline{\Psi}_K)} \sum_{\eta_1, \ldots, \eta_K} \Psi_1(\eta_1) \ldots \Psi_K(\eta_K) \sum_{\xi_1, \ldots, \xi_R} e\left(\mathfrak{S}(\eta_1(\xi_1 + \alpha_1) \ldots (\xi_R + \alpha_1) + \cdots)\right)$$

$$= \frac{1}{\tau(\overline{\Psi}_1) \ldots \tau(\overline{\Psi}_K)} \sum_{\eta_1, \ldots, \eta_K} \Psi_1(\eta_1) \ldots \Psi_K(\eta_K)\, e\left(\mathfrak{S}\left(\sum_{i=1}^{K} \eta_i \alpha_i^R\right)\right) T\left(\sum_{i=1}^{K} \eta_i \alpha_i^{R-1}, \ldots, \sum_{i=1}^{K} \eta_i\right).$$

Using (17), the result now follows.

Lemma 5. *Suppose that, in addition to the hypotheses of Lemma 4, $\Psi_1 \dots \Psi_K$ is the principal character. Let $\mu_1, \mu_2, \mu_3, \mu_4$ be elements of $[Q]$ satisfying*

$$\mu_1 \mu_4 - \mu_2 \mu_3 = 1, \quad \mu_3 \alpha_i + \mu_4 \neq 0 \qquad (i = 1, \dots, K). \tag{49}$$

Then

$$|S(\alpha_1, \dots, \alpha_K; \Psi_1, \dots, \Psi_K)| = |S(\beta_1, \dots, \beta_K; \Psi_1, \dots, \Psi_K)| + O(1),$$

where

$$\beta_i = \frac{\mu_1 \alpha_i + \mu_2}{\mu_3 \alpha_i + \mu_4} \qquad (i = 1, \dots, K).$$

Proof. By the linear transformation

$$\xi = \frac{\mu_4 \eta + \mu_2}{\mu_3 \eta + \mu_1}.$$

Lemma 6. *Suppose that $K \geqq 5$, and that $\alpha_1, \dots, \alpha_K$ are different elements of $[Q]$. The number of solutions of the $K + 3$ equations*

$$\sum_{i=1}^{K} \eta_i \left(\frac{\mu_1 \alpha_i + \mu_2}{\mu_3 \alpha_i + \mu_4}\right)^j = \sum_{i=1}^{K} \eta_i' \left(\frac{\mu'_1 \alpha_i + \mu'_2}{\mu'_3 \alpha_i + \mu'_4}\right)^j, \qquad j = 0, 1, \dots, K+2, \tag{50}$$

in elements $\eta_1, \dots, \eta_K, \eta'_1, \dots, \eta'_K, \mu_1, \dots, \mu_4, \mu'_1, \dots, \mu'_4$ of $[Q]$ subject to

$$\eta_i \neq 0, \quad \eta_i' \neq 0 \qquad (i = 1, \dots, K)$$

$$\mu_1 \mu_4 - \mu_2 \mu_3 = \mu'_1 \mu'_4 - \mu'_2 \mu'_3 = 1,$$

$$\mu_3 \alpha_i + \mu_4 \neq 0, \quad \mu'_3 \alpha_i + \mu'_4 \neq 0 \qquad (i = 1, \dots, K)$$

is $O(Q^{K+3})$.

Proof. Replacing $\dfrac{\mu'_1 \alpha_i + \mu'_2}{\mu'_3 \alpha_i + \mu'_4}$ by α_i, it is sufficient to prove that the number of solutions of

$$\sum_{i=1}^{K} \eta_i \left(\frac{\mu_1 \alpha_i + \mu_2}{\mu_3 \alpha_i + \mu_4}\right)^j = \sum_{i=1}^{K} \eta_i' \alpha_i^j, \qquad j = 0, \dots, K + 2, \tag{51}$$

subject to the other conditions is $O(Q^K)$. For there are $O(Q^3)$ possible sets of values for $\mu'_1, \mu'_2, \mu'_3, \mu'_4$.

Suppose first that $\mu_1, \mu_2, \mu_3, \mu_4$ are such that the two sets

$$\alpha_1, \dots, \alpha_K; \quad \frac{\mu_1 \alpha_1 + \mu_2}{\mu_3 \alpha_1 + \mu_4}, \dots, \frac{\mu_1 \alpha_K + \mu_2}{\mu_3 \alpha_K + \mu_4} \tag{52}$$

have at most two common elements. Then, since $K \geqq 5$, there exist suffixes i_1, i_2, i_3 such that

$$(53) \qquad \frac{\mu_1 \alpha_{i_1} + \mu_2}{\mu_3 \alpha_{i_1} + \mu_4}, \quad \frac{\mu_1 \alpha_{i_2} + \mu_2}{\mu_3 \alpha_{i_2} + \mu_4}, \quad \frac{\mu_1 \alpha_{i_3} + \mu_2}{\mu_3 \alpha_{i_3} + \mu_4}$$

are different from all of $\alpha_1, \ldots, \alpha_K$. Consider the equations (51) as $K + 3$ linear equations for $\eta'_1, \ldots, \eta'_K, \eta_{i_1}, \eta_{i_2}, \eta_{i_3}$ in terms of the remaining $K - 3$ η's. The determinant of these equations is not zero, since $\alpha_1, \ldots, \alpha_K$ and the numbers (53) are all different. Hence, for given $\mu_1, \mu_2, \mu_3, \mu_4$ of the above kind, the number of solutions of (51) in $\eta_1, \ldots, \eta_K, \eta'_1, \ldots, \eta'_K$ is $O(Q^{K-3})$. Also there are at most $O(Q^3)$ values for $\mu_1, \mu_2, \mu_3, \mu_4$.

Suppose now that $\mu_1, \mu_2, \mu_3, \mu_4$ are such that the two sets (52) have at least three common elements, say, without loss of generality,

$$(54) \qquad \frac{\mu_1 \alpha_1 + \mu_2}{\mu_3 \alpha_1 + \mu_4} = \beta_1, \quad \frac{\mu_1 \alpha_2 + \mu_2}{\mu_3 \alpha_2 + \mu_4} = \beta_2, \quad \frac{\mu_1 \alpha_3 + \mu_2}{\mu_3 \alpha_3 + \mu_4} = \beta_3.$$

Here $\beta_1, \beta_2, \beta_3$ are three of $\alpha_1, \ldots, \alpha_K$, necessarily different. The number of possibilities for $\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2, \beta_3$ is $O(1)$. Given the values of these, there are only $O(1)$ possibilities for $\mu_1, \mu_2, \mu_3, \mu_4$ to satisfy (54) and $\mu_1 \mu_4 - \mu_2 \mu_3 = 1$. For if this is not so, the linear equations

$$\mu_1 \alpha_1 + \mu_2 - \mu_3 \alpha_1 \beta_1 - \mu_4 \beta_1 = 0,$$
$$\mu_1 \alpha_2 + \mu_2 - \mu_3 \alpha_2 \beta_2 - \mu_4 \beta_2 = 0,$$
$$\mu_1 \alpha_3 + \mu_2 - \mu_3 \alpha_3 \beta_3 - \mu_4 \beta_3 = 0$$

are not independent, i. e. there exist A, B, C not all zero such that

$$A + B + C = 0,$$
$$A \alpha_1 + B \alpha_2 + C \alpha_3 = 0,$$
$$A \beta_1 + B \beta_2 + C \beta_3 = 0,$$
$$A \alpha_1 \beta_1 + B \alpha_2 \beta_2 + C \alpha_3 \beta_3 = 0.$$

Suppose, e. g., that $A \neq 0$. We have

$$A(\alpha_1 - \alpha_3) + B(\alpha_2 - \alpha_3) = 0,$$
$$A \beta_1 (\alpha_1 - \alpha_3) + B \beta_2 (\alpha_2 - \alpha_3) = 0,$$

whence

$$A(\beta_1 - \beta_2)(\alpha_1 - \alpha_3) = 0,$$

which is a contradiction.

Hence there are at most $O(1)$ sets of $\mu_1, \mu_2, \mu_3, \mu_4$ such that the two sets (52) have at least three common elements. Given the μ's, the first K of the equations (51) determine $\eta_1, \ldots, \eta_K$ uniquely in terms of $\eta'_1, \ldots, \eta'_K$, and so in this case we again obtain only $O(Q^K)$ solutions for (51).

Lemma 7. *If $K \geqq 5$, and $\alpha_1, \ldots, \alpha_K$ are different elements of $[Q]$, and $\Psi_1, \ldots, \Psi_K$ are non-principal characters of $[Q]$ such that $\Psi_1 \cdots \Psi_K$ is the principal character, then*

$$S = S(\alpha_1, \ldots, \alpha_K; \Psi_1, \ldots, \Psi_K) = O\left(Q^{1-\frac{3}{2(K+3)}}\right).$$

Proof. Choose $R = K + 3$. Let $\mu_1, \mu_2, \mu_3, \mu_4$ be any elements of $[Q]$ satisfying (49). By Lemmas 4, 5,

$$|S + O(1)|^R \leqq Q^{-\frac{1}{2}K} \sum_{\substack{\eta_1, \ldots, \eta_K \\ \eta_1 \neq 0, \ldots, \eta_K \neq 0}} \left| T\left(\sum_{i=1}^{K} \eta_i \left(\frac{\mu_1 \alpha_i + \mu_2}{\mu_3 \alpha_i + \mu_4}\right)^{K+2}, \ldots, \sum_{i=1}^{K} \eta_i\right)\right|.$$

Summing over all $\mu_1, \mu_2, \mu_3, \mu_4$ satisfying (49), we obtain

$$Q^3 |S + O(1)|^{K+3} = O\left(Q^{-\frac{1}{2}K} \sum_{\zeta_0, \ldots, \zeta_{K+2}} P(\zeta_{K+2}, \ldots, \zeta_0) |T(\zeta_{K+2}, \ldots, \zeta_0)|\right), \tag{55}$$

where $P(\zeta_{K+2}, \ldots, \zeta_0)$ denotes the number of solutions of the $K+3$ equations

$$\sum_{i=1}^{K} \eta_i \left(\frac{\mu_1 \alpha_i + \mu_2}{\mu_3 \alpha_i + \mu_4}\right)^j = \zeta_j, \qquad j = 0, 1, \ldots, K+2,$$

in $\eta_1, \ldots, \eta_K, \mu_1, \mu_2, \mu_3, \mu_4$ satisfying $\eta_i \neq 0$ and (49).

Now

$$\sum_{\zeta_{K+2}, \ldots, \zeta_0} (P(\zeta_{K+2}, \ldots, \zeta_0))^2$$

is precisely the number of solutions of (50) as defined in Lemma 6. Hence

$$\sum_{\zeta_{K+2}, \ldots, \zeta_0} (P(\zeta_{K+2}, \ldots, \zeta_0))^2 = O(Q^{K+3}). \tag{56}$$

By (55), (56), Lemma 3, and Cauchy's inequality,

$$Q^3 | S + O(1)|^{K+3} = O\left(Q^{-\frac{1}{2}K} \sqrt{Q^{K+3}}\, Q^{2(K+3)}\right)$$
$$= O\left(Q^{K+3+\frac{3}{2}}\right),$$

whence the result.

Theorem 4. *Let* $\theta_K = \frac{3}{2(K+4)}$. *If* (*a*) $K \geqq 4$, *or* (*b*) $K \geqq 5$ *and* $\chi_1^{k_1} \ldots \chi_r^{k_r} = \chi_0$, *the zeros of* $L(f, \chi; s)$ (*except* $s = 0$) *satisfy*

$$\theta_K \leqq \sigma \leqq 1 - \theta_K \qquad \textit{in case } (a),$$

and

$$\theta_{K-1} \leqq \sigma \leqq 1 - \theta_{K-1} \qquad \textit{in case } (b).$$

This follows from Lemma 7, in virtue of Lemma 1 and the remarks made in § 6.

9. The Distribution of Power-residues (mod p).

Let p be an odd prime, and let $\chi_1, \ldots, \chi_n$ be any non-principal characters (mod p). Denote their orders by $l_1, \ldots, l_n$. Let $\varepsilon_1, \ldots, \varepsilon_n$ be any set of n roots of unity, ε_i being an l_i-th root of unity. Let $E(\varepsilon_1, \ldots, \varepsilon_n)$ denote the number of sequences

$$x + 1,\ x + 2,\ \ldots,\ x + n$$

out of $1, 2, \ldots, p - 1$ for which

$$\chi_1(x + 1) = \varepsilon_1, \ \ldots, \ \chi_n(x + n) = \varepsilon_n. \tag{57}$$

Theorem 5. $\left| E(\varepsilon_1, \ldots, \varepsilon_n) - \frac{p}{l_1 \ldots l_n} \right| < n\left(p^{1-\theta_n} + 1\right)$, *where*

$$\theta_3 = \frac{1}{4}, \quad \theta_n = \frac{3}{2(n+4)} \qquad (n \geqq 4).$$

Proof. The expression

$$1 + \varepsilon_i^{-1}\chi_i(x) + \varepsilon_i^{-2}\chi_i^2(x) + \cdots + \varepsilon_i^{-(l_i-1)}\chi_i^{l_i-1}(x)$$

has the value l_i if $\chi_i(x) = \varepsilon_i$ and zero otherwise (for $x \not\equiv 0$). Hence

$$E(\varepsilon_1, \ldots, \varepsilon_n) = \frac{1}{l_1 \ldots l_n} \sum_{x=0}^{p-n-1} \prod_{i=1}^{n} \left\{1 + \varepsilon_i^{-1}\chi_i(x + i) + \cdots + \varepsilon_i^{-(l_i-1)}\chi_i^{l_i-1}(x + i)\right\}.$$

The error made in replacing the summation by one over a complete set of residues (mod p) does not exceed n in absolute value. On expanding the product, the right hand side then consists of $l_1 \ldots l_n$ sums. One of these has summand 1, the others are character sums of the form

$$\sum_{x=0}^{p-1} \chi'_1(x+i_1) \ldots \chi'_r(x+i_r),$$

with non-principal $\chi'_1, \ldots, \chi'_r$ where $1 \leqq r \leqq n$. The sums for which $r=1$ vanish, and those for which $r=2$ have absolute value $\leqq \sqrt{p} < np^{1-\theta_n}$. By (13), the absolute value of a sum with $3 \leqq r \leqq n$ does not exceed $(r-1)p^{1-\theta_r} < np^{1-\theta_n}$, where θ_n is given by (11). Hence the result.

Corollary. If $n \geqq 4$ *and* $p > (nl_1 \ldots l_n + 1)^{\frac{2(n+4)}{3}}$, *there exists a sequence* $x+1, \ldots, x+n$ *satisfying* (57).

For then

$$\begin{aligned} p^{\theta_n} &> nl_1 \ldots l_n + 1 \\ &> nl_1 \ldots l_n(1 + p^{-\theta_n}) \\ &> nl_1 \ldots l_n(1 + p^{-1+\theta_n}), \end{aligned}$$

whence

$$n(p^{1-\theta_n} + 1) < \frac{p}{l_1 \ldots l_n}.$$

In the particular case of quadratic residues ($l_1 = \cdots = l_n = 2$), the result of Theorem 5 can be improved upon by the use of various devices.[1] Using the theorem of Hasse, θ_n can be replaced by $\frac{1}{2}$ for $n = 4, 5$, and using the result of this paper, θ_n can be replaced by

$$\frac{3}{2(2n'+3)} \quad \text{for} \quad n = 2n',\ 2n'+1.$$

The University, Manchester.

[1] See Davenport, Journal London Math. Soc. 8 (1933), 46—52.