[5] J. P. Mc Carthy, *The probability that* $(n, f(n))$ *is r-free*, Amer. Math. Monthly 67 (1960), S. 368–369.

[6] H. Niederreiter, *On a class of sequences of lattice points*, J. Number Theory 4 (1972), S. 477–502.

[7] G. L. Watson, *On integers n relatively prime to* $[an]$, Canad. J. Math. 5 (1953), S. 451–455.

[8] H. Weyl, *Über die Gleichverteilung von Zahlen mod. Eins*, Math. Ann. 77 (1916), S. 313–352.

INSTITUT FÜR MATHEMATIK
MONTANUNIVERSITÄT LEOBEN
Leoben, Austria

Eingegangen am 26. 8. 1976
und in revidierter Form am 3. 2. 1977 (872)

ACTA ARITHMETICA
XXXV (1979)

Remarks on Hua's estimate of complete trigonometrical sums

by

O. Körner and H. Stähle (Ulm)

1. Introduction. We are concerned with trigonometrical sums of the form

$$S_f(q) = \sum_{a \bmod q} e^{2\pi i f(a)/q},$$

where q is an integer > 1 and $f(x) = a_k x^k + a_{k-1} x^{k-1} + \ldots + a_0$ is a polynomial with integral coefficients such that $(a_1, \ldots, a_k, q) = 1$.

Many problems in analytical number theory (e.g. Waring's problem extended to polynomial values) make it desirable to have precise estimates of $S_f(q)$ for large q. Since $S_f(q) = 0$ for $k = 1$, and since the case $k = 2$ can be settled by the theory of Gaussian sums, it is supposed in the sequel that $k \geqslant 3$.

For the special polynomial $f(x) = x^k$ Hardy and Littlewood [2] proved among other things that

$$|S_f(q)| \leqslant c(k) q^{1-1/k} \tag{1}$$

with a positive constant $c(k)$ depending only on k. Furthermore their results show that the estimate (1) is best possible except for the constant $c(k)$, if there is no restriction for q; namely for each k there exist infinitely many q with $S_f(q) = q^{1-1/k}$. The question arises whether (1) remains true for general f. It will be shown that an affirmative answer to this question can be given by means of the methods of Hua [3]–[6], e.g. in this way it is easy to see that (1) still holds with $c(k) = \exp(3^k)$ in the case $k > 8$. This estimate can be improved slightly. More precisely, for general f with $k \geqslant 3$ we shall deduce the following

Theorem 1. *We have*

$$|S_f(q)| \leqslant [k(k-1)]^{v(q,k)} q^{1-1/k},$$

where $v(q, k)$ *denotes the number of all primes* p *with* $p \mid q$ *and* $p < \max\{2^k, (k-1)^{2k/(k-2)}\}$.

The proof rests essentially on Hua's inductive procedure [3] by which

he proved that

$$|S_f(q)| \leqslant k^{3\tau(q)} q^{1-1/k}, \tag{2}$$

where $\tau(q)$ denotes the number of all prime divisors of q; and we start the induction with the deep estimate of Weil–Carlitz–Uchiyama [1]:

$$|S_f(q)| \leqslant (k-1)\sqrt{q}, \tag{3}$$

if q is a prime.

For q's with certain arithmetical properties Theorem 1 can be considerably improved. One example for this statement is already (3), another one is provided by

THEOREM 2. *If $q = p^l$ with a prime p and an integer $l \geqslant 2$, then*

$$|S_f(q)| \leqslant k(k-1)q^{1-s},$$

where $s = \max\{1/l, 1/k\}$.

If no special assumptions are made on f and k, Theorem 2 is sharp except for the factor $k(k-1)$, since Hardy and Littlewood [2] obtained $S_f(q) = q^{1-s}$ for $f(x) = x^k$, $q = p^l$, $2 \leqslant l \leqslant k$, p a prime with $p \nmid k$. The proof of Theorem 2 is almost identical with Hua's proof of (2), in particular independent of (3).

Hua generalized (2) for trigonometrical sums over algebraic number fields [4]. Improvements of that result are immediately obtained by the corresponding generalizations of Theorem 1 and 2 (see Theorems 3 and 4) whose proofs will be sketched in the last section of this paper.

More precise estimates than those of Theorem 2 are to be expected in some cases, if certain arithmetical properties of f and q are taken into account simultaneously. Results of this kind were mentioned by Hua [5], for instance that $|S_f(q)| \leqslant e(k)q^{1-1/(w+1)}$, if $q = p^l$, $l \geqslant 2$, p is a prime and w the maximum of the multiplicities of all zeros of $p^{-t}f'(x)$ modulo p, where t is defined by $p^t \| f'(x)$. But this route will not be pursued any further in this paper.

2. Notations. We put $e(x) = e^{2\pi i x}$. By $\sum_{a \bmod q}$ we mean summation over any complete residue system modulo q. The pair q, f is always the one defined in the introduction, except in the last section of this paper. By p we denote always a prime. For an integer v and a polynomial $g(x) = b_n x^n + b_{n-1}x^{n-1} + \ldots + b_0$ with integral coefficients the symbol $p^v \| g(x)$ stands for the two conditions $p^v | (b_0, \ldots, b_n)$, $p^{v+1} \nmid (b_0, \ldots, b_n)$. Let M be a non-negative integer. A zero z of $g(x)$ modulo p of multiplicity M is defined to be an integer such that $g(x) \equiv (x-z)^M h(x) \bmod p$ for some polynomial $h(x)$ with integral coefficients and $h(z) \not\equiv 0 \bmod p$.

3. Proofs of the Theorems 1 and 2. We use the following two lemmas of Hua [3]:

LEMMA 1. *If μ is an integer and $h(x)$ a polynomial with integral coefficients and*

$$p^0 \| \{h(x) - h(0)\} \quad \text{and} \quad p^v \| \{h(px+\mu) - h(\mu)\},$$

then $1 \leqslant v \leqslant$ degree of h.

LEMMA 2. *If $h(x)$ is a polynomial with integral coefficients and b a zero of $h(x)$ modulo p of multiplicity M, and if $p^u \| h(px+b)$, then the number of all zeros of $p^{-u}h(px+b)$ modulo p, counted modulo p with their multiplicities, does not exceed M.*

First we shall prove Theorem 2, i.e. we consider the case $q = p^l$. We define t by the condition $p^t \| f'(x)$. Consequently $p^t | (a_1, 2a_2, \ldots, ka_k)$, and combining this with $(a_1, \ldots, a_k, p) = 1$, we obtain

$$p^t \leqslant k. \tag{4}$$

Let $\mu_1, \ldots, \mu_r$ be the different zeros modulo p of the polynomial $p^{-t}f'(x)$ modulo p, and let $m_1, \ldots, m_r$ be their multiplicities. Putting $m = m(f) = m_1 + \ldots + m_r$, one has obviously

$$0 \leqslant m \leqslant k-1. \tag{5}$$

If we define σ_j by $p^{\sigma_j} \| \{f(px+\mu_j) - f(\mu_j)\}$, then Lemma 1 implies

$$1 \leqslant \sigma_j \leqslant k \quad (j = 1, \ldots, k). \tag{6}$$

Because of (5), Theorem 2 is contained in the following

LEMMA 3. *We have*

$$|S_f(p^l)| \leqslant \begin{cases} kp^{1-1/k} & \text{for} \quad l = 1, \\ k\max\{1, m\}p^{l(1-s)} & \text{for} \quad l \geqslant 2. \end{cases}$$

Proof. The assertion is proved by induction on l. The case $l = 1$ is contained in (3), but can also be settled by the elementary method of Mordell [8], [3]. For $l > 1$ we distinguish two cases:

(a) First let $l > 2t+1$. Then we use the obvious identity

$$S_f(p^l) = \sum_{\mu \bmod p} S_\mu \tag{7}$$

with

$$S_\mu = \sum_{a \bmod p^{l-1}} e\left(\frac{f(\mu + pa)}{p^l}\right) = \sum_{\substack{y \bmod p^{l-t-1} \\ y \equiv \mu \bmod p}} \sum_{z \bmod p^{t+1}} e\left(\frac{f(y + p^{l-t-1}z)}{p^l}\right). \tag{8}$$

We state the trivial estimate

$$|S_\mu| \leqslant p^{l-1} \quad \text{for all integers } \mu. \tag{9}$$

On the other hand, the binomial expansion of each term of $f(y + p^{l-t-1}z)$ in conjunction with the estimate $j(l-t-1) \geqslant l$ for $j \geqslant 2$ yields the con-

gruence

$$f(y+p^{l-t-1}z) \equiv f(y)+f'(y)p^{l-t-1}z \bmod p^l.$$

This shows that if $\mu \not\equiv \mu_j$ for $j = 1, \ldots, r$, then the last sum in (8) vanishes, hence by (7) we have

$$S_f(p^l) = \sum_{j=1}^{r} S_{\mu_j}. \tag{10}$$

If $l \leqslant k$, then by (10) and (9) we get

$$|S_f(p^l)| \leqslant rp^{l-1} \leqslant mp^{l(1-s)},$$

i.e. the assertion. Now let $l > k$, hence $l > \sigma_j$ $(1 \leqslant j \leqslant r)$ by (6). With the abbreviation

$$g_j(x) = p^{-\sigma_j}\{f(px+\mu_j)-f(\mu_j)\}$$

(8) implies

$$S_{\mu_j} = p^{\sigma_j-1}e\left(\frac{f(\mu_j)}{p^l}\right)S_{g_j}(p^{l-\sigma_j}). \tag{11}$$

Observing that by Lemma 2 (applied to $h(x) = p^{-t}f'(x)$ and $b = \mu_j$) $m(g_j) \leqslant m_j$, we obtain by the induction hypothesis on $S_{g_j}(p^{l-\sigma_j})$ that

$$|S_{\mu_j}| \leqslant km_j p^{\sigma_j-1+(l-\sigma_j)(1-1/k)} \leqslant km_j p^{l(1-1/k)}$$

in view of (6). Therefore (10) yields the assertion.

(b) Secondly, let $2 \leqslant l \leqslant 2t+1$. Then $t \geqslant 1$, hence $p \leqslant k$ by (4) and

$$|S_f(p^l)|/p^{l(1-s)} \leqslant p^{ls} \leqslant p^{\max(1,(2t+1)/k)} \leqslant \max\{k, k^{(2+1/t)/k}\} \leqslant k. \quad \blacksquare$$

As for Theorem 1, we reduce its proof first in a well-known manner to the case where q is a power of a prime. Namely, if $q = p_1^{l_1} \ldots p_d^{l_d}$ is the decomposition of q into powers of different primes with natural exponents, put $q_\nu = qp_\nu^{-l_\nu}$ $(\nu = 1, \ldots, d)$. Then $a = a_1q_1 + \ldots + a_dq_d$ represents a complete residue system modulo q, when each a_ν runs over a complete residue system modulo $p_\nu^{l_\nu}$. Inserting this in $S_f(q)$ yields

$$|S_f(q)| = |S_{f_1}(p_1^{l_1}) \ldots S_{f_d}(p_d^{l_d})|,$$

where $f_\nu(x) = \{f(q_\nu x)-a_0\}/q_\nu$. This formula and Lemma 3 show that the proof of Theorem 1 is complete, if we prove

LEMMA 4. *For all positive integers l and primes p with $p \mid q$ and $p \geqslant \max\{2^k, (k-1)^{2k/(k-2)}\}$ the estimate*

$$|S_f(p^l)| \leqslant p^{l(1-1/k)}$$

holds.

Proof. Using the notations of the proof of Lemma 3, we observe that $t = 0$ because of (4) and $p \geqslant 2^k > k$. Put $\sigma = \max\{\sigma_1, \ldots, \sigma_r\}$, then

$$r \leqslant k+1-\sigma, \tag{12}$$

since on the one hand side we have

$$r \leqslant k-w$$

with $w = \max\{m_1, \ldots, m_r\}$ because of $w+r-1 \leqslant m \leqslant k-1$; and on the other hand side the condition

$$p^{\sigma_j} \Big\| \sum_{\varrho=1}^{k} \frac{f^{(\varrho)}(\mu_j)}{\varrho!}p^\varrho x^\varrho \qquad (j = 1, \ldots, r)$$

shows that $f^{(\varrho)}(\mu_j) \equiv 0 \bmod p$ for $1 \leqslant \varrho \leqslant \sigma_j-1$, hence $m_j \geqslant \sigma_j-1$ hence $w \geqslant \sigma-1$. Now we prove Lemma 4 by induction on l. The starting point $l = 1$ is clear by (3) because of $p \geqslant (k-1)^{2k/(k-2)}$. Let $l > 1$, then we are in the case (a) of the proof of Lemma 3. If $l \leqslant \sigma$, then by (10), (9), (12) and (6) we infer that

$$|S_f(p^l)|/p^{l(1-1/k)} \leqslant rp^{-1+l/k} \leqslant rp^{-1+\sigma/k} \leqslant (k-\sigma+1)2^{\sigma-k} \leqslant 1$$

because of $p \geqslant 2^k$. If $l > \sigma$, then we apply the induction hypothesis to $S_{g_j}(p^{l-\sigma_j})$ in (11), and we conclude from (10) that

$$|S_f(p^l)|/p^{l(1-1/k)} \leqslant \sum_{j=1}^{r} p^{-1+\sigma_j/k} \leqslant rp^{-1+\sigma/k},$$

which as before turns out to be $\leqslant 1$. $\blacksquare$

4. Extensions to algebraic number fields. Let K be an algebraic number field of degree $n > 1$ over the field Q of all rational numbers. Let I be the ring of integers of K and D be the different of K. For analytical investigations in K the trigonometrical sums

$$S_f(A, g) = \sum_{a \bmod A} E\big(f(a)g\big)$$

are as useful as the sums of the previous sections with respect to Q (e.g. see [7]). Here A is a non-zero ideal of I, and $f(x) = a_kx^k + a_{k-1}x^{k-1} + \ldots + a_0$ is a polynomial with coefficients in I such that $(a_1, \ldots, a_k, A) = I$, and g is any number in K with $gDA + A = I$; and $E(x) = e\big(T(x)\big)$, where T denotes the trace $K \to Q$.

Let $N(A)$ be the norm of A. Again it may be supposed that $k \geqslant 3$. In order to generalize Theorem 1 and 2 to $S_f(A, g)$, we first prove the following analogue of (3):

LEMMA 5. *If A is a prime ideal of I, then*

$$|S_f(A, g)| \leqslant k^{n/2}\sqrt{N(A)}.$$

Proof. For $a \in I$ let $\bar{a}$ be the residue class of a modulo A, i.e. an element of the finite field I/A. Let p be the characteristic of this field. Then $\bar{a} \mapsto E(ag)$ defines a character of the additive group I/A. Consequently there exists a $b \in I$ such that

$$E(ag) = e\left(\frac{\tau(\overline{ab})}{p}\right) \quad \text{for all } a \in I,$$

where τ denotes the trace of I/A into the ring of rational integers modulo p. Therefore, with the abbreviation $F(x) = \overline{ba}_k x^k + \overline{ba}_{k-1}x^{k-1} + \ldots + \overline{ba}_0$, it follows that

$$S_f(A, g) = \sum_{c \in I/A} e\left(\frac{\tau(F(c))}{p}\right).$$

For the latter sum Carlitz and Uchiyama [1] proved that it is in absolute value $\leqslant (k-1)\sqrt{N(A)}$, provided that $p > k$. But, if $p \leqslant k$, then obviously

$$|S_f(A, g)| \leqslant N(A) \leqslant p^{n/2}\sqrt{N(A)} \leqslant k^{n/2}\sqrt{N(A)}. \blacksquare$$

The Lemmas 1 and 2 immediately extend to K as was shown by Hua [4] who also generalized to K the method of proof used for Lemma 3 and 4. Using that generalization we can easily translate the proofs of the Lemmas 3 and 4 to K, and thus we obtain the following generalizations of the Theorems 1 and 2 (note that (4) is merely replaced by $N(P)^l \leqslant k^n$):

THEOREM 3. *We have*

$$|S_f(A, g)| \leqslant [k^n(k-1)]^{v(A,k,K)}[N(A)]^{1-1/k},$$

where $v(A, k, K)$ denotes the number of all prime ideals P of I with $P|A$ and $N(P) < \max\{2^k, k^{nk/(k-2)}\}$.

THEOREM 4. *If $A = P^l$ with a prime ideal P of I and a rational integer $l \geqslant 2$, then*

$$|S_f(A, g)| \leqslant k^n(k-1)\,[N(A)]^{1-s}$$

with $s = \max\{1/l, 1/k\}$.

References

[1] L. Carlitz and S. Uchiyama, *Bounds for exponential sums*, Duke Math. J. 24 (1957), pp. 37–41.

[2] G. H. Hardy and J. E. Littlewood, *Some problems of 'Partitio Numerorum', IV, The singular series in Waring's problem and the value of the number $G(k)$*, Math. Zeitschr. (1922), pp. 161–188.

[3] L. K. Hua, *Additive Primzahltheorie*, B. G. Teubner Verlagges, Leipzig 1959.

[4] — *On exponential sums over an algebraic number field*, Canad. J. Math. 3 (1951), pp. 44–51.

[5] — *Die Abschätzung von Exponentialsummen und ihre Anwendung in der Zahlentheorie*, Enzykl. d. Math. Wiss. Bd I2 (1959), Heft 13, Teil I.

[6] — *On exponential sums*, Sci. Record (N.S.) 1 (1957), pp. 1–4.

[7] O. Körner, *Über Mittelwerte trigonometrischer Summen und ihre Anwendung in algebraischen Zahlkörpern*, Math. Ann. 147 (1962), pp. 205–239.

[8] L. J. Mordell, *On a sum analogous to a Gauss's sum*, Quart. J. Oxford 3 (1932), pp. 161–167.

ABTEILUNG FÜR MATHEMATIK IV
UNIVERSITÄT ULM
W. Germany

Received on 27. 10. 1976
and in revised form on 16. 4. 1977 (886)