ON AN EXPONENTIAL SUM

BY LOO-KENG HUA (華羅庚)

The main object of this paper is to prove the following theorem·

Let $f(x)$ be a polynomial of the k-th degree with integer coefficients.

$$f(x) = a_k x^k + \cdots + a_1 x$$

and let $(a_k, \cdots, a_1, q) = 1$. Then

$$S(q, f(x)) = \sum_{x=1}^{q} e_q(f(x)) = O(q^{1-1/k+\varepsilon}), e_q(z) = e^{2\pi i z/q},$$

where the constant implied by the symbol O depends only on k and ε.

This result is better than my previous one(1) in which the constant implied by O depends also on the coefficients of the polynomial.

In §§3,4 some easy applications of the theorem will be given. Another application of the theorem to a problem studied by Vinogradow will be given elsewhere.

§1. The theorem is a deduction of the following lemma:

MAIN LEMMA. *Let $l > 1$ and p be a prime, and let*

$$f(x) = a_k x^k + \cdots + a_1 x$$

and $p \nmid (a_1, \cdots, a_k)$. *Then*

$$S(p^l, f(x)) = O(p^{l(1-1/k)}),$$

---

(1) *Jour. of London Math. Soc.* 13 (1938), 54-61.

(2) *Quarterly Jour.* 3 (1932), 161-167.

where the constant implied by the symbol O depends on k only.

The proof of the lemma will be given in the next section.

LEMMA 1 (*Mordell*).

$$S(p, f(x)) = O(p^{1-1/k}).$$

LEMMA 2. *If* $(q_1, q_2) = 1$ *and* $f(o) = 0$, *then*

$$S(q_1 q_2, f(x)) = S(q_1, f(q_2 x)/q_2) S(q_2, f(q_1 x)/q_1)$$

Proof. Writing $x = q_1 y + q_2 z$, then as y and z run over the complete sets of residue systems mod q_1 and mod q_2 respectively, x runs over a complete set of residue system, mod $q_1 \; q_2$. Further we have evidently

$$e_{q_1 q_2}(f(q_1 y + q_2 z)) = q_1(f(e_{q_1} z)/q_2) e_{q_2}(f(q_1 z)/q_1).$$

Thus

$$S(q_1 q_2, f(x)) = \sum_{x=o}^{q_1 q_2 - 1} e_{q_1 q_2}(f(x)) = \sum_{y=o}^{q_2-1} e_{q_2}(f(q_1 y)/q_1) \sum_{z=o}^{q_1-1} e_{q_1}(f(q_2 z)/q_2)$$

$$= S(q_1, f(q_2 x)/q_2) S(q_2, f(q_1 x)/q_1).$$

THEOREM 1. *If* $(a_1, \cdots, a_k, q) = 1$, *then we have*

$$S(q, f(x)) = O(q^{1-1/k+\varepsilon}).$$

Proof. By the main lemma and the lemmas 1 and 2, we have

$$|S(q_1 f(x))| \leqq (c(k))^{\nu(q)} q^{1-\frac{1}{k}},$$

where $\nu(q)$ is the number of distinct prime factors of q. Since

$$c(k)^{\nu(q)} = O(q^{\varepsilon}),$$

the theorem is proved.

§2. DEFINITION. *Let*

$$f(x) = a_k x^k + \cdots + a_1 x$$

$p^{l_s} \| s a_s$, $t = \text{Min}\ (l_1, \cdots, l_k)$, $t \geq 0$. *Let s be the greatest integer such* *that* $p^t \| sa_s$. *This integer is then defined to be the index of* $f(x)$, *and we write* $s = \text{ind } f(x)$. *Immediately we have the following lemmas:*

LEMMA 1. $\text{ind } f(x) = \text{ind } f(x+\lambda)$.

LEMMA 2. $\text{ind } f(x) \geqq \text{ind } f(px)$.

LEMMA 3. *If* $\text{ind } f(x) = \text{ind } f(px)$, then

$$f'(x) \equiv 0 \pmod{p^{t+1}}$$

implies $p \mid x$.

Proof. By definition $l_s \leqq l_{s'}$, for any s', and also $l_s + s \leqq l_{s'} + s'$. Therefore

$$l_s < l_{s'} \qquad \text{for } s \neq s';$$

in fact, if $s < s'$, the result is a trivial consequence of the definition, while if $s > s'$, then $l_s \leqq l_{s'} + s' - s < l_{s'}$. Thus $f'(x) \equiv 0 \pmod{p^{t+1}}$ implies

$$sa_s x^{s-1} \equiv 0 \pmod{p^{t+1}},$$

i.e. $p \mid x$.

Proof of the main lemma. The lemma is immediate for $l \leqq t+1$, since

$$|S(p^l, f(x))| \leqq p^l \leqq p^{t+1} \leqq p^{2t} \leqq k^2, \text{ for } t > 0,$$

and, by a result due to Mordell

$$S(p, f(x)) = 0(p^{1-1/k}) \qquad \text{for } t = 0.$$

Therefore we may assume that $l \geqq t+2$. Let

$$\lambda_1, \cdots, \lambda_e$$

be the distinct roots of the congruence

$$f'(x) \equiv 0 \pmod{p^{t+1}}.$$

Then evidently $e \leqq p^t k \leqq k^2$, and

$$\sum_{x=1}^{p^l} e_{p^l}(f(x)) = \sum_{i=1}^{p^{t+1}} \sum_{\substack{x=1 \\ x \equiv i \ (p^{t+1})}}^{p^l} e_{p^l}(f(x)).$$

If i is not equal to any one of the λ's, then, letting $x = y + p^{l-t-1} z$, we have

$$\sum_{\substack{x=1 \\ x \equiv i,\ (p^{t+1})}}^{p^l} e_{p^l}(f(x)) = \sum_{\substack{y=1 \\ y \equiv i,\ (p^{t+1})}}^{p^{l-t-1}} e_{p^l}(f(y)) \sum_{\substack{z=1 \\ f'(y) \equiv 0,\ (p^{t+1})}}^{p^{t+1}} e_{p^{t+1}}(z f'(y)) = 0.$$

Therefore

$$\left| \sum_{x=1}^{p^l} e_{p^l}(f(x)) \right| = \left| \sum_{i=1}^{e} \sum_{\substack{x=1 \\ x \equiv \lambda_i,\ (p^{t+1})}}^{p^l} e_{p^l}(f(x)) \right|$$

$$\leqq e \operatorname*{Max}_{1 \leq i \leq e} \left| \sum_{y=1}^{p^{l-t-1}} e_{p^l}(f(\lambda_i + p^{t+1} y) - f(\lambda_i)) \right|$$

$$\leqq e \operatorname*{Max}_{1 \leq i \leq e} \left| \sum_{x=1}^{p^{l-t-1}} e_{p^{l-\mu_i}}(g_i(x)) \right|,$$

where p^{μ_i} is the highest power of p which divides all the coefficients of $f(\lambda_i + p^{t+1} y) - f(\lambda_i)$. Therefore

$$\left| \sum_{x=1}^{p^l} e_{p^l}(f(x)) \right| \leq e \operatorname*{Max}_{1 \leq i \leq e} p^{\mu_i - t - 1} \left| \sum_{x=1}^{p^{l-\mu_i}} e_{p^{l-\mu_i}}(g_i(x)) \right|$$

$$\leq k^2 \operatorname*{Max}_{1 \leq i \leq e} p^{\mu_i(1-1/k)} \left| \sum_{x=1}^{p^{l-\mu_i}} e_{p^{l-\mu_i}}(g_j(x)) \right|, \tag{1}$$

since $\mu_i \leq k(1+t)$.

If ind $f(x) =$ ind $f(px)$, then by lemma 3,

$$\sum_{x=1}^{p^l} e_{p^l}(f(x)) = p^{t+1} \sum_{y=1}^{p^{l-t-1}} e_{p^l}(f(y)) = p^{t+1} \sum_{y=1}^{p^{l-t-2}} e_{p^l}(f(p\,y))$$

$$= p^{t+1} \sum_{y=1}^{p^{l-t-2}} e_{p^{l-\mu}}(g(x)) = p^{\mu-1} \sum_{y=1}^{p^{l-\mu}} e_{p^{l-\mu}}(g(y)),$$

where p^μ is the highest power of p divides all the coefficients of $f(py)$ and $f(py)=p^\mu g(y)$. We have then

$$(2) \qquad \left| \sum_{x=1}^{p^l} e_{p^l}(f(x)) \right| \leq p^{\mu(1-\frac{1}{k})} \left| \sum_{x=1}^{p^{l-\mu}} e_{p^{l-\mu}}(g(x)) \right| .$$

If we apply this method repeatedly, then there are at most k steps each giving a factor less than k^2 (using (1)), the other ones giving factor 1 only (using (2)). Thus

$$S(p^l, f(x)) = O(p^{l(1-\frac{1}{k})}).$$

Remark. The ε in the theorem may be omitted in most cases. More precisely, by a little modification of the proof of the main lemma and a theorem due to Davenport(1), we have

$$S(q^l, f(x)) = O(q^{1-\frac{1}{k}})$$

provided that k is not of the form 2^ρ or $3\cdot 2^\rho$.

§3. The object of this section is to prove the following theorem:

THEOREM 1. *Let*

$$f(x) = a_k x^k + \cdots + a_1 x, \quad (a_k, \cdots, a_1, q) = 1,$$

then

$$\sum_{x=1}^{m} e_q(f(x)) = \frac{m}{q} S(q, f(x)) + O(q^{1-1/k+\varepsilon}).$$

Evidently it is sufficient to prove that, if $0 < m < q$, we have

$$\sum_{x=1}^{m} e_q(f(x)) = O(q^{1-1/k+\varepsilon}).$$

First, we shall find a function $g(x)$ with period q such that

$$g(x) = \begin{cases} 1 & \text{for } 0 < x < m, \\ 0 & \text{for } m < x < q. \end{cases}$$

(1) *Jour. für Math.* 169(1933), 158-176.

If we assume $g(0) = g(m) = \frac{1}{2}$, then $g(x)$ can be represented by the Fourier series:

$$g(x) = \frac{m}{q} + \sum_{n=-\infty}^{\infty'} \frac{1}{2\pi i n} \left(e_q(n x) - e_q(n(x - m)) \right),$$

where in the summation the term $n = 0$ is excluded. Let

$$S_{q'} = \sum_{n=q+1}^{q'} e_q(n x).$$

It is well-known that if x is not a multiple of q, then

$$S_{q'} \leq \tfrac{1}{2} \{ x/q \}^{-1}$$

where $\{t\}$ denotes the distance of t from the nearest integer. Consequently, by the method of partial summation, we have

$$\sum_{n=q+1}^{q'} \frac{1}{n} e_q(\pm n x) = O\left(\frac{1}{q\{x/q\}} \right).$$

Similarly, if $x \neq m$ and $0 < x < q$, then

$$\sum_{n=q+1}^{q'} \frac{1}{n} e_q(\pm (x - m) n) = O\left(\frac{1}{q\{(x - m)/q\}} \right).$$

Thus, for $x \neq m$ and $0 < x < q$, we have

$$g(x) = \frac{m}{q} + \sum_{n=-q}^{q}{}' \frac{1}{2\pi i n} (e_q(nx) - e_q(n(x - m))) \tag{3}$$

$$+ O\left(\frac{1}{q\{x/q\}}\right) + O\left(\frac{1}{q\{(x - m)/q\}}\right).$$

Next

$$\sum_{x=1}^{m} e_q(f(x)) = \sum_{x=1}^{q}{}^{*} e_q(f(x))\, g(x) + O(1)$$

where Σ^* denotes a sum excluding $x = m$ and $x = q$. By (3), we have immediately

$$\sum_{x=1}^{m} e_q(f(x)) = \frac{m}{q} \sum_{x=1}^{q}{}^{*} e_q(f(x)) + \frac{1}{2\pi i} \sum_{n=-q}^{q}{}' \frac{1}{n} \left(\sum_{x=1}^{q}{}^{*} e_q(f(x) + n x) - \sum_{x=1}^{q}{}^{*} e_q(f(x) + n x - m n) \right)$$

$$+ O\left(\sum_{x=1}^{q}{}^{*} \frac{1}{q\{x/q\}} \right) + O\left(\sum_{x=1}^{q}{}^{*} \frac{1}{q\{(x-m)/q\}} \right)$$

$$= I_1 + I_2 + I_3 + I_4 + I_5, say.$$

We have

$$I_4 = \sum_{x=1}^{q}{}^{*} \frac{1}{q\{x/q\}} \leq \frac{1}{q} \sum_{x=1}^{q/2} \frac{2q}{x} = O(\log q),$$

and the same result holds for I_5.

Finally we consider

$$\sum_{n=1}^{q} \frac{1}{n} \sum_{x=1}^{q} e_q(f(x) + n x)$$

Let $(a_k, \cdots, a_2, q) = q'$ and q'' be any factor of q'. We collect the terms of the sum for which n satisfies the condition

$$(a_k, \cdots, a_2, a_1+n, q) = q''.$$

$$\sum_{n=1}^{q} \frac{1}{n} \left| \sum_{x=1}^{q} e_q(f(x) + n x) \right|$$

$$\leq \sum_{q''/q} \sum_{\substack{n=1 \\ a_1+n \equiv o, (q'')}}^{q} \frac{1}{n} \left| \sum_{x=1}^{q} e_{q/q''} \left(\frac{1}{q''} (f(x)+n x) \right) \right|$$

$$= O\left(\sum_{q''|q} \sum_{\substack{n=1 \\ a_1+n \equiv o, (q'')}}^{q} \frac{1}{n} q'' (q/q'')^{1-1/k+\varepsilon} \right)$$

$$= O\left(\sum_{q''/q} \sum_{m=1}^{q/q''} \frac{1}{m q''} q'' (q/q'')^{1-1/k+\varepsilon} \right)$$

$$= O\left(q^{1-1/k+\varepsilon} \log q \sum_{q''/q} q''^{-1+1/k+\varepsilon} \right)$$

$$= O\left(q^{1-1/k+\varepsilon}\right)$$

This method gives

$$I_2 = O\left(q^{1-1/k+\varepsilon}\right), \qquad I_3 = O\left(q^{1-1/k+\varepsilon}\right).$$

Evidently

$$I_1 = O\left(q^{1-1/k+\varepsilon}\right).$$

Combining all these results we obtain theorem 1.

Since the denominator of an integral-valued polynomial of the k–th degree is $\leq k!$, the theorem 1 is still true, if we assume only that $f(x)$ is an integral-valued polynomial of the k–th degree and $f(x) \not\equiv f(0)$, (mod p), where p is any factor of q.

§4. Finally I shall prove a theorem which has an interesting application to the problem of the "major arc" in Waring's problem.

THEOREM 2. *Let $f(x)$ be an integral-valued polynomial. Let*

$$S(\alpha) = \sum_{x=0}^{P} e^{2\pi i f(x)\alpha}, \qquad \alpha = \frac{a}{q} + \beta,$$

$$I(\beta) = \int_0^P e^{2\pi i f(x)\beta}\, dx.$$

Then, if $q = O(P^{1-\varepsilon})$ and $|\beta| = O(q^{-1} P^{-k+1-\varepsilon})$, we have

$$S(\alpha) = \bar{q}^{-1} S_{a,q} I(\beta) + O(q^{1-1/k+\varepsilon}),$$

where $\bar{q} = q(q, d)$ and d is the least common denominator of the coefficients of $f(x)$, and

$$S_{a,q} = \sum_{x=1}^{q} e_q(a f(x))$$

and the constant implied by the symbol O depends on the coefficients of $f(x)$.

To prove this theorem we shall make use of the well-known Euler's summation formula:

We define

$$b_1(x) = x - [x] - \tfrac{1}{2},$$

where $[x]$ denotes the greatest integer which does not exceed x. We define $b_l(x)$ by induction

$$b_l(x+1) = b_l(x) \tag{1}$$

and

$$\int_o^x b_l(y)\,dy = b_{l+1}(x) - b_{l+1}(0). \tag{2}$$

Let $b > a$, and let $g(x)$ and its derivatives (as far as they occur below) be continuous for $a \leq x \leq b$. Then, for any t,

$$\sum_{\substack{m \\ a \leq m+t < b}} g(m+t) = \int_a^b g(x)\,dx + \sum_{r=o}^{l-1} \left\{ g^{(r)}(b)\, b_{r+1}(t-b) - g^{(r)}(a)\, b_{r+1}(t-a) \right\} - \int_a^b g^{(l)}(x)\, b_l(t-x)\,dx. \tag{3}$$

Proof of the theorem.

First step.

$$S(\alpha) = \sum_{x=o}^{P} e^{2\pi i f(x)\alpha} = \sum_{v=1}^{\bar{q}} \sum_{\substack{o \leq r \leq P \\ r \equiv v, (\bar{q})}} e_q(a f()v)\, e^{2\pi i \beta f(r)} = \sum_{v=1}^{\bar{q}} e_q(a f(v))\, d_v, \tag{4}$$

where

$$d_v = \sum_{\substack{j \\ o \leq \bar{q}j + v \leq P}} e^{2\pi i \beta f(\bar{q}j+v)} = \sum_{\substack{j \\ o \leq j + v/\bar{q} \leq P/\bar{q}}} \Phi(j + v/\bar{q}),$$

$$\Phi(x) = e^{2\pi i \beta f(\bar{q}x)}$$

By Euler's summation formula, we have

$$(5) \qquad d_v = \int_0^{P/\bar{q}} \Phi(x)\,dx + \sum_{r=1}^{l-1} \left\{ \Phi^{(r)}\left(\frac{P}{\bar{q}}\right) b_{r+1}\left(\frac{v}{\bar{q}} - \frac{P}{\bar{q}}\right) \right.$$

$$\left. - \Phi^{(r)}(o)\, b_{r+1}\left(\frac{v}{\bar{q}}\right)\right\} - \int_0^{P/\bar{q}} \Phi^{(l)}(x)\, b_l\left(\frac{v}{\bar{q}} - x\right) dx.$$

Since

$$\int_0^{P/\bar{q}} \Phi(x)\,dx = \int_0^{P/\bar{q}} e^{2\pi i\beta f(\bar{q}x)}\,dx = \frac{1}{\bar{q}} \int_0^{P} e^{2\pi i\beta f(y)}\,dy,$$

we have, from (4) and (5)

$$S(\alpha) = \frac{S_{aq}}{\bar{q}} I(p) + \sum_{r=1}^{l} \left\{ \Phi^{(r)}\left(\frac{P}{\bar{q}}\right) a_{r+1}\left(\frac{v}{\bar{q}} - \frac{P}{\bar{q}}\right) \right.$$

$$\left. - \Phi^{(r)}(0)\, b_{r+1}\left(\frac{v}{\bar{q}}\right)\right\} - R$$

where

$$a_{r+1}\left(\frac{v}{\bar{q}} - t\right) = \sum_{v=1}^{\bar{q}} e_q(af(v))\, b_{r+1}\left(\frac{v}{\bar{q}} - t\right),$$

$$R = \sum_{v=1}^{\bar{q}} e_q(a f(v)) \int_0^{P/\bar{q}} \Phi^{(l)}(x)\, b_l\left(\frac{v}{\bar{q}} - x\right) dx.$$

Second step. If $q = O(P^{1-\varepsilon})$, $\beta = O(q^{-1}P^{-k+1-\varepsilon})$ and $0 < x \leq P/\bar{q}$, then

$$(6) \qquad \Phi^{(r)}(x) = O(P^{-r\varepsilon}).$$

Suppose $f(v)$ have only one term, namely $f(v) = Av^k$. Let

$$\psi(x) = e^{2\pi i\beta A(\bar{q}x)^k}.$$

First, we shall prove that

$$\psi^{(r)}(x) = O(P^{-r\varepsilon}).$$

Let $\psi_1(z) = e^{z^k}$, then

$$\psi_1^{(r)}(z) = e^{z^k} F_r(z),$$

where $F_r(z)$ is a polynomial of the $r(k-1)$-th degree. Therefore

$$\psi^{(r)}(x) = e^{2\pi i\beta A(\bar{q}x)^k} F_r((2\pi i\beta A)^{1/k}\, \bar{q}\, x)((2\pi i\beta A)^{1/k}\, \bar{q})^r.$$

Consequently

$$\psi^{(r)}(x) = O(1 + (|\beta|^{1/k} q\, x)^{(k-1)r})(|\beta|^{1/k} q)^r$$
$$= O(P^{-r\varepsilon}).$$

Next, we suppose $f(x)$ to be a polynomial with the first coefficient A. Let

$$\Phi(x) = \psi(x)\psi_1(x), \qquad \psi_1(x) = e^{2\pi i\beta(f(\bar{q}x) - A(\bar{q}x)^k)}.$$

Suppose (6) to be true for $k-1$, i.e. when $|\beta| \leq q^{-1} P^{-k+2-\varepsilon}$, we have

$$\psi_1^{(r)}(x) = O(P^{-r\varepsilon}).$$

Since $q^{-1} P^{-k+2-\varepsilon} > q^{-1} P^{-k+1-\varepsilon}$, we have

$$\psi_1^{(r)}(x) = O(P^{-r\varepsilon}),$$

for $|\beta| = O(q^{-1} P^{-k+1-\varepsilon})$. Further, since

$$\Phi^{(r)}(x) = \psi^{(r)}(x)\psi_1(x) + \binom{r}{1} \psi^{(r-1)}(x)\psi_1'(x) + \cdots + \psi(x)\psi_1^{(r)}(x),$$

we have

$$\Phi^{(r)}(x) = O\left(\underset{o \leq i \leq r}{Max}(\psi^{(r-i)}(x)\psi_1^{(i)}(x))\right) = O(P^{-r\varepsilon}).$$

Third step. Take

$$l = [1/\varepsilon] + 1,$$

then

$$\Phi^{(l)}(x) = O(P^{-1}),$$

Therefore

$$|R| = O\left(\frac{1}{q}\int_0^{P/\bar{q}} P^{-1}\, dx\right) = O(1).$$

Fourth step. Let

$$S_v = \sum_{h=1}^{v} e_q(af(h)).$$

By the definition of $a_r(t)$, we have

$$a_r\left(\frac{v}{\bar{q}} - t\right) = S_1 b_{r+1}\left(\frac{1}{\bar{q}} - t\right) + \sum_{v=2}^{\bar{q}} (S_v - S_{v-1})\, b_{r+1}\left(\frac{v}{\bar{q}} - t\right)$$

$$= \sum_{m=1}^{\bar{q}-1} S_m \left\{ b_{r+1}\left(\frac{m}{\bar{q}} - t\right) - b_{r+1}\left(\frac{m+1}{\bar{q}} - t\right)\right\} + S_q b_{r+1}(1-t).$$

By theorem 1,

$$S_v = O(\bar{q}^{1-\frac{1}{k}+\varepsilon}) \qquad \text{for } 0 < v \leq q.$$

Thus

$$a_r\left(\frac{v}{\bar{q}} - t\right) = O\left(\bar{q}^{\,1-1/k+\varepsilon}\left\{\sum_{m=1}^{\bar{q}-1}\left| b_{r+1}\left(\frac{m}{\bar{q}} - t\right) - b_{r+1}\left(\frac{m+1}{\bar{q}} - t\right)\right| + 1\right\}\right).$$

Since b_{r+1} is a function of bounded variation, we have

$$a_r\left(\frac{v}{\bar{q}} - t\right) = O\left(\bar{q}^{\,1-1/k+\varepsilon}\right).$$

Fifth step. Combining the results of the 2nd, 3rd and 4th steps, we have, in conclusion, that

$$S(a) - \bar{q}^{-1} S_{aq} I(p) = O\left(\bar{q}^{\,1-\frac{1}{k}+\varepsilon}\sum_{r=1}^{l-1} P^{-r\varepsilon} + 1\right) = O\left(\bar{q}^{\,1-1/k+\varepsilon}\right).$$

National Tsing Hua University

(Received 14, April, 1939).