BULL. AUSTRAL. MATH. SOC. 11L07
VOL. 50 (1994) [451–458]

ON HAU'S LEMMA

W.K.A. LOH

Let $f \in \mathbb{Z}[X]$ and let q be a prime power $p^l (l \geqslant 2)$. Hua stated and proved that

$$\sum_{0 \leqslant x < q} \exp\left(2\pi i f(x) q^{-1}\right) < C q^{(1-1/(M+1))},$$

for some unspecified constant $C > 0$ depending on the derivative f' of f; M denoting the maximum multiplicity of the roots of the congruence

$$p^{-t} f'(x) \equiv 0 \pmod{p},$$

where t is an integer chosen so that the polynomial $p^{-t} f'(x)$ is primitive. An explicit value for C was given by Chalk for $p \geqslant 3$. Subsequently, Ping Ding (in two successive articles) obtained better estimates for $p \geqslant 2$.

This article provides a better result, based upon a more precise form of Hua's main lemma, previously overlooked.

1. INTRODUCTION

Let

$$f(X) = a_k X^k + \ldots + a_1 X + a_0 \in \mathbb{Z}[X], \tag{1}$$

and let p denote any prime. The p-content $\nu_p(f)$ of f is defined by

$$\nu_p(f) = \alpha \text{ if } p^\alpha \mid (a_k, \ldots, a_0),\ p^{\alpha+1} \nmid (a_k, \ldots, a_0).$$

In particular,

$$\nu_p(a) = \alpha \text{ if } p^\alpha \mid a,\ p^{\alpha+1} \nmid a.$$

Let $e_q(\alpha) = \exp\left(2\pi i \alpha q^{-1}\right)$ and let

$$S(q, f) = \sum_{0 \leqslant x < q} e_q[f(x)]. \tag{2}$$

Received 1 February 1994
I wish to thank Professors J.H.H. Chalk and R.C. Vaughan for their very helpful advice, comments and suggestions.

https://doi.org/10.1017/S0004972700013563 Published online by Cambridge University Press

Now suppose that $q = p^\ell$ is a power of p and that

(3) $$\nu_p[f(X) - f(0)] = 0, \quad \nu_p[f'(X)] = t \geqslant 0.$$

Let m, M denote the sum and the maximum, respectively, of the multiplicities of the roots of the congruence (where (mod p) is denoted by (p) for convenience)

(4) $$p^{-t} f'(x) \equiv 0 \quad (p), \quad (0 \leqslant x < p).$$

Let $r = r(f)$ denote the number of distinct roots of the congruence (4). If $r(f) > 0$, let $\mu_1, \mu_2, \ldots, \mu_r$ denote the roots of (4) and let their multiplicities be $m_1, m_2, \ldots, m_r$. Thus $m = m_1 + m_2 + \ldots + m_r$ and $M = \max(m_1, m_2, \ldots, m_r)$.

In [4], Hua derived the estimate

$$\left|S(p^\ell, f)\right| \leqslant k^3 p^{l(1-1/k)},$$

by induction on l. In [**1**], Chalk derived a more precise form of Hua's lemma.

THEOREM. *Suppose $f(X)$ satisfies (1) and (4), let $p \geqslant 2$ be a prime and l an integer $\geqslant 2$. Then*

(i) $\left|S(p^1, f)\right| \leqslant mkp^{t/(M+1)}p^{l[1-1/(M+1)]}$, *if $r(f) > 0$;*
(ii) $S(p^l, f) = 0$, *if $r(f) = 0$; for all $l \geqslant 2(t+1)$. Otherwise $\left|S(p^l, f)\right| \leqslant p^{2t+1}$, where $p^t \leqslant k$.*

Chalk further conjectured that

(5) $$\left|S(p^l, f)\right| \leqslant mp^{t/(M+1)}p^{l(1-1/(M+1))}.$$

In [**2**], Ping Ding obtained a better upper bound

(6) $$|S(p^n, f(x))| \leqslant mp^{\tau/(M+1)}p^{t/(M+1)}p^{n(1-1/(M+1))},$$

where $\tau = [\log k / \log p]$.

Loxton and Vaughan [**5**] proved that

$$\left|S(p^l, f)\right| \leqslant (k-1)p^{\sigma/(e+1)}p^{\tau/(e+1)}p^{l(1-1/(e+1))},$$

where

$$e = \max_{1 \leqslant i \leqslant s} e_i, \qquad \tau = \begin{cases} 1, & \text{if } p \leqslant k; \\ 0, & \text{if } p > k. \end{cases}$$

Here

$$f'(x) = ka_k(X-\zeta_1)^{e_1}(X-\zeta_2)^{e_2}\cdots(X-\zeta_s)^{e_s},$$

where $\zeta_1, \zeta_2, \ldots, \zeta_s$ are the distinct roots of $f'(x)$ in a finite extension K_p of the p-adic field Q_p and

$$\delta = \nu_p[\theta(f')],$$

where $\theta(f')$ denotes the different of $f'(x)$ and ν_p the unique extension of the valuation in Q_p to K_p.

In this paper, we shall prove a result which is close to the conjecture of Chalk. We follow Chalk's argument in [1] using induction on l. The improved estimate stated in Theorem 1 is due to an improved form of Lemma 3 in [1].

Theorem 1. *Suppose that f satisfies (4). Let $p \leqslant k$ be a prime and*

$$\theta(p) = \begin{cases} 1 & \text{if } p \geqslant 3, \\ 2 & \text{if } p = 2. \end{cases}$$

Suppose that $l \geqslant 2$,

(i) *if $r(f) > 0$, then*

$$|S(p^l, f)| \leqslant mp^{(t+\theta)/(M+1)} p^{l(1-1/(M+1))}; \tag{7}$$

(ii) *if $r(f) = 0$, then*

$$S(p^l, f) = 0,$$

for all $l > t + \theta$ and otherwise $|S(p^l, f)| \leqslant p^{t+\theta}$.

Theorem 2. *Suppose that $r(f) > 0$, $l \geqslant 2$ and f is as in (1). Let $p > k \geqslant 2$ be a prime. Then*

$$|S(p^l, f)| \leqslant mp^{l(1-1/(M+1))}. \tag{8}$$

2. Lemmata

Lemma 1. (See Hua [3].)

(i) *Suppose that*

$$\nu_p[f(X) - f(0)] = 0, \text{ and } \nu_p[f(pX + \mu) - f(\mu)] = \sigma(\mu) = \sigma.$$

Then

$$1 \leqslant \sigma \leqslant k.$$

(ii) *Suppose that*

$$\nu_p[f(X) - f(0)] = 0, \text{ and } f(X) \equiv (X - \mu)^\omega h(X) \quad (p),$$

where $(h(0), p) = 1$. *Then*

$$p^{-\sigma} f(pX + \mu) \equiv H(X)(p),$$

where $\sigma = \nu_p[f(pX + \mu)]$ and

$$\deg H(X) \leqslant \omega. \tag{9}$$

Lemma 2. (See [1], Lemma 2.) *Suppose that*

$$\nu_p[f(X) - f(0)] = 0, \quad \nu_p[f'(X)] = t$$

and that μ $(0 \leqslant \mu < p)$ *is a root of the congruence*

$$p^{-1} f(X) \equiv 0 \quad (p)$$

with multiplicity $\omega \geqslant 1$. *Let*

$$g(X) = p^{-\sigma}[f(pX + \mu) - f(\mu)],$$

where $\sigma = \nu_p[f(pX + \mu) - f(\mu)]$. *If* $\nu_p[g'(X)] = \tau$, *then*

$$\sigma + \tau \leqslant \omega + 1 + t. \tag{10}$$

Definition: Let

$$S_\mu = \sum_{0 \leqslant x < p^l,\, x \equiv \mu \quad (p)} e_{p^l}[f(x)].$$

Then

$$|S_\mu| \leqslant p^{l-1},$$

and

$$S(p^l, f) = \sum_{0 \leqslant \mu < p} S_\mu. \tag{11}$$

Lemma 3. *Suppose that* $l \geqslant t + 2$ and $p \geqslant 3$. *Then*

(i) $S_\mu = 0$, *unless* μ *is a root of the congruence (4).*

(ii) *If* μ *is any such root and*

$$g(X) = p^{-\sigma}[f(pX + \mu) - f(\mu)],$$

where σ *is chosen so that* $\nu_p[g(X)] = 0$, *then*

$$|S_\mu| \leqslant p^{\sigma - 1} \left| S(p^{l-\sigma}, g) \right|, \tag{12}$$

provided that

$$l > \sigma.$$

https://doi.org/10.1017/S0004972700013563 Published online by Cambridge University Press

Further, (i) and (ii) hold in the special case $p = 2$, provided that $l \geqslant t+3$.

PROOF: Put

$$x = y + p^{l-t-1}z,\ 0 \leqslant y < p^{l-t-1},\ 0 \leqslant z < p^{t+1}.$$

Let

$$g(x) = p^{-t}f'(x),\ g'(x) = p^{-t}f''(x),\ \dots,\ g^{(n-1)}(x) = p^{-t}f^{(n)}(x), \dots.$$

Now $p^{-t}f'(X)$ has integer coefficients. Therefore,

$$\frac{g^{(n-1)}(X)}{(n-1)!} = \frac{p^{-t}f^{(n)}(X)}{(n-1)!} \in \mathbb{Z}[X]. \tag{13}$$

The coefficient a_n of z^n in the Taylor expansion of $f\big(y + p^{l-t-1}z\big)$ is

$$a_n = p^{n(l-t-1)}\frac{f^{(n)}(y)}{n!} = p^{n(l-t-1)}\frac{p^t}{n}\frac{g^{(n-1)}(y)}{(n-1)!}. \tag{14}$$

Hence,

$$\nu_p(a_n) \geqslant n(l-t-1) + t - \nu_p(n).$$

For $n = 2$,

$$\begin{aligned}\nu_p(a_2) &\geqslant 2(l-t-1) + t - \nu_p(2),\\ &= (l-t-2-\nu_p(2)) + l.\end{aligned}$$

If $p \geqslant 3$ and $l \geqslant t+2$ or $p = 2$ and $l \geqslant t+3$, then $\nu_p(a_2) \geqslant l$. For $n \geqslant 3$,

$$\begin{aligned}\nu_p(a_n) &\geqslant n(l-t-1) + t - \nu_p(n),\\ &= (n-1)(l-t-2) + n - \nu_p(n) - 2 + l.\end{aligned}$$

If $l \geqslant t+2$, then $\nu_p(a_n) \geqslant l$ for all p. Therefore, the coefficient a_n has a p^l factor for $p \geqslant 3$ and $l \geqslant t+2$ or $p = 2$ and $l \geqslant t+3$. Hence, we have

$$\begin{aligned}S_\mu &= \sum_{\substack{0 \leqslant y < p^{l-t-1}\\ y \equiv \mu \quad (p)}} \sum_{0 \leqslant z < p^{t+1}} e_{p^l}[f(y) + p^{l-t-1}f'(y)z + p^{2l-2t-2}f''(y)z^2],\\ &= \sum_{\substack{0 \leqslant y < p^{l-t-1}\\ y \equiv \mu \quad (p)}} \sum_{0 \leqslant z < p^{t+1}} e_{p^l}[f(y) + p^{l-t-1}f'(y)z],\\ &= \sum_{\substack{0 \leqslant y < p^{l-t-1}\\ y \equiv \mu \quad (p)}} e_{p^l}[f(y)] \sum_{0 \leqslant z < p^{t+1}} e_{p^{t+1}}[f'(y)z].\end{aligned}$$

https://doi.org/10.1017/S0004972700013563 Published online by Cambridge University Press

Now if $f'(y) \not\equiv 0 \pmod{p^{t+1}}$, then the inner sum equals 0 and as $y \equiv \mu \pmod{p}$, we see that $S_\mu = 0$, unless μ is a root of (4). Further, for any μ, we have the following reductive formula for S_μ:

$$\begin{aligned} S_\mu &= \sum_{0 \leqslant y < p^{l-1}} e_{p^l}[f(py+\mu)], \\ &= e_{p^l}[f(\mu)] \sum_{0 \leqslant y < p^{l-1}} e_{p^l}[p^\sigma g(y)], \\ &= e_{p^l}[f(\mu)] p^{\sigma-1} S\left(p^{l-\sigma}, g\right), \text{ if } l > \sigma. \end{aligned}$$

□

3. Proof of the Theorems

Proof of Theorem 1: (A) If $2 \leqslant l \leqslant t+\theta$, then by a trivial estimate

(15) $$\left|S\left(p^l, f\right)\right| \leqslant p^l \leqslant p^{(t+\theta)/(M+1)} p^{l(1-1/(M+1))}.$$

(B) If $l > t+\theta$, $S_\mu = 0$, unless $\mu = \mu_i$ for some i, by Lemma 3. By lemma 2 we have

$$\sigma_i + t_i \leqslant m_i + 1 + t.$$

(i) If $l - \sigma_i \leqslant t_i + \theta$ for some i, a trivial estimate gives

(16) $$\left|S_{\mu_i}\right| \leqslant p^{l-1} = p^{(l-m_i-1)/(m_i+1)} p^{l(1-1/(m_i+1))} \leqslant p^{(t+\theta)/(m_i+1)} p^{l(1-1/(m_i+1))},$$

since $l - m_i - l \leqslant \sigma_i + t_i + \theta - m_i - 1 \leqslant t + \theta$ by (10).

(ii) Otherwise, if $l > \sigma_i + t_i + \theta$ for some i, we obtain

(17) $$\left|S_{\mu_i}\right| \leqslant p^{\sigma_i - 1}\left|S\left(p^{(l-\sigma_i)}, g_i\right)\right|,$$

by Lemma 3. Since $m(g_i) \leqslant m_i$, by induction and (10),

(18) $$\begin{aligned} \left|S_{\mu_i}\right| &\leqslant m(g_i) p^{\sigma_i - 1} p^{(l-\sigma_i)\left(1-(1-(t_i+\theta)/(l-\sigma_i))/(M(g_i)+1)\right)}, \\ &\leqslant m_i p^{\sigma_i - 1} p^{(l-\sigma_i)\left(1-(1-(t_i+\theta)/(l-\sigma_i))/(m_i+1)\right)}, \\ &= m_i p^{\sigma_i-1} p^{(t_i+\theta)/(m_i+1)} p^{(l-\sigma_i)(1-(1/(m_i+1)))}, \\ &= m_i p^{(\sigma_i+t_i+\theta)/(m_i+1)-1} p^{l(1-(1/m_i+1))}, \\ &\leqslant m_i p^{(t+\theta)/(m_i+1)} p^{l(1-(1/m_i+1))}, \\ &= m_i p^{l\left(1-(1-(t+\theta)/l)/(m_i+1)\right)}, \\ &\leqslant m_i p^{(t+\theta)/(M+1)} p^{l(1-(1/M+1))}. \end{aligned}$$

https://doi.org/10.1017/S0004972700013563 Published online by Cambridge University Press

For $r(f) > 0$, $l > t + \theta$, by (11), (16) and (18), we have

$$\begin{aligned}|S(p^l, f)| &\leqslant \sum_{1 \leqslant i \leqslant r(f)} m_i p^{(t+\theta)/(M+1)} p^{l(1-(1/M+1))}, \\ &= m p^{(t+\theta)/(M+1)} p^{l(1-(1/M+1))}.\end{aligned}$$

□

Proof of Theorem 2: Since $p > k \geqslant 2$, therefore $t = 0$ and all $t_i = 0$. By Lemma 2 we have

$$\sigma_i \leqslant m_i + 1, \tag{19}$$

and by Lemma 3 we have

$$|S_\mu| \leqslant p^{\sigma-1} \left|S(p^{l-\sigma}, g)\right|.$$

(A) When $l = 2$, we have

$$\left|S_{\mu_i}\right| = \left|\sum_{0 \leqslant y < p} e_{p^2}[f(py + \mu_i) - f(\mu_i)]\right| = p,$$

and so

$$\left|S(p^l, f)\right| \leqslant mp = mp^{2(1-1/2)} \leqslant mp^{l(1-(1/M+1))}.$$

(B) When $l > 2$, we consider three cases:

Case (i). If $\ell \geqslant \sigma_i$ for some i, using the trivial estimate

$$\left|S_{u_i}\right| \geqslant p^{\ell-1} \geqslant p^{\ell(1/m_i+1)} \geqslant p^{\ell(1-(1/M+1))}, \tag{20}$$

Case (ii). If $l - \sigma_i = 1$, then by Lemma 3 (ii)

$$\left|S_{\mu_i}\right| \leqslant p^{\sigma_i - 1} |S(p, g)|.$$

Since

$$S(p, g) = \sum_{0 \leqslant y < p} e_p \left[\frac{f'(\mu_i)}{p^{l-2}} y + \frac{f''(\mu_i)}{2! p^{l-3}} y^2 + \cdots + \frac{f^{(l-2)}(\mu_i)}{(l-2)!} y^{(l-1)}\right]$$

by Weil's estimate, we have

$$|S(p, g)| \leqslant (l-2) p^{1/2},$$

since $l = \sigma_i + 1 \leqslant m_i + 2$. Therefore

$$|S(p, g)| \leqslant m_i p^{1/2}.$$

https://doi.org/10.1017/S0004972700013563 Published online by Cambridge University Press

Thus

$$|S_\mu| \leqslant p^{\sigma_i - 1} m_i p^{1/2}, \tag{21}$$
$$\leqslant m_i p^{\sigma_i - 1} p^{(l-\sigma_i)(1-(1/M+1))},$$
$$\leqslant m_i p^{l(1-(1/M+1))},$$

since $\sigma_i \leqslant m_i + 1$.

Case (iii). Otherwise, if $2 \leqslant l - \sigma_i$, then by induction

$$\left|S_{\mu_i}\right| \leqslant p^{\sigma_i - 1} m(g_i) p^{(l-\sigma_i)(1-(1/M(g_i)+1))}, \tag{22}$$
$$\leqslant m_i p^{\sigma_i/(m_i+1)-1} p^{l(1-(1/(m_i+1)))},$$
$$\leqslant m_i p^{l(1-(1/M+1))},$$

since $m(g_i) \leqslant m_i$ and $\sigma_i \leqslant m_i + 1$.

For $r(f) > 0$ and $l \geqslant 2$, by (11), (20), (21) and (22), we have

$$\left|S(p^l, f)\right| \leqslant \sum_{1 \leqslant i \leqslant r(f)} m_i p^{l(1-(1/M+1))},$$
$$= m p^{l(1-(1/M+1))}.$$

$\square$

References

[1] J.H.H. Chalk, 'On Hua's estimates for exponential sums', *Mathematika* **34** (1987), 115–123.

[2] Ping Ding, 'An improvement to Chalk's estimation of exponential sums', *Acta Arith.* **LIX.2** (1991), 149–155.

[3] Loo-Keng Hua, *Additive theory of prime numbers* (American Mathematical Society, Providence, 1965), **pp.** 2–7.

[4] Loo-Keng Hua, 'Die abschätzung von Exponentialsummen und ihre Anwendung in der Zahlentheorie', *Enzyklopädie der Math. Wiss* **Bd I2, H.13, TI** (1959), p. 41.

[5] J.H. Loxton and R.C. Vaughan, 'The estimation of complete exponential sums', *Canad. Math. Bull.* **28** (1985), 440–454.

Department of Mathematics
Imperial College
Huxley Building
180 Queen's Gate
London SW7 2BZ
United Kingdom