Let $f \in \mathbb{Z}[X]$ and let $q$ be a prime power $p^l (l \geq 2)$. Hua stated and proved that
\[
\sum_{0 \leq z < q} \exp \left( 2\pi i f(z)q^{-1} \right) < Cq^{\frac{1}{l-1/(M+1)}},
\]
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 $p \geq 3$. Subsequently, Ping Ding (in two successive articles) obtained better estimates for $p \geq 2$.

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

1. INTRODUCTION

Let
\[
f(X) = a_k X^k + \ldots + a_1 X + a_0 \in \mathbb{Z}[X],
\]
and let $p$ denote any prime. The $p$-content $\nu_p(f)$ of $f$ is defined by
\[
\nu_p(f) = \alpha \text{ if } p^\alpha \mid (a_k, \ldots, a_0), \quad p^{\alpha+1} \nmid (a_k, \ldots, a_0).
\]
In particular,
\[
\nu_p(a) = \alpha \text{ if } p^\alpha \mid a, \quad p^{\alpha+1} \nmid a.
\]
Let $e_q(\alpha) = \exp(2\pi i \alpha q^{-1})$ and let
\[
S(q, f) = \sum_{0 \leq z < q} e_q[f(z)].
\]
Now suppose that \( q = p^t \) is a power of \( p \) and that
\[
\nu_p[f(X) - f(0)] = 0, \quad \nu_p[f'(X)] = t \geq 0.
\]

Let \( m, M \) denote the sum and the maximum, respectively, of the multiplicities of the roots of the congruence (where \( \text{mod } p \) is denoted by \( (p) \) for convenience)
\[
p^{-t} f'(x) \equiv 0 \pmod{p}, \quad (0 \leq x < p).
\]

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 \cite{4}, Hua derived the estimate
\[
|S(p^l, f)| \leq k^3 p^{(1-1/k)},
\]
by induction on \( l \). In \cite{1}, Chalk derived a more precise form of Hua’s lemma.

**Theorem.** Suppose \( f(X) \) satisfies \((1)\) and \((4)\), let \( p \geq 2 \) be a prime and \( l \) an integer \( \geq 2 \). Then
\[
\begin{align*}
(i) \quad |S(p^l, f)| &\leq mp^{t/(M+1)}p^{l(1-1/(M+1))}, \text{ if } r(f) > 0; \\
(ii) \quad S(p^l, f) = 0, \text{ if } r(f) = 0; \text{ for all } l \geq 2(t + 1). \text{ Otherwise } |S(p^l, f)| \leq p^{2t+1}, \text{ where } p^l \leq k.
\end{align*}
\]

Chalk further conjectured that
\[
|S(p^l, f)| \leq mp^{t/(M+1)}p^{l(1-1/(M+1))}.
\]

In \cite{2}, Ping Ding obtained a better upper bound
\[
|S(p^l, f(x))| \leq mp^{r/(M+1)}p^{l(1-1/(M+1))},
\]
where \( r = \lceil \log k / \log p \rceil \).

Loxton and Vaughan \cite{5} proved that
\[
|S(p^l, f)| \leq (k - 1)p^{a/(e+1)}p^{r/(e+1)}p^{l(1-1/(e+1))},
\]
where
\[
e = \max_{1 \leq i \leq s} e_i, \quad \tau = \begin{cases} 1, & \text{if } p \leq k; \\ 0, & \text{if } p > k. \end{cases}
\]

Here
\[
f'(x) = k\alpha_k(X - \zeta_1)^{e_1}(X - \zeta_2)^{e_2} \cdots (X - \zeta_s)^{e_s},
\]
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 \( \nu_p \) 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 \( p \leq k \) be a prime and

\[
\theta(p) = \begin{cases} 
1 & \text{if } p \geq 3, \\
2 & \text{if } p = 2.
\end{cases}
\]

Suppose that \( l \geq 2 \),

(i) if \( r(f) > 0 \), then

\[
|S(p^l, f)| \leq mp^{(\ell+\theta)/(M+1)}p^{l(1-1/(M+1))},
\]

(ii) if \( r(f) = 0 \), then

\[
S(p^l, f) = 0,
\]

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

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

\[
|S(p^l, f)| \leq mp^{l(1-1/(M+1))}.
\]

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

\[
1 \leq \sigma \leq k.
\]

(ii) Suppose that

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

where \( \omega \) is an integer.
where \( (h(0), p) = 1 \). Then
\[
p^{-\sigma} f(pX + \mu) \equiv H(X)(p),
\]
where \( \sigma = \nu_p[f(pX + \mu)] \) and
\[
\text{deg } H(X) \leq \omega.
\]

**Lemma 2.** (See [1], Lemma 2.) Suppose that
\[
\nu_p[f(X) - f(0)] = 0, \quad \nu_p[f'(X)] = t
\]
and that \( \mu (0 \leq \mu < p) \) is a root of the congruence
\[
p^{-1} f(X) \equiv 0 \pmod{p}
\]
with multiplicity \( \omega \geq 1 \). 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
\[
\sigma + \tau \leq \omega + 1 + t.
\]

**Definition:** Let
\[
S_{\mu} = \sum_{0 \leq z < p', z \equiv \mu} e_{p'}[f(z)].
\]
Then
\[
|S_{\mu}| \leq p^{l-1},
\]
and
\[
S(p', f) = \sum_{0 \leq \mu < p} S_{\mu}.
\]

**Lemma 3.** Suppose that \( l \geq t + 2 \) and \( p \geq 3 \). Then
(i) \( S_{\mu} = 0 \), unless \( \mu \) is a root of the congruence (4).
(ii) If \( \mu \) is any such root and
\[
g(X) = p^{-\sigma}[f(pX + \mu) - f(\mu)],
\]
where \( \sigma \) is chosen so that \( \nu_p[g(X)] = 0 \), then
\[
|S_{\mu}| \leq p^{\sigma-1} |S(p^{l-\sigma}, g)|,
\]
provided that
\[
l > \sigma.
\]
Further, (i) and (ii) hold in the special case $p = 2$, provided that $l \geq t + 3$.

**Proof:** Put

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

Let

$$g(z) = p^{-t}f'(z), \quad g'(z) = p^{-t}f''(z), \quad \ldots, \quad g^{(n-1)}(z) = p^{-t}f^{(n)}(z), \quad \ldots. $$

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

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

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

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

Hence,

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

For $n = 2$,

$$\nu_p(a_2) \geq 2(l-t-1) + t - \nu_p(2),$$

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

$$\nu_p(a_n) \geq n(l-t-1) + t - \nu_p(n),$$

$$= (n-1)(l-t-2) + n - \nu_p(n) - 2 + l.$$ If $l \geq t + 2$, then $\nu_p(a_n) \geq l$ for all $p$. Therefore, the coefficient $a_n$ has a $p^l$ factor for $p \geq 3$ and $l \geq t + 2$ or $p = 2$ and $l \geq t + 3$. Hence, we have

$$S_\mu = \sum_{0 \leq y < p^{l-t-1}} \sum_{y \equiv \mu \pmod{p}} e_p[ f(y) + p^{l-t-1}f'(y)z + p^{2l-2t-2}f''(y)z^2],$$

$$= \sum_{0 \leq y < p^{l-t-1}} \sum_{y \equiv \mu \pmod{p}} e_p[ f(y) + p^{l-t-1}f'(y)z],$$

$$= \sum_{0 \leq y < p^{l-t-1}} \sum_{y \equiv \mu \pmod{p}} e_p[ f(y)] \sum_{0 \leq z < p^{t+1}} e_p[ f'(y)z].$$
Now if \( f'(y) \neq 0 \) \((p^{l+1})\), then the inner sum equals 0 and as \( y = \mu \) \((p)\), we see that \( S_\mu = 0 \), unless \( \mu \) is a root of \((4)\). Further, for any \( \mu \), we have the following reductive formula for \( S_\mu \):

\[
S_\mu = \sum_{0 \leq y < p^{l-1}} e_p[f(py + \mu)],
\]

\[
= e_p[f(\mu)] \sum_{0 \leq y < p^{l-1}} e_p[p^\sigma g(y)],
\]

\[
= e_p[f(\mu)]p^{-1}S(p^{l-\sigma}, g), \text{ if } l > \sigma.
\]

\[\square\]

### 3. Proof of the Theorems

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

\[
|S(p^l, f)| \leq p^l \leq p^{(l+\theta)/(M+1)}p^{(1-1/(M+1))}.
\]

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

\[
\sigma_i + t_i \leq m_i + 1 + t.
\]

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

\[
|S_{\mu_i}| \leq p^{l-1} = p^{(l-m_i-1)/(m_i+1)}p^{l/(1-1/(m_i+1))} \leq p^{(t+\theta)/(m_i+1)}p^{l/(1-1/(m_i+1))},
\]

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

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

\[
|S_{\mu_i}| \leq p^{\sigma_i+1}S(p^{(l-\sigma_i)}),
\]

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

\[
|S_{\mu_i}| \leq m(g_i)p^{\sigma_i+1}p^{(l-\sigma_i)(1-1/(t_i+\theta)/(1-\sigma_i))/(M+1)}.
\]

\[
\leq m_i p^{\sigma_i+1}p^{(l-\sigma_i)(1-1/(t_i+\theta)/(1-\sigma_i))}(1/(1/(M+1)))
\]

\[
= m_i p^{\sigma_i+1}p^{(l-\sigma_i)(1-1/(t_i+\theta)/(1-\sigma_i))}(1/(1/(M+1)))
\]

\[
= m_i p^{(l-\sigma_i)(1-1/(t_i+\theta)/(1-\sigma_i))}(1/(1/(M+1)))
\]

\[
\leq m_i p^{(l-\sigma_i)(1-1/(t_i+\theta)/(1-\sigma_i))}(1/(1/(M+1)))
\]

\[
\leq m_i p^{(l-\sigma_i)(1-1/(t_i+\theta)/(1-\sigma_i))}(1/(1/(M+1)))
\]

\[
\leq m_i p^{(l-\sigma_i)(1-1/(t_i+\theta)/(1-\sigma_i))}(1/(1/(M+1)))
\]

\[
\leq m_i p^{(l-\sigma_i)(1-1/(t_i+\theta)/(1-\sigma_i))}(1/(1/(M+1)))
\]

\[
\leq m_i p^{(l-\sigma_i)(1-1/(t_i+\theta)/(1-\sigma_i))}(1/(1/(M+1)))
\]
For $r(f) > 0$, $l > t + \theta$, by (11), (16) and (18), we have
\[
|S(p^l, f)| \leq \sum_{1 \leq i \leq r(f)} m_i p^{(t+\theta)/(M+1)} p^{(1-(1/M+1))},
\]
\[
= m p^{(t+\theta)/(M+1)} p^{(1-(1/M+1))}.
\]

**Proof of Theorem 2:** Since $p > k \geq 2$, therefore $t = 0$ and all $t_i = 0$. By Lemma 2 we have
\[
(19) \quad \sigma_i \leq m_i + 1,
\]
and by Lemma 3 we have
\[
|S_{\mu_i}| \leq p^{\sigma_i-1} |S(p^{1-\sigma}, g)|.
\]

(A) When $l = 2$, we have
\[
|S_{\mu_i}| = \left| \sum_{0 \leq y < p} e_p^2 [f(py + \mu_i) - f(\mu_i)] \right| = p,
\]
and so
\[
|S(p^l, f)| \leq m p = m p^{2(1-1/2)} \leq m p^{(1-(1/M+1))}.
\]

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

Case (i). If $\ell \geq \sigma_i$ for some $i$, using the trivial estimate
\[
(20) \quad |S_{\mu_i}| \geq p^{\ell-1} \geq p^{(1/m_i+1)} \geq p^{(1-(1/M+1))},
\]

Case (ii). If $l - \sigma_i = 1$, then by Lemma 3 (ii)
\[
|S_{\mu_i}| \leq p^{\sigma_i-1} |S(p, g)|.
\]

Since
\[
S(p, g) = \sum_{0 \leq y < p} e_p \left[ f'(\mu_i) p^{l-2} y + \frac{f''(\mu_i)}{2!} p^{l-3} y^2 + \cdots + \frac{f^{(l-2)}(\mu_i)}{(l-2)!} p^{l-(l-1)} y^{l-1} \right]
\]
by Weil's estimate, we have
\[
|S(p, g)| \leq (l-2)p^{1/2},
\]
since $l = \sigma_i + 1 \leq m_i + 2$. Therefore
\[
|S(p, g)| \leq m_i p^{1/2}.
\]
Thus

(21) \[ |S_\mu| \leq p^{\sigma_i - 1} m_i p^{1/2}, \]

\[ \leq m_i p^{\sigma_i - 1} p^{(1-\sigma_i)(1-(1/M+1))}, \]

\[ \leq m_i p^{(1-(1/M+1))}, \]

since \( \sigma_i \leq m_i + 1 \).

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

(22) \[ |S_{\mu_i}| \leq p^{\sigma_i - 1} m(g_i) p^{(l-\sigma_i)(1-(1/M(g_i)+1))}, \]

\[ \leq m_i p^{\sigma_i/(m_i+1) - 1} p^{(1-(1/(m_i+1)))}, \]

\[ \leq m_i p^{(1-(1/M+1))}, \]

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

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

\[ |S(p^l, f)| \leq \sum_{1 \leq i \leq r(f)} m_i p^{(1-(1/M+1))}, \]

\[ = mp^{(1-(1/M+1))}. \]

\[ \square \]

References


