On Waring’s problem with polynomial summands II

by

HONG BING YU (Hefei)

1. Introduction. Let \( f_k(x) \) be an integral-valued polynomial of degree \( k \) with positive leading coefficient, \( f_k(0) = 0 \) and satisfying the condition that there do not exist integers \( c \) and \( q > 1 \) such that \( f_k(x) \equiv c \pmod{q} \) identically. It is known that \( f_k(x) \) is of the form

\[
(1.1) \quad f_k(x) = a_k F_k(x) + \ldots + a_1 F_1(x),
\]

where \( F_i(x) = x(x-1)\ldots(x-i+1)/i! \) (\( 1 \leq i \leq k \)), and \( a_1, \ldots, a_k \) are integers satisfying

\[
(1.2) \quad (a_1, \ldots, a_k) = 1 \quad \text{and} \quad a_k > 0.
\]

Let \( G(f_k) \) be the least \( s \) such that the equation

\[
(1.3) \quad f_k(x_1) + \ldots + f_k(x_s) = n, \quad x_i \geq 0,
\]
is soluble for all sufficiently large integers \( n \). The problem of estimation for \( G(f_k) \) has been investigated by many authors (see Wooley [6] for references). Here we remark only that Hua [3] has shown that \( G(f_k) \leq (k-1)2^{k+1} \); and, if

\[
(1.4) \quad H_k(x) = 2^{k-1} F_k(x) - 2^{k-2} F_{k-1}(x) + \ldots + (-1)^{k-1} F_1(x), \quad k \geq 4,
\]

then \( G(H_k) = 2^k - \frac{1}{2}(1 - (-1)^k) \). In [3] Hua conjectured further that generally

\[
(1.5) \quad G(f_k) \leq 2^k - \frac{1}{2}(1 - (-1)^k).
\]

This was confirmed in [7] for \( k = 4, 5 \) and \( 6 \). The purpose of this paper is to prove that (1.5) is true for all \( k \geq 7 \). In fact, we prove the following slightly more precise result.

**Theorem 1.** Let \( H_k(x) \) be as in (1.4). For \( k \geq 6 \), if \( f_k(x) \) satisfies

\[
(1.6) \quad 2 \nmid f_k(1) \quad \text{and} \quad f_k(x) \equiv (-1)^{k-1} f_k(1) H_k(x) \pmod{2^k} \quad \text{for any} \ x,
\]

1991 Mathematics Subject Classification: Primary 11P05.

Project supported by the National Natural Science Foundation of China.

[245]
then \(G(f_k) = 2^k - 1\) for odd \(k\) and \(2^k - 1\) or \(2^k\) for even \(k\); otherwise,
\[
G(f_k) \leq 2^{k-1} + 4(k - 1).
\]

In order to investigate the solubility of (1.3), we define
\[S^*(f_k)\]

as the least number such that if \(s \geq S^*(f_k)\) then \(S_s(f_k, n) \geq c\) for some positive \(c\) independent of \(n\), where \(S_s(f_k, n)\) is the singular series corresponding to the equation (1.3) (see Hua [2] and the remark of Wooley [6]). We also define \(G^*(f_k)\) to be the least number \(s\) with the property that all sufficiently large numbers \(n\) with \(S_s(f_k, n) \geq c\) are represented in the form (1.3). From earlier works on \(G^*(f_k)\) (see Hua [4]) we have, in particular,
\[
(1.7) \quad G^*(f_k) < 2^{k-1} + 4(k - 1) \quad \text{for} \quad k \geq 6.
\]

(We remark that very sharp estimates on \(G^*(f_k)\) for large \(k\) have recently been obtained by Wooley [6].) Therefore, in view of (1.7) and (2.9) below, to prove Theorem 1 it suffices to prove the following result.

**Theorem 2.** For \(k \geq 6\), if \(f_k(x)\) satisfies (1.6), then \(S^*(f_k) \leq 2^k - \frac{1}{2}(1 - (-1)^k)\); otherwise, \(S^*(f_k) \leq 2^{k-1} + 4(k - 1)\).

We note that, for quartic and quintic polynomials, more precise results on \(S^*(f_k)\) have been established in [7] and [8]:

If \(f_k(x)\) (\(k = 4\) and 5) does not satisfy (1.6), then
\[
\max_{f_4} S^*(f_4) = 11 \quad \text{and} \quad \max_{f_5} S^*(f_5) = 16.
\]

**2. Notation and preliminary results.** Let \(f_k(x)\) be as in (1.1), and let \(d\) be the least common denominator of the coefficients of \(f_k(x)\). For each prime \(p\), we define \(t = t(f_k, p)\) by \(p^t \parallel d\). Let \(\theta = \theta(f_k, p)\) be the greatest integer such that
\[
(2.1) \quad p^t f_k'(x) \equiv 0 \pmod{p^\theta}\quad \text{for any } x,
\]

and let \(f_k^*(x) = p^{-\theta} p^t f_k'(x)\). Define the integer \(\delta = \delta(p, k)\) by
\[
(2.2) \quad p^\delta \leq k - 1 < p^{\delta+1},
\]

and let
\[
(2.3) \quad \gamma = \gamma(f_k, p) = \begin{cases} \theta - t + \delta + 2 & \text{for } p = 2, \\ \theta - t + \delta + 1 & \text{for } p > 2. \end{cases}
\]

We record for later use that (see Hua [3, Lemma 3.3])
\[
(2.4) \quad \gamma \leq k + \delta + 1 \quad \text{for } p = 2 \quad \text{and} \quad \gamma \leq \left\lfloor \frac{k}{p-1} \right\rfloor + \delta + 1 \quad \text{for } p \geq 3.
\]

Let \(M_s(f_k, p^l, n)\) denote the number of solutions of the congruence
\[
(2.5) \quad f_k(x_1) + \ldots + f_k(x_s) \equiv n \pmod{p^l}, \quad 0 \leq x_i < p^{l+t},
\]
and let $\Gamma(f_k, p')$ be the least value of $s$ for which (2.5) is soluble for every $n$. From Hua [2, Section 7] we see that, if $s \geq 2k + 1$, to establish $\mathcal{S}(f_k) \leq s$ it suffices to show that for all primes $p$ and any integers $n$ and $l \geq c$,

$$M_s(f_k, p^l, n) \geq p^{(s-1)(l-c)},$$

where $c$ is a positive constant depending only on $f_k(x)$. Since a direct treatment of (2.6) presents certain technical difficulties, we define $N_s(f_k, p^l, n)$ to be the number of solutions of the congruence (2.5) with the $f_k(x_i)$ not all divisible by $p$. Then (see [2, Lemma 7.6])

$$N_s(f_k, p^l, n) = p^{(s-1)(l-\gamma)}N_s(f_k, p^γ, n) \quad \text{for } l \geq \gamma.$$

Let $\Gamma^*(f_k, p^γ, n)$ be the least $s$ such that $N_s(f_k, p^γ, n) \geq 1$. Then, by (2.7) and $M_s(f_k, p^l, n) \geq N_s(f_k, p^l, n)$, (2.6) holds (with $c = \gamma$) when $s = \Gamma^*(f_k, p^γ, n)$. Moreover, we define $\Gamma^*(f_k, p^γ) = \max_n \Gamma^*(f_k, p^γ, n)$. Then, in particular, when $s = \Gamma^*(f_k, p^γ)$ the congruence (2.5) is soluble for any $n$ and $l \geq 1$. Also, by the definition, we have

$$\Gamma(f_k, p^γ) \leq \Gamma^*(f_k, p^γ) \leq \Gamma(f_k, p^γ) + 1.$$

Now we see that to prove Theorem 2, it suffices to establish the following two results.

**Theorem 3.** Suppose $k \geq 6$.

(i) If $f_k(x)$ satisfies (1.6), then

$$\Gamma(f_k, 2^k) = 2^{2k} - 1;$$

and, when $s = 2^{k} - \frac{1}{2}(1 - (-1)^k)$, we have

$$M_s(f_k, 2^l, n) \geq 2^{(s-1)(l-2k)} \quad \text{for all } n \text{ and } l \geq 2k.$$

(ii) Otherwise, we have $\Gamma^*(f_k, 2^γ) \leq 2^{2k-1} + 4(k - 1)$.

**Theorem 4.** For $k \geq 6$ and prime $p \geq 3$, we have

$$\Gamma^*(f_k, p^γ) \leq 2^{2k-1} + 4(k - 1).$$

Our proof of Theorems 3 and 4 is motivated by Hua [3] and Yu [7] (see Sections 3 to 5 of this paper). Before proceeding further we record two lemmas. Lemma 2.1 (below) may be compared with Hua [3, Lemmas 4.4 and 4.5]. It follows from (1.1) and a simple calculation. Lemma 2.2 can be seen from the proof of Hua [3, Lemma 3.2] (see also Lovász [5, Problem 1.43(e)].)

**Lemma 2.1.** Let $f_k(x)$ be as in (1.1). Then

(i) $f_k(x + 2) - f_k(x) = 2a_kF_{k-1}(x) + \sum_{i=1}^{k-1}(2a_i + a_{i+1})F_i-1(x)$ with $F_0(x)$ being interpreted as 1.

(ii) $f_k(x + 1) + f_k(x) - f_k(1) = 2a_kF_k(x) + \sum_{i=1}^{k-1}(2a_i + a_{i+1})F_i(x).$
Lemma 2.2. Let

\[ P_m(x) = \sum_{i=1}^{m} \alpha_i F_i(x) \]

and write \( P'_m(x) = \sum_{i=0}^{m-1} \beta_i F_i(x) \). Then \( \beta_i \) \((0 \leq i \leq m-1)\) are given by

\[ \beta_i = (-1)^{m-i-1} \left( \frac{\alpha_m}{m-i} - \frac{\alpha_{m-1}}{m-i+1} + \ldots + (-1)^{m-i-1} \alpha_{i+1} \right). \]

3. Proof of Theorem 3(i). In this section, we will use the notation introduced in Section 2 for \( p = 2 \) only. Moreover, for an integral-valued polynomial \( Q(x) \), we will define \((p = 2)\)

\[ t(Q), \theta(Q), \gamma(Q) \] and \( Q^*(x) \) in the same way as \( t = t(f_k, 2), \theta = \theta(f_k, 2), \gamma = \gamma(f_k, 2) \) and \( f^*_k(x) \) for \( f_k(x) \) in Section 2.

Suppose that \( f_k(x) \) satisfies (1.6). Without loss of generality we may assume that \( a_1 = f_k(1) = (-1)^{k-1} \). Then, by (1.1) and (1.6),

\[ a_i \equiv (-1)^{k-i} 2^{i-1} \pmod{2^k} \quad (2 \leq i \leq k). \]

It follows that

\[ \sum_{i=1}^{k} \alpha_i F_i(x) \]

(3.1) \( 2^k \| 2a_k \) and \( 2^k \| (2a_i + a_{i+1}) \) \((1 \leq i \leq k-1)\).

By Lemma 2.1(i) and (3.2), we have

\[ f_k(x+2) - f_k(x) \equiv 0 \pmod{2^k} \quad \text{for any } x. \]

Thus \( f_k(x) \) takes only two different values, 0 and \((-1)^{k-1}, \mod{2^k}, \) and then (2.9) follows.

Let

\[ G_k(x) = 2^{-k}(f_k(x+1) + f_k(x) - (-1)^{k-1}) \]

and write

\[ G_k(x) = \sum_{i=1}^{k} b_i F_i(x). \]

(3.5)

By Lemma 2.1(ii) and (3.2), \( b_i \) \((1 \leq i \leq k)\) are integers and \( 2 \nmid b_k \).

Define integers \( \tau \) and \( \sigma \) by \( 2^\tau \| \| k! \) and \( 2^\tau \leq k < 2^{\tau+1} \). Since \( 2 \nmid b_k \), we have \( t(G_k) = \tau \), and hence \( \theta(G_k) = \tau - \sigma \) by Lemma 2.2. Thus \( G^*_k(x) = 2^\sigma G^*_k(x) \), and so

\[ G^*_k(x) = 2^{-(k-\sigma)}(f'_k(x+1) + f'_k(x)) \]

by (3.4). Furthermore, writing

\[ G^*_k(x) = \sum_{i=0}^{k-1} c_i F_i(x) \]

(3.7)
with 2-adic integral $c_i$ ($0 \leq i \leq k - 1$), we see from Lemma 2.2 that

\begin{equation}
    c_i \equiv \begin{cases} 
    0 & \text{mod } 2 \text{ for } i > k - 2^\sigma, \\
    b_{i+2^\sigma} & \text{mod } 2 \text{ for } 0 \leq i \leq k - 2^\sigma.
    \end{cases}
\end{equation}

The following result is an analogue of Hua [3, Theorem 4].

**Lemma 3.1.** (i) The congruence

$$G_k(x) \equiv A \pmod{2^l}, \quad 2 \nmid G_k^*(x),$$

is soluble for any $A$ and $l \geq 1$.

(ii) If $2 \nmid G_k^*(x_0)$ for some $x_0$, then either $2 \nmid f_k^*(x_0)$ or $2 \nmid f_k^*(x_0 + 1)$.

**Proof.** We prove that, for any integers $x,y$ and $m \geq 0$,

\begin{equation}
    G_k(x + 2^m \sigma y) - G_k(x) \equiv 2^m y G_k^*(x) \pmod{2^{m+1}}
\end{equation}

and

\begin{equation}
    G_k^*(x + 2^m \sigma y) \equiv G_k^*(x) \pmod{2^{m+1}}.
\end{equation}

This suffices to prove part (i) by induction on $l$ (when $l = 1$ the result follows immediately from (3.9) and (3.10) with $m = 0$).

We now prove (3.9). By Vandermonde’s identity (see Lovász [5, Problem 1.45]), we have for $1 \leq i \leq k$,

$$F_i(x + 2^m \sigma y) - F_i(x) = \sum_{j=1}^{i} \binom{2^m \sigma y}{j} F_{i-j}(x).$$

It is easily seen that, for any integer $y$,

$$\binom{2^m \sigma y}{2^\sigma} \equiv 2^m \pmod{2^{m+1}}$$

and

$$\binom{2^m \sigma y}{j} \equiv 0 \pmod{2^{m+1}} \text{ for } j \neq 2^\sigma$$

(note $j \leq k < 2^{\sigma+1}$). Hence

$$F_i(x + 2^m \sigma y) - F_i(x) \equiv 2^m y F_{i-2^\sigma}(x) \pmod{2^{m+1}}$$

for any integers $x$ and $y$ (where $F_i(x)$ with $j < 0$ is interpreted to be 0). From this, (3.5), (3.7) and (3.8) we have

$$G_k(x + 2^m \sigma y) - G_k(x) \equiv \sum_{i=1}^{k} 2^m y b_i F_{i-2^\sigma}(x) \equiv \sum_{i=0}^{k-2^\sigma} 2^m y b_{i+2^\sigma} F_{i}(x)$$

$$\equiv \sum_{i=0}^{k-2^\sigma} 2^m y c_i F_{i}(x) \equiv 2^m y G_k^*(x) \pmod{2^{m+1}},$$

as required. (3.10) can be proved similarly.
To prove (ii), we note that now \( t = 0 \), so (3.6) implies that \( \theta \leq k - \sigma \). If \( \theta = k - \sigma \), then \( G_k = f_k(x + 1) + f_k(x) \), and the result follows at once. Suppose that \( \theta \leq k - \sigma - 1 \). By (3.2), Lemmas 2.1(i) and 2.2 we have

\[
(3.11) \quad f_k(x + 2) - f_k(x) \equiv 0 \pmod{2^{k-\delta}} \quad \text{for any } x.
\]

(Recall that in this section \( \delta \) satisfies \( 2^\delta \leq k - 1 < 2^{\delta+1} \).) Clearly \( \delta \leq \sigma \), so that \( 2^{\theta + 1} \mid 2^{k-\delta} \). It follows from (3.11) that \( 2 \mid f_k(x) \) either for all odd \( x \) or for all even \( x \), and therefore the desired result also follows.

Our next step is to establish the results analogous to Hua [3, Lemmas 4.6–4.8]. We define

\[
E_k(x) = 2^{-k}f_k(2x) \quad \text{and} \quad O_k(x) = 2^{-k}(f_k(2x + 1) - (-1)^{k-1}).
\]

By (3.3), both \( E_k(x) \) and \( O_k(x) \) are integral-valued polynomials. We write

\[
E_k(x) = \sum_{i=1}^{k} d_i F_i(x) \quad \text{and} \quad O_k(x) = \sum_{i=1}^{k} d_i' F_i(x).
\]

**Lemma 3.2.** (i) If \( k \geq 7 \) is odd, then neither \( E_k(x) \) nor \( O_k(x) \) is constant modulo 2, and \( \gamma(E_k) \leq (k - 1)/2 + \delta \) and \( \gamma(O_k) \leq (k - 1)/2 + \delta \).

(ii) If \( k \geq 8 \) is even, then either \( E_k(x) \) is not constant modulo 2 and \( \gamma(E_k) \leq k/2 + \delta \) or \( O_k(x) \) is not constant modulo 2 and \( \gamma(O_k) \leq k/2 + \delta \).

**Proof.** From Kemmer’s identity (see Gupta [1, Chapter 8, §9.2]) it follows that

\[
F_i(2x) = \sum_{l \leq i} 2^{2i-l}(\binom{i}{l-i}) F_i(x) \quad \text{for any } x.
\]

Then by (1.1) we have

\[
(3.14) \quad f_k(2x) = \sum_{i=1}^{k} F_i(x) \sum_{l=i}^{\min(2i,k)} a_i 2^{2i-l}(\binom{i}{l-i}).
\]

This, together with \( F_i(2x + 1) = F_i(2x) + F_{i-1}(2x) \), gives

\[
(3.15) \quad f_k(2x + 1) - (-1)^{k-1}
\]

\[
= f_k(2x) + \sum_{i=1}^{k-1} F_i(x) \sum_{l=i}^{\min(2i,k-1)} a_i 2^{2i-l}(\binom{i}{l-i}).
\]

Now by (3.1) and (3.12) to (3.15) we see that

\[
(3.16) \quad 2^{k-1} \mid (d_k, d_k') \quad \text{and} \quad 2^{k-3} \mid (d_{k-1}, d_{k-1}').
\]

Also, we have \( 2 \mid d_{(k+1)/2} \) and \( 2 \mid d_{(k+1)/2}' \) for odd \( k \), thus the first assertion of (i) follows. Further, by \( 2 \mid d_{(k+1)/2} \), (3.16) and Lemma 2.2, it can be proved easily that \( \theta(E_k) \leq k - (k + 1)/2 - 2 + t(E_k) \) for \( k \geq 7 \) (cf. the proof of Hua
Waring’s problem

Thus \( \gamma(E_k) \leq (k-1)/2 + \delta \) (cf. (2.3)). The same argument gives \( \gamma(O_k) \leq (k-1)/2 + \delta \).

If \( k \) is even, then either \( 2 \nmid d_k / 2 \) or \( 2 \nmid d_k' / 2 \). The assertions of (ii) follow as above.

We are now in a position to prove the second assertion of Theorem 3(i).

(I) \( k \) is odd. Let \( s = 2^k - 1 \), and for any \( n \) let \( r_n \) be the integer satisfying \( n \equiv r_n \pmod{2^k} \) and \( 0 \leq r_n < 2^k \). We consider several cases.

(i) \( 1 \leq r_n \leq 2^k - 2 \). By Lemma 3.1(i) the congruence

\[
G_k(x) + \sum_{i=2}^{r_n} O_k(y_i) \equiv m \pmod{2^l}, \quad 2 \nmid G_k^*(x),
\]

is soluble for any \( m, y_i \) (\( 2 \leq i \leq r_n \)) and \( l \geq 1 \). Hence in case (i) we have, by (3.4), (3.12) and Lemma 3.1(ii),

\[
\Gamma^*(f_k, 2^\gamma, n) \leq r_n + 1 \leq 2^k - 1,
\]

which implies that \( N_s(f_k, 2^\gamma, n) \geq 1 \), and the result follows immediately (cf. Section 2 and note that \( \gamma < 2k \) by (2.4) for \( p = 2 \)).

(ii) \( r_n = 0 \). We note that, by Lemma 3.2(i), \( s > 2^{\gamma(E_k)} \) for \( k \geq 7 \). Thus, by the Davenport–Chowla lemma (cf. [7, Lemma 2.2]), for \( l = \gamma(E_k) \) the congruence

\[
\sum_{i=1}^{s} E_k(x_i) \equiv m \pmod{2^l}
\]

has a solution with \( 2 \nmid E_k^*(x_1) \), i.e. \( N_s(E_k, 2^{\gamma(E_k)}, m) \geq 1 \), for any \( m \). Thus the number \( M_s(E_k, 2^k, m) \) of solutions of the congruence (3.17) is at least \( 2^{(s-1)/(l-\gamma(E_k))} \) for all \( m \) and \( l \geq k > \gamma(E_k) \) (cf. Section 2). Hence, in view of (3.12), the result holds in case (ii).

(iii) \( r_n = 2^k - 1 \). The same argument as in (ii) with \( E_k(x) \) replaced by \( O_k(x) \) shows that \( N_s(O_k, 2^{\gamma(O_k)}, m) \geq 1 \) for all \( m \), and the result also follows in case (iii).

(II) \( k \) is even. When \( k = 6 \) the result has been proved in [7]. For \( k \geq 8 \) let \( s = 2^k \), and for any \( n \) let \( r_n \) be the integer satisfying \( n \equiv -r_n \pmod{2^k} \) and \( 0 \leq r_n < 2^k \).

When \( 1 \leq r_n \leq 2^k - 1 \), in a similar way to (I)(i), we have \( \Gamma^*(f_k, 2^\gamma, n) \leq r_n + 1 \leq 2^k \) and hence the result. Moreover, by Lemma 3.2(ii) and a similar argument to (I)(ii), it is easily seen that either \( N_s(E_k, 2^{\gamma(E_k)}, m) \geq 1 \) or \( N_s(O_k, 2^{\gamma(O_k)}, m) \geq 1 \), for all \( m \). Thus for \( r_n = 0 \) the desired result also holds.

The proof of Theorem 3(i) is now complete.
4. Proof of Theorem 3(ii). We need the following simple lemma.

LEMMA 4.1. Let $\lambda$ be the greatest integer such that
\[ f_k(x + 2) - f_k(x) \equiv 0 \pmod{2^{\lambda}} \text{ for any } x. \]
Then $\lambda \leq k$, and equality holds if and only if $f_k(x)$ satisfies (1.6).

Proof. By Lemma 2.1(i), we have
\[ 2a_k \equiv 0 \pmod{2^{\lambda}} \quad \text{and} \quad 2a_i + a_{i+1} \equiv 0 \pmod{2^{\lambda}} \quad (1 \leq i \leq k-1). \]
Then by contradiction and (1.2) it follows that $\lambda \leq k$. Further, if $\lambda = k$, then it is easily seen by (4.1) and induction on $i$ that $a_i \equiv (-2)^{i-1}a_1 \pmod{2^k}$ for $2 \leq i \leq k$. Hence (1.6) follows. The converse result has already been proved in Section 3 (cf. (3.3)).

We now prove Theorem 3(ii) by induction. We note that by Yu [7, Section 5] both (i) and (ii) of Theorem 3 hold for $k = 5$. Suppose that $k \geq 6$ and that Theorem 3(ii) is true for polynomials of degree $k - 1$. We then prove
\[ \Gamma(f_k, 2^\gamma) \leq 2^{k-1} + 4(k-1) - 1 \]
for any $f_k(x)$ not satisfying (1.6), which, in view of (2.8), completes our proof.

Since $f_k(x)$ does not satisfy (1.6), we have $\lambda \leq k - 1$ by Lemma 4.1. If $\gamma \leq \lambda$ the result is trivial. Thus we may assume that $\gamma > \lambda$. By the definition of $\lambda$, there exists an integer $x_0$ such that $f_k(x_0 + 2) - f_k(x_0) \not\equiv 0 \pmod{2^{\lambda+1}}$. By the Davenport–Chowla lemma we see that, when $l = 2^\lambda - 1$, the congruence
\[ f_k(x_1) + \ldots + f_k(x_l) \equiv n - mf_k(x_0) \pmod{2^{\lambda}} \]
is soluble for any $m$ and $n$.

The next step is to consider the solubility of the congruence
\[ f_k(x_0 + 2y_1) + \ldots + f_k(x_0 + 2y_m) \equiv mf_k(x_0) + 2^\lambda A \pmod{2^\gamma} \]
for any $A$. We write
\[ g_k(y) = 2^{-\lambda}(f_k(x_0 + 2y) - f_k(x_0)); \]
then (4.4) is equivalent to
\[ g_k(y_1) + \ldots + g_k(y_m) \equiv A \pmod{2^{\gamma-\lambda}}. \]
Note that $g_k(y)$ is an integral-valued polynomial. Also, $g_k(0) = 0$ and $g_k(1) \not\equiv 0 \pmod{2}$, so that $g_k(y) \pmod{2}$ is not constant. Thus, when $m = 2^{\gamma-\lambda} - 1$ the congruence (4.6) is soluble for any $A$. Then, by (4.3) and (4.4) we have (cf. [7, Lemma 2.3])
\[ \Gamma(f_k, 2^\gamma) \leq (2^\lambda - 1) + (2^{\gamma-\lambda} - 1) = 2^\lambda + 2^{\gamma-\lambda} - 2. \]
On the other hand, by (1.1), (4.5) and Taylor’s expansion we see that the coefficient of \( y^k \) in \( g_k(y) \) is \( a_k \cdot 2^{k-\lambda} / k! \). Then, writing \( g_k(y) = \sum_{i=1}^{k} a_i F_i(y) \), we have \( a'_k = 2^{k-\lambda} a_k \). We define \( \mu \) by \( 2^\mu \parallel a_k \). By (2.1) and Lemma 2.2, \( 2^\theta \parallel 2^\phi a_k \), and so \( \theta \leq t + \mu \). Thus \( a'_k \) is divisible by \( 2 \) to the power \( k-\lambda+\theta-t \), which is greater than or equal to \( \gamma - \lambda \) by (2.2) and (2.3) (for \( p = 2 \)). Thus \( g_k(y) \mod 2^{\gamma-\lambda} \) is a polynomial of degree at most \( k-1 \). Then, by the induction hypothesis and the second assertion of Theorem 3(i), we see that when \( m = 2^{k-1} \) the congruence (4.6) is soluble. Hence

\[
(4.8) \quad \Gamma(f_k, 2^{-\lambda}) \leq (2^\lambda - 1) + 2^{k-1}.
\]

Now (4.2) can be proved easily. Recall \( \lambda \leq k - 1 \). If \( \lambda \geq \delta + 2 \), then the function \( 2^\lambda + 2^{\gamma-\lambda} \) of \( \lambda \) has a maximum value at \( \lambda = \delta + 2 \) or \( \lambda = k - 1 \). It follows from (4.7), (2.2) and (2.4) (for \( p = 2 \)) that

\[
\Gamma(f_k, 2^{-\lambda}) \leq 2^{k-1} + 2^{\delta+2} - 2 \leq 2^{k-1} + 4(k-1) - 2,
\]

as required. If \( \lambda < \delta + 2 \), then (4.8) gives the result at once.

5. Proof of Theorem 4. We note that the case \( p > k \) of Theorem 4 follows readily from Hua [3, Lemma 2.3]. Thus, to prove Theorem 4 it suffices to consider the cases when \( 3 \leq p \leq k \). We proceed by induction on \( k \geq 5 \).

When \( k = 5 \) the result has been proved in Yu [7, Section 6]. Suppose that the assertion of Theorem 4 is true for polynomials of degree \( k - 1 \) \((k \geq 6)\). We then prove

\[
(5.1) \quad \Gamma(f_k, p^{-\lambda}) \leq 2^{k-1} + 4(k-1) - 1 \quad \text{for} \quad 3 \leq p \leq k,
\]

and hence complete the proof. Since the argument of (5.1) is the same as that used in Section 4, we only give a brief sketch.

For \( 3 \leq p \leq k \), define \( \lambda \) to be the greatest integer such that

\[
f_k(x + p) - f_k(x) \equiv 0 \pmod{p^{\lambda}} \quad \text{for any} \quad x.
\]

By Vandermonde’s identity, we have

\[
f_k(x + p) - f_k(x) = \sum_{i=0}^{k-1} F_i(x) \sum_{j=1}^{k-i} a_{i+j} \binom{p}{j}.
\]

From this it can be proved that

\[
(5.2) \quad \lambda \leq \left[ \frac{k-1}{p-1} \right] + 1.
\]

When \( \gamma \leq \lambda \) the result is trivial. We thus assume that \( \gamma > \lambda \). In analogy to (4.7) and (4.8) we have

\[
(5.3) \quad \Gamma(f_k, p^{-\lambda}) \leq p^{\lambda} + p^{\gamma-\lambda} - 2
\]
and (by the induction hypothesis, and using Hua’s result mentioned above if \( p = k \))

\[
\Gamma(f_k, p^\gamma) \leq (p^\lambda - 1) + (2^{k-2} + 4(k - 2)).
\]

If \( \lambda \geq \delta + 1 \), then the function \( p^\lambda + p^{\gamma - \lambda} \) of \( \lambda \) has a maximum value at \( \lambda = \delta + 1 \) or \( \lambda = \left[ \frac{k-1}{p-1} \right] + 1 \) (cf. (5.2)). Then, by (5.3), (2.2) and (2.4) (for \( p \geq 3 \)), it is easily verified that (5.1) holds for \( 6 \leq k \leq 10 \) and

\[
\Gamma(f_k, p^\gamma) < p^{\left\lfloor \frac{k-1}{p-1} \right\rfloor + 1} + p^{\delta + 1} \leq p^{\frac{k-1}{p-1} + 1} + k(k - 1) < 2^{k-1} + 4(k - 1) - 1
\]

for \( k \geq 11 \). If \( \lambda < \delta + 1 \), then (5.1) follows readily from (5.4).

Acknowledgements. The author is grateful to Professor M. G. Lu for suggesting this problem and for his encouragement.

References


Department of Mathematics
University of Science and Technology of China
Hefei, Anhui 230026
The People’s Republic of China
E-mail: yuhb@math.ustc.edu.cn

Received on 1.12.1997