On values of a polynomial at arithmetic progressions with equal products

by

N. SARADHA (Bombay), T. N. SHOREY (Bombay) and R. Tijdeman (Leiden)

1. Introduction. Let $f(X)$ be a monic polynomial of degree $\nu > 0$ with rational coefficients. Let $d_1, d_2, l, m$ with $l < m$ and $\gcd(l, m) = 1$ be given positive integers. In this paper, we consider the equation

\[(1) \quad f(x)f(x+d_1) \cdots f(x+(lk-1)d_1) = f(y)f(y+d_2) \cdots f(y+(mk-1)d_2)\]

in integers $x, y$ and $k \geq 2$ such that

\[(2) \quad f(x+jd_1) \neq 0 \quad \text{for } 0 \leq j \leq lk - 1.\]

We refer to [3] and [4] for an account of results on equation (1) with $f(X) = X$. It was shown in [3] that for positive integers $x, y$ and $k \geq 2$, equation (1) with $f(X) = X$ implies that $\max(x, y, k) \leq C_1$ where $C_1$ is an effectively computable number depending only on $d_1, d_2, m$ unless

\[(3) \quad l = 1, \quad m = k = 2, \quad d_1 = 2d_2^2, \quad x = y^2 + 3d_2y.\]

When $f$ is a power of an irreducible polynomial, it was shown in [1] that equation (1) with $l = d_1 = d_2 = 1$ and (2) implies that $\max(|x|, |y|, k) \leq C_2$ where $C_2$ is an effectively computable number depending only on $m$ and $f$. In this paper, we extend these results as follows.

**Theorem.** (a) Equation (1) with (2) implies that $k$ is bounded by an effectively computable number depending only on $d_1, d_2, m$ and $f$.

(b) Let $f$ be a power of an irreducible polynomial. There exists an effectively computable number $C_3$ depending only on $d_1, d_2, m$ and $f$ such that equation (1) with (2) implies that

\[(4) \quad \max(|x|, |y|, k) \leq C_3\]

unless

\[(5) \quad l = 1, \quad m = k = 2, \quad d_1 = 2d_2^2, \quad f(X) = (X + r)^\nu \quad \text{with } r \in \mathbb{Z}, \quad x + r = (y + r)(y + r + 3d_2).\]
It is clear that condition (2) is necessary. We observe that equation (1) is, in fact, satisfied in the cases given by (5). For irreducible \( f \), we apply Theorem (b) to \( f^2 \) for deriving that if \( x, y \) and \( k \geq 2 \) are integers satisfying (2) and

\[
|f(x)f(x + d_1) \ldots f(x + (lk - 1)d_1)| = |f(y)f(y + d_2) \ldots f(y + (mk - 1)d_2)|
\]

then \( \max(|x|, |y|, k) \) is bounded by an effectively computable number depending only on \( d_1, d_2, m \) and \( f \) unless (5) holds. In particular, we observe that if \( x, y \) and \( k \geq 2 \) are integers satisfying \( x + jd_1 \neq 0 \) for \( 0 \leq j \leq lk - 1 \) and

\[
x(x + d_1) \ldots (x + (lk - 1)d_1) = \pm y(y + d_2) \ldots (y + (mk - 1)d_2)
\]

then \( \max(|x|, |y|, k) \) is bounded by an effectively computable number depending only on \( d_1, d_2 \) and \( m \), unless (3) holds.

2. Notation. Let \( \{\alpha_1, \alpha_2, \ldots, \alpha_\nu\} \) be the roots of \( f \) and we assume without loss of generality that \( |\alpha_1| \geq |\alpha_2| \geq \ldots \geq |\alpha_\nu| \). Let \( a_0 \) be the absolute value of the product of the denominators of the coefficients of \( f \). We observe that \( a_0\alpha_1, \ldots, a_0\alpha_\nu \) are algebraic integers. We define the coefficients \( A_0, A_1, \ldots \) and \( B_0, B_1, \ldots \) by

\[
X^{-l} \prod_{j=0}^{lk-1} (f(X + jd_1))^{1/(\nu k)} = \prod_{i=1}^{\nu} \prod_{j=0}^{lk-1} \left(1 + \frac{jd_1 - \alpha_i}{X}\right)^{1/(\nu k)} = \sum_{n=0}^{\infty} A_n d_1^n X^{-n}
\]

and

\[
Y^{-m} \prod_{j=0}^{mk-1} (f(Y + jd_2))^{1/(\nu k)} = \prod_{i=1}^{\nu} \prod_{j=0}^{mk-1} \left(1 + \frac{jd_2 - \alpha_i}{Y}\right)^{1/(\nu k)}
= \sum_{n=0}^{\infty} B_n d_2^n Y^{-n}.
\]

We observe that for \( n \geq 1 \), \( A_n \) and \( B_n \) are rational numbers and that \( A_0 = B_0 = 1 \). We put

\[
\chi_n = ((a_0\nu k)n)!^n \quad \text{for } n = 0, 1, 2, \ldots
\]

Further, we write

\[
F(X) = X^l + A_1 d_1 X^{l-1} + \ldots + A_ld_1^l,
\]
\[
G(Y) = Y^m + B_1 d_2 Y^{m-1} + \ldots + B_m d_2^m
\]

and

\[
L(X, Y) = F(X) - G(Y).
\]

We notice that \( F(X) \) and \( G(Y) \) are the polynomial parts of the \( \nu k \)th root of left and right hand sides of equation (1), respectively, with \( x \) and \( y \) re-
Values of a polynomial at arithmetic progressions

placed by $X$ and $Y$. For a rational number $\beta$, we write $d(\beta)$ for the least positive integer such that $d(\beta)\beta$ is a rational integer. We denote by $c_1, c_2, \ldots$ effectively computable positive numbers depending on $d_1, d_2, m$ and $f$.

3. $k$ is bounded. In this section, we shall show that equation (1) with (2) implies that $k \leq c_1$. The proof is similar to that of Theorem 2 of [1]. Therefore, we mention only the main steps of the proof and the readers are referred to [1] for details. We assume that equation (1) with (2) is satisfied. Then we observe that

$$|x|^l \leq c_2(|y| + mkd_2)^m, \quad |y|^m \leq c_3(|x| + lkd_1)^l. \tag{6}$$

For $n \geq 0$, $A_n$ and $B_n$ are polynomials in $k$ of degrees not exceeding $n$ satisfying

$$|A_n|d_1^n \leq 2^{n+l}(lkd_1 + |\alpha_1|)^n, \quad |B_n|d_2^n \leq 2^{n+m}(mkd_2 + |\alpha_1|)^n$$

and

$$d(A_n d_1^n) | \chi_n, \quad d(B_n d_2^n) | \chi_n.$$ 

Further, we obtain

$$\log(|y| + 2) \geq c_4 k. \tag{7}$$

For the proof of (7), we take prime $p$ of Lemma 4 of [1] exceeding $a_0 d_1 d_2$ in place of $a_0$.

We assume from now onward that $|y| > c_5$ with $c_5$ sufficiently large, otherwise (4) follows from (7) and (6). By taking $\nu k$th root on both the sides of equation (1), we have

$$x^l \left(1 + \frac{A_1 d_1}{x} + \frac{A_2 d_1^2}{x^2} + \ldots \right) = y^m \left(1 + \frac{B_1 d_2}{y} + \frac{B_2 d_2^2}{y^2} + \ldots \right).$$

This implies that

$$F(x) = G(y). \tag{8}$$

Further, we show that

$$A_{l+1} = \ldots = A_{2l-1} = 0 \quad \text{or} \quad B_{m+1} = \ldots = B_{2m-1} = 0. \tag{9}$$

We prove (9) by contradiction. If not, there exist integers $I$ and $J$ with $1 \leq I < l$ and $1 \leq J < m$ such that

$$A_{l+1} = \ldots = A_{l+I-1} = 0, \quad A_{l+I} \neq 0$$

and

$$B_{m+1} = \ldots = B_{m+J-1} = 0, \quad B_{m+J} \neq 0.$$ 

Then we derive that

$$\frac{A_{l+I} d_1^{l+I}}{x^I} + \ldots = \frac{B_{m+J} d_2^{m+J}}{y^J} + \ldots,$$
which implies that \( mI = lJ \). This is not possible since \( \gcd(l, m) = 1 \) and \( J < m \). Further, we derive from (8) and (9) that

\[
A_{l+1} = \ldots = A_{2l-1} = 0, \quad B_{m+1} = \ldots = B_{2m-1} = 0
\]

and

\[
B_{2m}d_2^{2m} = A_{2l}d_1^{2l}.
\]

Finally, we apply the proof of §4 of [1] for deriving from the above relations that \( k \leq c_1 \). This completes the proof of Theorem (a).

4. Proof of Theorem (b). We assume that equation (1) with (2) is satisfied. Then, by Theorem (a), we restrict ourselves to \( k \leq c_1 \). Let \( k \) be fixed. By (6), we may assume that \( |x| > c_5 \) and \( |y| > c_5 \) with \( c_5 \) sufficiently large. Then the relation (8) is valid. Let \( f = g_1^b \), where \( g_1 \) is irreducible and \( b \) is a positive integer. Then \( g_1 \) has rational coefficients and its leading coefficient is \( \pm 1 \). By putting \( f = g_1^b \) in (1), we have

\[
(g_1(x)g_1(x + d_1) \ldots g_1(x + (lk - 1)d_1))^b = (g_1(y)g_1(y + d_2) \ldots g_1(y + (mk - 1)d_2))^b.
\]

Taking the \( b \)th root on either side, we see that

\[
g_1(x)g_1(x + d_1) \ldots g_1(x + (lk - 1)d_1) = \pm g_1(y)g_1(y + d_2) \ldots g_1(y + (mk - 1)d_2).
\]

Now, we set \( g_1(x) = g(x) \) if \( g_1 \) is monic and \( g_1(x) = -g(x) \) if \( g_1 \) has leading coefficient \(-1\) so that \( g \) is a monic irreducible polynomial with rational coefficients. Then the latter equation is valid with \( g_1 \) replaced by \( g \). Thus we assume that either \( f = g \) or \( f = g^2 \) in Theorem (b). Put \( \delta = 1 \) if \( f = g \) and \( \delta = 2 \) if \( f = g^2 \). Let \( \mu \) be the degree of \( g \). Thus \( \mu = \nu/\delta \). Let \( \beta_1, \ldots, \beta_\mu \) be the roots of \( g, K = \mathbb{Q}(\beta_1, \ldots, \beta_\mu) \) and we write \( a \) for the coefficient of \( X^{\mu-1} \) in \( g(X) \). Further, let \( \sigma_1, \ldots, \sigma_\mu \) be all the automorphisms of \( K \) and we write \( \sigma_q(\beta) = \beta^{(q)} \) for \( \beta \in K \) and \( 1 \leq q \leq \mu \). We set

\[
H(X, Y) = (g(X) \ldots g(X + (lk - 1)d_1))^\delta - (g(Y) \ldots g(Y + (mk - 1)d_2))^\delta,
\]

\[
T = \{ \beta_i - Jd_1 \mid 1 \leq i \leq \mu, \ 0 \leq J < lk \}
\]

and

\[
U = \{ \beta_i - Jd_2 \mid 1 \leq i \leq \mu, \ 0 \leq J < mk \}.
\]

Since \( g \) is irreducible, we observe that \( |T| = lk\mu \) and \( |U| = mk\mu \). For \( t = \beta_i - Jd_1 \in T \), we write \( \overline{t} = Jd_1 \). Similarly, for \( u = \beta_i - Jd_2 \in U \), we write \( \overline{u} = Jd_2 \).

Let \( R(Y) \) be the resultant of \( H(X, Y) \) and \( L(X, Y) \) with respect to \( X \). Then we observe from equations (1) and (8) that \( R(y) = 0 \), which implies that \( R(Y) \equiv 0 \) if \( c_5 \) is sufficiently large. By a result of Ehrenfeucht (see
of these polynomials divides \( g \) and further, we have
\[
\prod_{i=1}^{s} (F(X) - v_i^\prime) = (F(X))^s + A'_1(F(X))^{s-1} + \ldots + A'_s
\]
and
\[
\prod_{i=1}^{s} (G(Y) - v_i^\prime) = (G(Y))^s + B'_1(G(Y))^{s-1} + \ldots + B'_s.
\]
As \( g(x)g(x+d_1) \ldots g(x+(l-1)d_1) = \pm g(y)g(y+d_2) \ldots g(y+(m-1)d_2) \),
by (8) we have either
\[
(A'_1 - B'_1)(F(x))^{s-1} + \ldots + (A'_s - B'_s) = 0
\]
or
\[
2(F(x))^s + (A'_1 + B'_1)(F(x))^{s-1} + \ldots + (A'_s + B'_s) = 0.
\]
If \( c_0 \) is sufficiently large, the latter possibility is excluded and the former
possibility implies that \( A'_1 = B'_1, \ldots, A'_s = B'_s \). Consequently, we conclude
that
\[ \{v'_1, \ldots, v'_s\} = \{v''_1, \ldots, v''_s\}. \]

By rearrangement, if necessary, we may assume without loss of generality that \( v'_i = v''_i =: v_i \) for \( 1 \leq i \leq s \) and we write \( S = \{v_1, \ldots, v_s\} \). Then we have

\[(10) \quad F(X) - v_i = (X - t_{i,1}) \ldots (X - t_{i,l}) \quad \text{for} \quad 1 \leq i \leq s \]

and

\[(11) \quad G(Y) - v_i = (Y - u_{i,1}) \ldots (Y - u_{i,m}) \quad \text{for} \quad 1 \leq i \leq s, \]

where \( t_{i,p} = \gamma_{i,p} - \bar{t}_{i,p} \) for \( 1 \leq p \leq l \) and \( u_{i,h} = \beta_{i,h} - \bar{u}_{i,h} \) for \( 1 \leq h \leq m \).

Here \( \gamma_{i,p} \) and \( \beta_{i,h} \) belong to \( \{\beta_1, \ldots, \beta_p\} \).

We now fix \( i \) with \( 1 \leq i \leq s \) and let \( r \) be the number of automorphisms of \( K \) which fix \( v_i \). By re-arranging \( \sigma_1, \ldots, \sigma_\mu \), there is no loss of generality in assuming that \( \sigma_q(v_i) = v_i^{(q)} = v_i \) for \( 1 \leq q \leq r \). The sets \( \{\sigma_q(t_{i,p}) \mid 1 \leq q \leq r\} \) for \( 1 \leq p \leq l \) are either disjoint or identical. Consequently, by considering the images under \( \sigma_q \) with \( 1 \leq q \leq r \) on both sides of (10), we observe that the number of times \( \bar{t}_{i,p} \) with \( 1 \leq p \leq l \) occurs in \( \{\bar{t}_{i,1}, \ldots, \bar{t}_{i,l}\} \) is a multiple of \( r \). Consequently, we derive that \( l \) is a multiple of \( r \). Similarly, by considering (11) and arguing as above, we derive that \( m \) is also a multiple of \( r \). Since \( \gcd(l, m) = 1 \), we have \( r = 1 \). In other words, every element of \( S \) has \( \mu \) distinct conjugates. Therefore, the maximal number of elements of \( S \) such that no two of them are conjugates is precisely \( k \). By re-arranging elements of \( S \), we may assume that \( v_1, \ldots, v_k \) are such that no two of them are conjugates. Then we derive from (10) and (11) that \( \bar{t}_{i,p} \) with \( 1 \leq i \leq k, 1 \leq p \leq l \) are pairwise distinct elements of the set \( \{\bar{J}d_1 \mid 0 \leq J < lk\} \) and \( \bar{u}_{i,h} \) with \( 1 \leq i \leq k, 1 \leq h \leq m \) are pairwise distinct elements of the set \( \{\bar{J}d_2 \mid 0 \leq J < mk\} \). By subtracting (10) with \( X = x \) from (11) with \( Y = y \) and taking norms over \( K \), we derive that

\[ (12) \quad g(x + \bar{t}_{i,1}) \ldots g(x + \bar{t}_{i,l}) = g(y + \bar{u}_{i,1}) \ldots g(y + \bar{u}_{i,m}) \quad \text{for} \quad 1 \leq i \leq k. \]

Let \( 1 \leq i, j \leq k \) with \( i \neq j \). This is possible since \( k \geq 2 \). We derive from (12) that

\[ \begin{align*}
\frac{g(x + \bar{t}_{i,1}) \ldots g(x + \bar{t}_{i,l})}{g(x + \bar{t}_{j,1}) \ldots g(x + \bar{t}_{j,l})} &= \frac{g(y + \bar{u}_{i,1}) \ldots g(y + \bar{u}_{i,m})}{g(y + \bar{u}_{j,1}) \ldots g(y + \bar{u}_{j,m})}.
\end{align*} \]

Taking logarithms on both sides, we get

\[ \frac{V_1}{x} + \frac{V_2}{x^2} + \ldots = \frac{W_1}{y} + \frac{W_2}{y^2} + \ldots \]

for certain numbers \( V, W \), satisfying \( \max(|V|, |W|) \leq c \) for \( c \geq 1 \). In
Values of a polynomial at arithmetic progressions

73

We have
\[
W_e = \left( -1 \right)^{e-1} \sum_{h=1}^{m} \sum_{q=1}^{\mu} \left\{ (\bar{u}_{i,h} - \beta_q)^e - (\bar{u}_{j,h} - \beta_q)^e \right\}.
\]

Now, we shall derive that
(13) \[ V_1 = \ldots = V_{l-1} = 0, \quad W_1 = \ldots = W_{m-1} = 0. \]

We prove (13) by contradiction like we proved (9). Suppose \( I \) and \( J \) are integers with \( 1 \leq I < l, 1 \leq J < m \) such that \( V_1 = \ldots = V_{I-1} = 0, V_I \neq 0, W_1, \ldots, W_{J-1} = 0, W_J \neq 0 \). Then
\[
\frac{V_I}{x_I} + \ldots = \frac{W_J}{y_J} + \ldots,
\]
which implies that \( mI = lJ \). Since \( \gcd(l, m) = 1 \), this implies \( l \) divides \( I \) and \( m \) divides \( J \), whence (13) follows.

Now, by induction on \( e \), it follows from (13) that
\[
W'_e = \left( -1 \right)^{e-1} \sum_{h=1}^{m} \left( (\bar{u}_{i,h})^e - (\bar{u}_{j,h})^e \right)
\]
satisfies \( W'_1 = \ldots = W'_{m-1} = 0 \). This implies that
\[
\log \prod_{h=1}^{m} \left( \frac{1 + \bar{u}_{i,h}}{y} \right) = \frac{W'_m}{y^m} + \ldots
\]
Thus
\[
\prod_{h=1}^{m} \left( y + \bar{u}_{i,h} \right) = \prod_{h=1}^{m} \left( y + \bar{u}_{j,h} \right) + W'_m + O(1/y).
\]

By taking \( y \) sufficiently large and writing \( E_{i,j} \) for \( W'_m \), we get the polynomial relation
(14) \[ \prod_{h=1}^{m} \left( Y + \bar{u}_{i,h} \right) = \prod_{h=1}^{m} \left( Y + \bar{u}_{j,h} \right) + E_{i,j} \quad \text{for } 1 \leq i, j \leq k, i \neq j \]
for some number \( E_{i,j} \). We observe that \( E_{i,j} \neq 0 \) for \( 1 \leq i, j \leq k \) and \( i \neq j \).

We put
\[
g_2(Y) = \prod_{h=1}^{m} \left( Y + \bar{u}_{1,h} \right).
\]

By (14), we have
(15) \[ g_2(Y) = \prod_{h=1}^{m} \left( Y + \bar{u}_{j,h} \right) + E_j \quad \text{for } 2 \leq j \leq k \text{ with } E_j = E_{1,j}. \]

We observe from (15) and (14) that \( E_j \) for \( 2 \leq j \leq k \) are pairwise distinct non-zero numbers. Further, we see from (15) that every number \( 0 =: E_1 \),
$E_2, \ldots, E_k$ is assumed by the polynomial $g_2$ at $m$ distinct integers from $\{-Jd_2 \mid 0 \leq J \leq mk - 1\}$. Now, we may follow an argument of the proof of Theorem 2 of [3] to conclude that

$$\max(|x|, |y|) \leq c_7 \quad \text{unless } m = 2.$$  

This argument depends on Rolle’s theorem. Here we give a proof of the preceding assertion without using Rolle’s theorem.

As already observed, the elements of the sets $\overline{U}_i = \{\overline{u}_{i,1}, \ldots, \overline{u}_{i,m}\}$ for $1 \leq i \leq k$ are distinct and $\overline{U}_i \cap \overline{U}_j = \emptyset$ for $i \neq j$, $1 \leq i, j \leq k$. Then

$$\sum_{i=1}^{k} \sum_{h=1}^{m} \overline{u}_{i,h} = \sum_{j=0}^{mk-1} Jd_2 = mk(mk-1)d_2/2.$$  

Further, by equating the coefficients of $Y^{m-1}$ on both sides of (14), we obtain

$$\sum_{h=1}^{m} \overline{u}_{i,h} = \sum_{h=1}^{m} \overline{u}_{j,h} \quad \text{for } 1 \leq i, j \leq k.$$  

Consequently, we have

$$\sum_{h=1}^{m} \overline{u}_{i,h} = \sum_{h=1}^{m} \overline{u}_{j,h} \quad \text{for } 1 \leq i \leq k.$$  

We assume without loss of generality that

$$\overline{u}_{i,1} < \overline{u}_{i,2} < \ldots < \overline{u}_{i,m} \quad \text{for } 1 \leq i \leq k$$  

and

$$0 = \overline{u}_{1,1} < \overline{u}_{2,1} < \ldots < \overline{u}_{k,1}.$$  

We show by induction on $i$ that

$$\overline{u}_{i,1} = (i-1)d_2 \quad \text{for } 1 \leq i \leq k.$$  

We observe that (20) with $i = 1$ is true by (19). We assume that (20) is valid for $1 \leq i \leq i_0$ with $i_0 \leq k - 1$. If $i_0d_2 \in \overline{U}_{i_1}$ with $1 \leq i_1 \leq i_0$, we consider (14) with $i = i_1$, $j = i_0 + 1$ and we put $Y = -(i_1 - 1)d_2$, $-i_0d_2$ to get a contradiction. Then (20) with $i = i_0 + 1$ follows from (18) and (19).

Next, we show by induction on $h$ that

$$\overline{u}_{k,h} = (k + h - 2)d_2 \quad \text{for } 1 \leq h \leq m.$$  

If $h = 1$, we observe that (21) is (20) with $i = k$. We suppose that $\overline{u}_{k,h} = (k + h - 2)d_2$ for $1 \leq h \leq h_0$ with $h_0 \leq m - 1$. If $(k + h_0 - 1)d_2 \in \overline{U}_{i_2}$ with $1 \leq i_2 \leq k - 1$, we consider (14) with $i = i_2$, $j = k$ and we put $Y = -(i_2 - 1)d_2$, $-(k + h_0 - 1)d_2$ to find that

$$(k - i_2)(k - i_2 + 1) \ldots (k - i_2 + h_0 - 1)(\overline{u}_{k,h_0 + 1} - (i_2 - 1)d_2) \ldots (\overline{u}_{k,m} - (i_2 - 1)d_2)$$
= (-1)^k h_0(h_0 - 1) \ldots 1(\pi_{k,h_0+1} - (k + h_0 - 1)d_2) \ldots
\ldots (\pi_{k,m} - (k + h_0 - 1)d_2).

This is not possible since \((k - i_2) \ldots (k - i_2 + h_0 - 1) \geq h_0!\) and (18). Hence (21) with \(h = h_0 + 1\) follows. This completes the proof of (21). Then

\[
\sum_{h=1}^{m} \pi_{k,h} = \left( mk + \frac{1}{2} m(m - 3) \right) d_2,
\]

which, together with (17), implies that \(k = 1\) whenever \(m \geq 3\). This completes the proof of (16) without using Rolle’s theorem.

Next we turn to the case \(m = 2\). Then \(l = 1\). Let \(1 \leq i < j \leq k\). It follows from (13) that the corresponding \(W_1\) satisfies \(W_1 = 0\). Extending the argument used for proving (13) we see that \(V_1 = W_2\). By definition \(V_1 = \mu(\tilde{t}_{i,1} - \tilde{t}_{j,1})\). Further, by \(W_1 = 0\), we have \(E_{i,j} = W_2' = W_2\). Consequently, \(E_{i,j} = \mu(\tilde{t}_{i,1} - \tilde{t}_{j,1})\). Hence and from (14), (20) and (17) we derive

\[
(22) \quad (Y + (i - 1)d_2)(Y + (2k - i)d_2)
= (Y + (j - 1)d_2)(Y + (2k - j)d_2) + \mu(\tilde{t}_{i,1} - \tilde{t}_{j,1}).
\]

Since \(z(2k - 1 - z)\) is an increasing function for \(0 \leq z \leq k - 1\), it follows that \(\tilde{t}_{i,1} < \tilde{t}_{j,1}\) for \(i < j\). Thus

\[
(23) \quad \tilde{t}_{i,1} = (i - 1)d_1 \quad \text{for} \quad 1 \leq i \leq k.
\]

Suppose first \(k \geq 3\). From (23) and (22) with \(i = 1, j = 2\) we obtain

\[
(2k - 2)d_2^2 = \mu d_1.
\]

Similarly, with \(i = 1, j = 3\), we get

\[
2(2k - 3)d_2^2 = 2\mu d_1.
\]

Hence \(2k - 2 = 2k - 3\), which is impossible.

It remains to consider \(m = k = 2\). Then, from (23) and (22) with \(i = 1, j = 2\), we have

\[
(24) \quad 2d_2^2 = \mu d_1.
\]

Note that (17)–(20) imply that \(\pi_{1,1} = 0, \pi_{2,1} = d_2, \pi_{1,2} = 3d_2, \pi_{2,2} = 2d_2\). Hence, by (12) and (23),

\[
(25) \quad g(x) = g(y)g(y + 3d_2), \quad g(x + d_1) = g(y + d_2)g(y + 2d_2).
\]

Write \(g(X) = X^\mu + aX^{\mu - 1} + bX^{\mu - 2} + O(X^{\mu - 3})\). Then the first equation of (25) implies \(x = y^2 + O(y)\) in obvious notation. By computing the higher order terms we obtain

\[
g(x + d_1) - g(x) = \mu d_1 x^{\mu - 1} + O(x^{\mu - 2})
\]

and

\[
g(y + d_2)g(y + 2d_2) - g(y)g(y + 3d_2) = \left( 2\mu^2 - 4\left( \frac{\mu}{2} \right)^2 \right) d_2^2 y^{2\mu - 2} + O(y^{2\mu - 3}).
\]
Hence, on using (25) and substituting \( x = y^2 + O(y) \),
\[
d_1 = 2d_2^2 + O(1/y).
\]
Together with (24) this implies \( \mu = 1 \). Thus \( g(X) = X + a \) with \( a \in \mathbb{Q} \).
By (25) we find that \( a \in \mathbb{Z} \) and (5) follows. This completes the proof of Theorem (b).

References