

N. SARADHA

On blocks of arithmetic progressions with equal products

Journal de Théorie des Nombres de Bordeaux, tome 9, n° 1 (1997),
p. 183-199

http://www.numdam.org/item?id=JTNB_1997__9_1_183_0

© Université Bordeaux 1, 1997, tous droits réservés.

L'accès aux archives de la revue « Journal de Théorie des Nombres de Bordeaux » (<http://jtnb.cedram.org/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

On blocks of arithmetic progressions with equal products

par N. SARADHA

RÉSUMÉ. Soit $f(X) \in \mathbb{Q}[X]$ un polynôme qui est une puissance d'un polynôme $g(X) \in \mathbb{Q}[X]$ de degré $\mu \geq 2$ et dont les racines réelles sont simples. Etant donnés les entiers positifs d_1, d_2, ℓ, m satisfaisant $\ell < m$, $\text{pgcd}(\ell, m) = 1$ et $\mu \leq m + 1$ si $m > 2$, nous démontrons que l'équation

$$f(x)f(x+d_1)\cdots f(x+(\ell k-1)d_1) = f(y)f(y+d_2)\cdots f(y+(mk-1)d_2)$$

avec $f(x+jd_1) \neq 0$ pour $0 \leq j < \ell k$ ne possède qu'un nombre fini de solutions en les entiers x, y et $k \geq 1$, excepté dans le cas

$$m = \mu = 2, \ell = k = d_2 = 1, f(X) = g(X), x = f(y) + y.$$

ABSTRACT Let $f(X) \in \mathbb{Q}[X]$ be a monic polynomial which is a power of a polynomial $g(X) \in \mathbb{Q}[X]$ of degree $\mu \geq 2$ and having simple real roots. For given positive integers d_1, d_2, ℓ, m with $\ell < m$ and $\text{gcd}(\ell, m) = 1$ with $\mu \leq m + 1$ whenever $m > 2$, we show that the equation

$$f(x)f(x+d_1)\cdots f(x+(\ell k-1)d_1) = f(y)f(y+d_2)\cdots f(y+(mk-1)d_2)$$

with $f(x+jd_1) \neq 0$ for $0 \leq j < \ell k$ has only finitely many solutions in integers x, y and $k \geq 1$ except in the case

$$m = \mu = 2, \ell = k = d_2 = 1, f(X) = g(X), x = f(y) + y.$$

1. Introduction.

The letters d_1, d_2, μ, ℓ, m denote positive integers satisfying $\ell < m$ and $\text{gcd}(\ell, m) = 1$ throughout this paper. Let s_1, \dots, s_μ be rational integers with $s_1 < s_2 < \dots < s_\mu$. For $1 \leq i \leq \mu$, we put

$$P_i(X) = (X - s_i)(X - s_i + d_1)\cdots(X - s_i + (\ell k - 1)d_1)$$

and

$$Q_i(Y) = (Y - s_i)(Y - s_i + d_2)\cdots(Y - s_i + (mk - 1)d_2).$$

In this paper we consider the equation

$$(1) \quad P_1(x) \cdots P_\mu(x) = \pm Q_1(y) \cdots Q_\mu(y)$$

in integers x, y and $k \geq 1$ with

$$(2) \quad P_i(x) \neq 0 \quad \text{for } 1 \leq i \leq \mu.$$

By taking $f(X) = (X - s_1) \cdots (X - s_\mu)$ if equation (1) holds with $+$ sign and $f(X) = ((X - s_1) \cdots (X - s_\mu))^2$ if equation (1) holds with $-$ sign in Theorem (a) of [5], we derive that equation (1) with $k \geq 2$ and (2) implies that k is bounded by an effectively computable number depending only on $d_1, d_2, m, \mu, s_1, \dots, s_\mu$. Therefore, we restrict to consider equation (1) with fixed k . It was shown in [5] that if x, y and $k \geq 2$ are integers satisfying $x + jd_1 \neq 0$ for $0 \leq j < \ell k$, then equation (1) with $\mu = 1$ and $s_1 = 0$, that is, the equation

$$x(x + d_1) \cdots (x + (\ell k - 1)d_1) = \pm y(y + d_2) \cdots (y + (mk - 1)d_2)$$

implies that $\max(|x|, |y|, k)$ is bounded by an effectively computable number depending only on d_1, d_2 and m unless

$$\ell = 1, m = k = 2, d_1 = 2d_2^2, x = y(y + 3d_2).$$

We extend this result as follows.

THEOREM 1. *Let $x, y, k \geq 1$ and $\mu \geq 2$ be integers satisfying equation (1) with (2). Assume that the polynomials $P_1(X) \cdots P_\mu(X)$, $Q_1(Y) \cdots Q_\mu(Y)$ have simple roots. Suppose that one of the following conditions holds:*

$$(3) \quad \begin{cases} (i) \ m = 2 & (ii) \ \mu \in \{2, 3, 4\} & (iii) \ d_2 = 1 \\ (iv) \ d_1 = 1, \ell k \neq 1 \text{ and } \mu \not\equiv 0 \pmod{2} & \text{if } \ell = 2 \end{cases}$$

Then

$$(4) \quad \max(|x|, |y|) \leq C$$

unless

$$(5) \quad m = \mu = 2, \ell = k = d_2 = 1, x = y^2 + y(1 - s_1 - s_2) + s_1 s_2$$

where C is an effectively computable number depending only on $d_1, d_2, m, \mu, s_1, \dots, s_\mu$.

It is clear that condition (2) is necessary and equation (1) is satisfied for the possibilities given by (5). The assumption that polynomials $P_1(X) \cdots P_\mu(X)$ and $Q_1(Y) \cdots Q_\mu(Y)$ have simple roots is equivalent to saying that the linear factors on the left hand side as well as the right hand side of equation (1) are distinct. We derive Theorem 1 from a more general result. For this, we introduce the following notation and assumptions. Let $f(X)$ be a monic polynomial with rational coefficients of positive degree. We consider the equation

$$(6) \quad f(x)f(x+d_1) \cdots f(x+(\ell k-1)d_1) = f(y)f(y+d_2) \cdots f(y+(mk-1)d_2)$$

in integers x, y and $k \geq 1$ with

$$(7) \quad f(x+jd_1) \neq 0 \quad \text{for } 0 \leq j < \ell k.$$

It has been shown in Theorem (a) of [5] that equation (6) with $k \geq 2$ and (7) implies that k is bounded by an effectively computable number depending only on d_1, d_2, m and f . Further, when f is a power of an irreducible polynomial, it was shown in Theorem (b) of [5] that equation (6) with (7) and $k \geq 2$ implies that $\max(|x|, |y|)$ is bounded by an effectively computable number depending only on d_1, d_2, m, k and f unless

$$\ell = 1, m = k = 2, d_1 = 2d_2^2,$$

$$f(X) = (X+r)^\nu \quad \text{with } r \in \mathbb{Z}, (x+r) = (y+r)(y+r+3d_2).$$

We do not have the analogous result when f is not a power of an irreducible polynomial. In this paper, we take $f(X) = g^b(X)$ where $g(X)$ has real roots $\beta_1, \dots, \beta_\mu$ such that $\beta_1 < \beta_2 < \dots < \beta_\mu$, the leading coefficient of $g(X)$ is ± 1 and b is a positive integer. We put

$$T = \{\beta_i - Jd_1 \mid 1 \leq i \leq \mu, 0 \leq J < \ell k\}$$

and

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

We assume that $|T| = \ell k \mu$ and $|U| = mk \mu$ so that the elements of T as well as the elements of U are pairwise distinct. This assumption is satisfied whenever g is irreducible. We do not intend to consider the case $\mu = k = 1$. Therefore, in view of the preceding result on equation (6), we may assume henceforth that $\mu \geq 2$. Further, by the same result, we may take k fixed. We follow the above notation and assumptions without any further reference. We refer to [4] and [6] for a survey of earlier results on equation (6) with $f(X) = X$. Here we prove

THEOREM 2.

(a) Let $k \geq 1, m = 2$ and $\mu \geq 2$. Then $l = 1$ and equation (6) with (7) implies that $\max(|x|, |y|)$ is bounded by an effectively computable number depending only on d_1, d_2, k and f unless

$$(8) \quad \mu = 2, \ell = k = d_2 = 1, x = y^2 + y(1 - \beta_1 - \beta_2) + \beta_1\beta_2.$$

(b) Let $k \geq 1, m > 2$ and $2 \leq \mu \leq m + 1$. Equation (6) with (7) implies that $\max(|x|, |y|)$ is bounded by an effectively computable number depending only on d_1, d_2, m, k and f .

The proof of Theorem 2 is elementary except for the case $k = 1, \mu = 2, m = 3$ and $\beta_2 - \beta_1 > d_2$, where we apply a theorem of Baker [1] on finiteness of integral solutions of hyper elliptic equations. This theorem has also been utilised in the proof of Theorem 1 when $d_1 = 1, l = 2, \mu \equiv 1 \pmod{2}$ and $d_1 = 1, l = 1, k \geq 2$.

If $m > 2$ and $\beta_i \geq 0$ for $1 \leq i \leq \mu$, we shall derive the assertion of Theorem 2 whenever β_μ is large as compared with $\beta_1, \dots, \beta_{\mu-1}, m, k, d_1$ and d_2 . We have

COROLLARY. Let $k \geq 1, \mu \geq 2$ and $0 \leq \beta_1 < \dots < \beta_\mu$. Equation (6) with (7) and

$$\beta_\mu > \begin{cases} \frac{\ell}{m-\ell+2} (\beta_1 + \dots + \beta_{\mu-1}) + \frac{(m+2)(\ell-2)(\ell k-1)d_1}{2(m-\ell+2)} & \text{if } \ell \geq 2 \\ \frac{m}{2} (\beta_1 + \dots + \beta_{\mu-1}) + \frac{(m^2-4)(mk-1)d_2}{4} & \text{if } \ell = 1. \end{cases}$$

imply that $\max(|x|, |y|)$ is bounded by an effectively computable number depending only on d_1, d_2, m, k and f unless (8) holds.

Acknowledgement. I thank Professor T.N. Shorey for many useful discussions.

2. Proof of Theorem 2

Let all the assumptions of Theorem 2 stated in section 1 be satisfied. Let c_1, c_2 and c_3 denote effectively computable numbers depending only on d_1, d_2, m, k and f . By equation (6) we may assume that $|y| > c_1$ where c_1 is sufficiently large. Now, we follow the proof of section 4 of [5] to conclude (10) and (11) of [5] which implies the following: There exist $T_i = \{t_{i,h} \mid 1 \leq h \leq \ell\} \subset T$ for $1 \leq i \leq \mu k$ satisfying $T_i \cap T_j = \emptyset$ for $i \neq j$ and

$U_i = \{u_{i,h} \mid 1 \leq h \leq m\} \subset U$ for $1 \leq i \leq \mu k$ satisfying $U_i \cap U_j = \emptyset$ for $i \neq j$ such that

$$(9) \quad (x - t_{i,1}) \cdots (x - t_{i,\ell}) = (y - u_{i,1}) \cdots (y - u_{i,m}) \quad \text{for } 1 \leq i \leq \mu k.$$

There is no loss of generality in assuming that $t_{i,1} < \cdots < t_{i,\ell}$ and $u_{i,1} < \cdots < u_{i,m}$ for $1 \leq i \leq \mu k$. Let $1 \leq i, j \leq \mu k, i \neq j$. Then we have

$$\frac{(x - t_{i,1}) \cdots (x - t_{i,\ell})}{(x - t_{j,1}) \cdots (x - t_{j,\ell})} = \frac{(y - u_{i,1}) \cdots (y - u_{i,m})}{(y - u_{j,1}) \cdots (y - u_{j,m})}.$$

Taking logarithms and expanding we get

$$\frac{V_1}{x} + \frac{V_2}{x^2} + \cdots = \frac{W_1}{y} + \frac{W_2}{y^2} + \cdots$$

We derive as in the proof of (13) of [5] that

$$V_1 = \cdots = V_{\ell-1} = 0, \quad W_1 = \cdots = W_{m-1} = 0$$

which implies that $V_\ell = W_m$. Put

$$(10) \quad V_\ell = W_m = E_{i,j}.$$

Then, by using (10), we derive as in the proof of (14) of [5] the polynomial relations

$$(11) \quad \begin{cases} (X - t_{i,1}) \cdots (X - t_{i,\ell}) = (X - t_{j,1}) \cdots (X - t_{j,\ell}) + E_{i,j} \\ (Y - u_{i,1}) \cdots (Y - u_{i,m}) = (Y - u_{j,1}) \cdots (Y - u_{j,m}) + E_{i,j} \end{cases}$$

for $1 \leq i, j \leq \mu k$. We observe that $E_{i,j} \neq 0$ for $i \neq j$. Further, from (11) and $m \geq 2$, we get

$$(12) \quad \sum_{h=1}^m u_{i,h} = \sum_{h=1}^m u_{j,h} \quad \text{for } 1 \leq i, j \leq \mu k$$

and since

$$\sum_{i=1}^{\mu k} \sum_{h=1}^m u_{i,h} = \sum_{i=1}^{\mu} \sum_{J=0}^{mk-1} (\beta_i - Jd_2),$$

we have

$$(13) \quad \sum_{h=1}^m u_{i,h} = \frac{m}{\mu}(\beta_1 + \cdots + \beta_\mu) - \frac{m}{2}(mk-1)d_2 \quad \text{for } 1 \leq i \leq \mu k.$$

We set

$$f_0(X) = \prod_{h=1}^{\ell} (X - t_{1,h})$$

and

$$g_0(Y) = \prod_{h=1}^m (Y - u_{1,h}).$$

We observe from (11) that

$$f_0(X) = \prod_{h=1}^{\ell} (X - t_{j,h}) + E_j \quad \text{and} \quad g_0(Y) = \prod_{h=1}^m (Y - u_{j,h}) + E_j$$

where $E_j = E_{1,j}$ for $2 \leq j \leq \mu k$. Further, we put $E_1 = 0$. We re-arrange E_j 's, if necessary, so that $E_1 < E_2 < \cdots < E_{\mu k}$. Now, we follow an argument depending on Rolle's Theorem of the proof of Theorem 2 of [4] to obtain the distribution of t 's and u 's as in Figure (1) and Figure (2) respectively.

↓ indicates t (or u) is increasing. ↑ indicates t (or u) is decreasing.

ℓ odd				
$t_{1,1}$	$t_{1,2}$	$< \cdots$	$t_{1,\ell-1}$	$< t_{1,\ell}$
↑	↓		↓	↑
$t_{2,1}$	$t_{2,2}$	\cdots	$t_{2,\ell-1}$	$t_{2,\ell}$
↑	↓		↓	↑
\vdots	\vdots		\vdots	\vdots
↑	↓		↓	↑
$t_{\mu k-1,1}$	$t_{\mu k-1,2}$	\cdots	$t_{\mu k-1,\ell-1}$	$t_{\mu k-1,\ell}$
↑	↓		↓	↑
$t_{\mu k,1}$	$< t_{\mu k,2}$	$\cdots <$	$t_{\mu k,\ell-1}$	$t_{\mu k,\ell}$

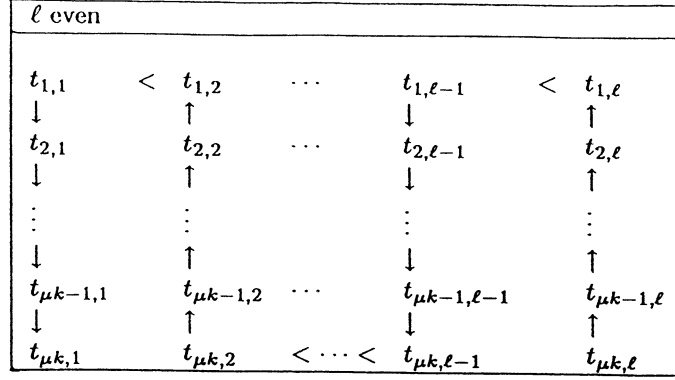


Figure (1)

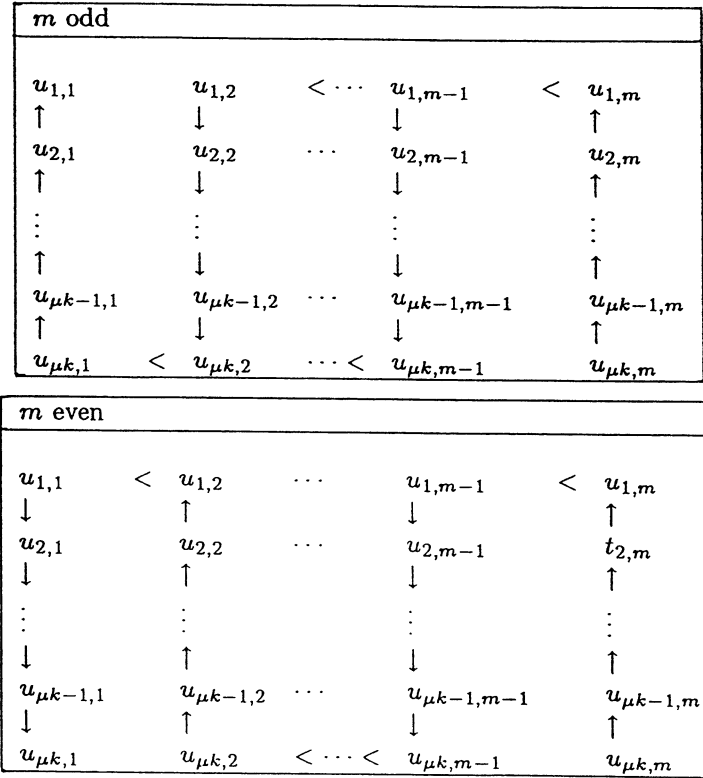


Figure (2)

We shall use Figure (1) and Figure (2) without reference at many places in

Proof of Theorem 2 (a). Let $m = 2$. Then $\ell = 1$. For any i, j with $1 \leq i, j \leq \mu k$ we compute $V_1 = t_{j,1} - t_{i,1}$. Then we obtain from (11) and (10) that

$$(14) \quad u_{i,1} u_{i,2} = u_{j,1} u_{j,2} + t_{j,1} - t_{i,1} \quad \text{for } 1 \leq i, j \leq \mu k.$$

Further, we have $u_{\mu k,1} = \beta_1 - (2k - 1)d_2$, $u_{\mu k,2} = \beta_\mu$. Hence by (12), $(u_{\mu k-1,2}, u_{\mu k-1,1}) = (\beta_{\mu-1}, \beta_1 + \beta_\mu - \beta_{\mu-1} - (2k - 1)d_2)$ or $(\beta_\mu - d_2, \beta_1 - (2k - 2)d_2)$. Also, we have $t_{\mu k,1} = \beta_\mu$, $t_{\mu k-1,1} = \beta_{\mu-1}$ or $\beta_\mu - d_1$. Now, we use (14) with $i = \mu k - 1, j = \mu k$ to obtain the following four possibilities:

$$(i) \quad \beta_{\mu-1} - \beta_1 + (2k - 1)d_2 = 1$$

$$(ii) \quad (\beta_\mu - \beta_1)d_2 + (2k - 2)d_2^2 = \beta_\mu - \beta_{\mu-1}$$

if $t_{\mu k-1,1} = \beta_{\mu-1}$ and

$$(iii) \quad (\beta_\mu - \beta_{\mu-1})(\beta_{\mu-1} - \beta_1 + (2k - 1)d_2) = d_1$$

$$(iv) \quad (\beta_\mu - \beta_1)d_2 + (2k - 2)d_2^2 = d_1$$

if $t_{\mu k-1,1} = \beta_\mu - d_1$. When $t_{\mu k-1,1} = \beta_\mu - d_1$, we have $\beta_{\mu-1} < \beta_\mu - d_1$ i.e. $\beta_\mu - \beta_{\mu-1} > d_1$. Thus the possibilities (iii) and (iv) do not hold. If either (i) or (ii) holds, we see that $\mu = 2, k = d_2 = 1$. This yields by (9) with $i = 2, u_{2,1} = \beta_1 - 1, u_{2,2} = \beta_2, t_{2,1} = \beta_2$, the possibilities (8).

Now, we turn to the proof of Theorem 2(b). Therefore, we suppose that $m \geq 3$ from now onward in this section. The proof of Theorem 2(b) depends on the following lemmas.

LEMMA 1. *Let $1 \leq i < j \leq \mu k$. Then*

$$u_{i,m-1} - u_{j,m-1} > u_{j,m} - u_{i,m}.$$

Proof. It is clear that $u_{j,m} > u_{i,m} > u_{i,m-1} > u_{j,m-1} > u_{i,m-2} > u_{i,m-3} > \dots > u_{i,1}$. In (11), we put $Y = u_{j,m}$ and $u_{j,m-1}$ to get

$$\begin{aligned} & (u_{j,m} - u_{i,m})(u_{j,m} - u_{i,m-1})(u_{j,m} - u_{i,m-2}) \cdots (u_{j,m} - u_{i,1}) = \\ & (u_{j,m-1} - u_{i,m})(u_{j,m-1} - u_{i,m-1})(u_{j,m-1} - u_{i,m-2}) \cdots (u_{j,m-1} - u_{i,1}). \end{aligned}$$

The product of the last $(m-2)$ terms on the left hand side is greater than the product of the last $(m-2)$ terms on the right hand side in the above equality. Thus we derive that

$$(u_{j,m} - u_{i,m})(u_{j,m} - u_{i,m-1}) < (u_{i,m} - u_{j,m-1})(u_{i,m-1} - u_{j,m-1}).$$

Therefore,

$$u_{j,m}^2 - u_{j,m-1}^2 + (u_{i,m} + u_{i,m-1})(u_{j,m-1} - u_{j,m}) < 0$$

which, since $u_{j,m} > u_{j,m-1}$, implies the lemma. \square

The next lemma is more general than necessary. This generalisation may be useful for polynomials whose roots are not far apart.

LEMMA 2. *Let $K_0 = 0$ and K_1 be the number of roots of $g(X)$ in $(\beta_\mu - d_2, \beta_\mu]$. For an integer h with $2 \leq h \leq k$, let K_h denote the number of roots of $g(X)$ in $(\beta_\mu - hd_2, \beta_\mu - (h-1)d_2)$. We assume that*

$$(15) \quad \mu < \frac{m}{2}(K_1 + \cdots + K_k) - \frac{K_2 + 2K_3 + \cdots + (k-1)K_k - \frac{1}{2}}{k}.$$

Then equation (6) with (7) and (15) imply that $\max(|x|, |y|, k)$ is bounded by an effectively computable number depending only on d_1, d_2, m and f .

Proof. We may assume that $|y| > c_1$ so that Figure (2) is valid and we shall arrive at a contradiction implying the assertion of the lemma. We observe that $K_1 \geq 1$ and

$$(16) \quad \begin{cases} \beta_\mu - d_2 < \beta_i \leq \beta_\mu & \text{if and only if } \mu - K_1 + 1 \leq i \leq \mu. \\ \text{For } h \geq 2, \beta_\mu - hd_2 < \beta_i < \beta_\mu - (h-1)d_2 & \text{if and only if} \\ \mu - K_1 - \cdots - K_h + 1 \leq i \leq \mu - K_1 - \cdots - K_{h-1}. \end{cases}$$

We now show that

$$(17) \quad u_{\mu k - K, m} = \beta_\mu - kd_2 \quad \text{where } K = kK_1 + (k-1)K_2 + \cdots + K_k.$$

Suppose $K_1 = \mu$. Then we have $u_{\mu k, m} = \beta_\mu, \dots, u_{\mu k - \mu + 1, m} = \beta_1, u_{\mu k - \mu, m} = \beta_\mu - d_2, \dots, u_{\mu k - 2\mu + 1, m} = \beta_1 - d_2, \dots, u_{\mu, m} = \beta_\mu - (k-1)d_2, \dots, u_{1, m} = \beta_1 - (k-1)d_2; u_{1, m-1} = \beta_\mu - kd_2, \dots, u_{\mu, m-1} = \beta_1 - kd_2$. Then we apply Lemma 1 with $i = 1, j = \mu$ to get a contradiction. Thus $K_1 \leq \mu - 1$. It is clear that the number of elements of U in $[\beta_\mu - kd_2, \beta_\mu]$ is

equal to $K + 1 = kK_1 + \cdots + K_k + 1 \leq K_1 + (k - 1)(K_1 + \cdots + K_k) + 1 \leq K_1 + (k - 1)\mu + 1 \leq \mu k$. Thus $\beta_\mu - kd_2$ lies in the m -th column of Figure (2). This proves (17).

Let

$$u_{\mu k - K, m-1} = \beta_r - Jd_2 \quad \text{with } 1 \leq r \leq \mu, 0 \leq J < mk.$$

We claim that there exist i, J_1 and h such that

$$(18) \quad \beta_r - Jd_2 \geq \beta_i - J_1d_2$$

with

$$(19) \quad \begin{cases} \mu - K_1 - \cdots - K_h + 1 \leq i \leq \mu - K_1 - \cdots - K_{h-1}, \\ 0 \leq J_1 \leq mk - k - h, \quad 1 \leq h \leq k. \end{cases}$$

Suppose (18) does not hold. Then $\beta_r - Jd_2 < \beta_i - J_1d_2$ for all i, J_1 and h satisfying (19). The number of such $\beta_i - J_1d_2$ is $\sum_{h=1}^k (mk - k - h + 1)K_h$. The total number of u 's exceeding $\beta_r - Jd_2$ is $2\mu k - K - 1$. Thus

$$\sum_{h=1}^k (mk - k - h + 1)K_h \leq 2\mu k - kK_1 - \cdots - K_k - 1.$$

Therefore

$$mk(K_1 + \cdots + K_k) \leq 2\mu k + 2K_2 + \cdots + (2k - 2)K_k - 1$$

which contradicts (15). This proves (18). We now show that

$$(20) \quad J \leq mk - k - 1.$$

For, if $J \geq mk - k$, (18) and (19) imply that $\beta_r - \beta_i \geq (J - J_1)d_2 \geq hd_2$. On the other hand, we observe from (19) and (16) that $\beta_r - \beta_i \leq \beta_\mu - \beta_i < hd_2$. This contradiction proves (20).

Now, we choose i_0, J_0, h_0 such that $\beta_{i_0} - J_0d_2$ is the largest among $\beta_i - J_1d_2$ satisfying (18) with (19). Thus we derive from (19), (16) and (17) that there exists n_0 satisfying

$$\beta_{i_0} = u_{n_0, m}, \quad \mu k - K + 1 \leq n_0 \leq \mu k.$$

Consider $u_{n_0+1,m}$ when $n_0 < \mu k$. From (16) it is clear that $\beta_\mu - h_0 d_2 < u_{n_0+1,m} \leq \beta_\mu - (h_0 - 1)d_2$. Let $u_{n_0+1,m} = \beta_{i_1} - J_2 d_2$. Then $\beta_\mu - h_1 d_2 < \beta_{i_1} \leq \beta_\mu - (h_1 - 1)d_2$ with $h_1 = h_0 - J_2$. Hence $u_{n_0+1,m} - J_0 d_2 = \beta_{i_1} - (h_0 - h_1 + J_0)d_2$. By (16) and (19), we have

$$\mu - K_1 - \cdots - K_{h_1} + 1 \leq i_1 \leq \mu - K_1 - \cdots - K_{h_1-1},$$

$$0 \leq h_0 - h_1 + J_0 \leq mk - k - h_1, \quad 1 \leq h_1 \leq k.$$

Therefore

$$\beta_{i_1} - (h_0 - h_1 + J_0)d_2 > u_{n_0,m} - J_0 d_2 = \beta_{i_0} - J_0 d_2.$$

Hence by the maximality of $\beta_{i_0} - J_0 d_2$, we have

$$(21) \quad u_{n_0+1,m} - J_0 d_2 > \beta_r - J d_2 \geq u_{n_0,m} - J_0 d_2 \quad \text{if } n_0 < \mu k.$$

Let $n_0 = \mu k$. Then $i_0 = \mu, h_0 = 1$ and $J_0 \geq k + 1$. We apply the preceding argument to $u_{\mu k - K + 1, m} - (J_0 - k)d_2$. By (17), we observe that $\beta_\mu - k d_2 < u_{\mu k - K + 1, m} \leq \beta_\mu - (k - 1)d_2$. There exist i_2, J_3, h_2 such that $u_{\mu k - K + 1, m} = \beta_{i_2} - J_3 d_2$ with $\beta_\mu - h_2 d_2 < \beta_{i_2} \leq \beta_\mu - (h_2 - 1)d_2, h_2 = k - J_3$. Hence $u_{\mu k - K + 1, m} - (J_0 - k)d_2 = \beta_{i_2} - (J_0 - h_2)d_2$ with $\mu - K_1 - \cdots - K_{h_2} + 1 \leq i_2 \leq \mu - K_1 - \cdots - K_{h_2-1}, 0 \leq J_0 - h_2 \leq mk - k - h_2, 1 \leq h_2 \leq k$. Therefore, $\beta_{i_2} - (J_0 - h_2)d_2 > \beta_\mu - k d_2 - (J_0 - k)d_2 = \beta_\mu - J_0 d_2$. Hence by the maximality of $\beta_\mu - J_0 d_2$, we have

$$(22) \quad u_{\mu k - K + 1, m} - (J_0 - k)d_2 > \beta_r - J d_2 \geq \beta_\mu - J_0 d_2 \quad \text{if } n_0 = \mu k.$$

We derive from (21) and (17) that

$$\begin{aligned} \beta_r - J d_2 &\geq u_{n_0,m} - J_0 d_2 > \cdots > u_{\mu k - K, m} - J_0 d_2 = \beta_\mu - (J_0 + k)d_2 = \\ u_{\mu k, m} - (J_0 + k)d_2 &> \cdots > u_{n_0+1, m} - (J_0 + k)d_2 > \beta_r - (J + k)d_2, \end{aligned}$$

if $n_0 < \mu k$. Similarly, we obtain from (22) that

$$\beta_r - J d_2 \geq u_{\mu k, m} - J_0 d_2 > \cdots > u_{\mu k - K + 1, m} - J_0 d_2 > \beta_r - (J + k)d_2,$$

if $n_0 = \mu k$. Consequently by (19) and (20), there are at least K elements of U in $[\beta_r - (J + k)d_2, \beta_r - J d_2]$. Recalling that $u_{\mu k - K, m - 1} = \beta_r - J d_2$, we have $u_{\mu k, m - 1} \geq \beta_r - (J + k)d_2 = u_{\mu k - K, m - 1} - k d_2$

i.e.,

$$u_{\mu k - K, m - 1} - u_{\mu k, m - 1} \leq k d_2.$$

On the other hand, we apply Lemma 1 with $i = \mu k - K, j = \mu k$ and (17) for deriving that

$$u_{\mu k - K, m-1} - u_{\mu k, m-1} > u_{\mu k, m} - u_{\mu k - K, m} = kd_2.$$

This is a contradiction. □

Proof of Theorem 2 (b). By Lemma 2, we may assume that

$$\mu \geq \frac{m}{2}K_1 + \left(\frac{m}{2} - \frac{1}{k}\right)K_2 + \cdots + \left(\frac{m}{2} - \frac{k-1}{k}\right)K_k + \frac{1}{2k} > \frac{m}{2}K_1.$$

Therefore, since $\mu \leq m + 1$, we derive that either $K_1 = 1$ or $K_1 = 2, \mu = m + 1$.

First, we consider the case $K_1 = 1$. Thus $u_{\mu k, m} = \beta_\mu$ and $u_{\mu k-1, m} = \beta_\mu - d_2$. Suppose there exists β_r with $1 \leq r \leq \mu$ such that

$$(23) \quad \beta_r - (J_4 + 1)d_2 < u_{\mu k-1, m-1} \leq \beta_r - J_4 d_2$$

for some J_4 with $0 \leq J_4 \leq mk - 2$, then $u_{\mu k, m-1} \geq \beta_r - (J_4 + 1)d_2$ and hence $u_{\mu k-1, m-1} - u_{\mu k, m-1} \leq d_2$ which contradicts Lemma 1 with $i = \mu k - 1, j = \mu k$. Thus we may assume that (23) does not hold. Then it is easy to observe that for any r with $1 \leq r \leq \mu$, either $u_{\mu k-1, m-1} > \beta_r - Jd_2$ for all J with $0 \leq J < mk$ or $u_{\mu k-1, m-1} \leq \beta_r - (J + 1)d_2$ for all J with $0 \leq J \leq mk - 2$. Let ϵ_0 be the number of r 's for which the latter inequality holds. Then $mk\epsilon_0$ is the number of elements of U greater than or equal to $u_{\mu k-1, m-1}$. It is clear from Figure (2) that this number is also equal to $2\mu k - 1$. Thus $mk\epsilon_0 = 2\mu k - 1$ which, together with $\mu \leq m + 1$, implies that

$$k = 1, \quad \epsilon_0 = 1, \quad m = 2\mu - 1.$$

First, suppose $\mu \geq 3$. We see that

$$u_{\mu k-2, m} = \beta_\mu - 2d_2, u_{\mu k-2, m-1} = \beta_\mu - (m-2)d_2, u_{\mu k-1, m-1} = \beta_\mu - (m-1)d_2.$$

We use Lemma 1 with $i = \mu k - 2, j = \mu k - 1$ to get a contradiction. Thus we may assume that $\mu = 2$. Then $m = 3$ and we have

$$\begin{aligned} u_{1,1} &= \beta_1 - 2d_2, u_{1,2} = \beta_2 - 2d_2, u_{1,3} = \beta_2 - d_2 \\ u_{2,1} &= \beta_1 - d_2, u_{2,2} = \beta_1, u_{2,3} = \beta_2. \end{aligned}$$

We observe from Figure (1) that

$$t_{1,1} = \beta_1, t_{2,1} = \beta_2 \quad \text{if } \ell = 1$$

$(t_{1,1}, t_{1,2}) = (\beta_1, \beta_2 - d_1)$ or $(\beta_2 - d_1, \beta_1)$; $(t_{2,1}, t_{2,2}) = (\beta_1 - d_1, \beta_2)$ if $\ell = 2$.

We use (13) and (9) to get $\beta_2 = \beta_1 + 4d_2$ and if $\ell = 1$, we have

$$\begin{aligned} x - \beta_1 &= (y - \beta_1 + 2d_2)(y - \beta_2 + 2d_2)(y - \beta_2 + d_2) \\ x - \beta_2 &= (y - \beta_1 + d_2)(y - \beta_1)(y - \beta_2) \end{aligned}$$

and if $\ell = 2$, we have

$$\begin{aligned} (x - \beta_1)(x - \beta_2 + d_1) &= (y - \beta_1 + 2d_2)(y - \beta_2 + 2d_2)(y - \beta_2 + d_2) \\ (x - \beta_1 + d_1)(x - \beta_2) &= (y - \beta_1 + d_2)(y - \beta_1)(y - \beta_2) \end{aligned}$$

Thus, by subtracting second equation from the first in both the cases $\ell = 1, 2$ and using $\beta_2 = \beta_1 + 4d_2$, we derive that $3d_2^2 = 1$ if $\ell = 1$ and $3d_2^2 = d_1$ if $\ell = 2$. Thus we need to consider only $\ell = 2$. In this case using $\beta_2 = \beta_1 + 4d_2, \beta_1 + \beta_2 \in \mathbb{Q}$ and $d_1 = 3d_2^2$, we see that $\beta_1 \in \mathbb{Q}$ and $x_1^2 = y^3 - 3(\beta_1 + d_2)y^2 + (3\beta_1^2 + 6\beta_1d_2 - 4d_2^2)y - \beta_1^3 - 3\beta_1^2d_2 + 4\beta_1d_2^2 + \frac{9}{4}d_2^4 + 6d_2^3 + 4d_2^2$ where $x_1 = x + \frac{3d_2^2 - 4d_2 - 2\beta_1}{2}$. This is an elliptic equation. Suppose α is a double root of $h(Y)$ where $h(Y) = Y^3 - 3(\beta_1 + d_2)Y^2 + (3\beta_1^2 + 6\beta_1d_2 - 4d_2^2)Y - \beta_1^3 - 3\beta_1^2d_2 + 4\beta_1d_2^2 + \frac{9}{4}d_2^4 + 6d_2^3 + 4d_2^2$. Then $\alpha = \beta_1 + (1 \pm \sqrt{\frac{7}{3}})d_2$ and $0 = h(\alpha) = \frac{9}{4}d_2^4 \mp \frac{14}{3}\sqrt{\frac{7}{3}}d_2^3 + 4d_2^2$. This is impossible since $\sqrt{\frac{7}{3}}$ is irrational. Hence the roots of $h(Y)$ are simple. We now apply a theorem of Baker [1] to conclude that $\max(|x_1|, |y|) < c_2$ which implies that $\max(|x|, |y|) < c_3$.

Next, we consider the case $K_1 = 2$ and $\mu = m + 1$. Then $u_{\mu k, m} = \beta_\mu, u_{\mu k-1, m} = \beta_{\mu-1}, u_{\mu k-2, m} = \beta_\mu - d_2$. Suppose there exist β_s and β_r with $1 \leq s, r \leq \mu$ and $s \neq r$ such that

$$(24) \quad \beta_s - (J_5 + 1)d_2 < \beta_r - (J_6 + 1)d_2 < u_{\mu k-2, m-1} \leq \beta_s - J_5d_2 < \beta_r - J_6d_2$$

for some J_5, J_6 with $0 \leq J_5, J_6 \leq mk - 2$, then $u_{\mu k, m-1} \geq \beta_s - (J_5 + 1)d_2$ and hence $u_{\mu k-2, m-1} - u_{\mu k, m-1} \leq d_2$ which contradicts Lemma 1 with $i = \mu k - 2, j = \mu k$. Thus we may assume that (24) does not hold. This means there can be at most one $\beta_s, 1 \leq s \leq \mu$ satisfying

$$(25) \quad \beta_s - (J_5 + 1)d_2 < u_{\mu k-2, m-1} \leq \beta_s - J_5d_2$$

for some J_5 with $0 \leq J_5 \leq mk - 2$ and for any β_r with $1 \leq r \leq \mu$ and $r \neq s$

$$(26) \quad \text{either } u_{\mu k-2, m-1} \leq \beta_r - (mk - 1)d_2 \text{ or } u_{\mu k-2, m-1} > \beta_r.$$

The number of elements of U greater than or equal to $u_{\mu k-2, m-1}$ is $2\mu k-2$. Let ϵ_1 be the number of β_r 's with $u_{\mu k-2, m-1} \leq \beta_r - (mk-1)d_2$. Suppose there is no β_s satisfying (25). Then $2\mu k-2 = 2(m+1)k-2 = mk\epsilon_1$. This is possible only when $\epsilon_1 = 2, k = 1$. In this case, we have $u_{\mu k-3, m-1} = \beta_\mu - (m-1)d_2, u_{\mu k-3, m} = \beta_{\mu-1} - d_2, u_{\mu k-2, m-1} = \beta_{\mu-1} - (m-1)d_2$ and $u_{\mu k-2, m} = \beta_\mu - d_2$. We apply Lemma 1 with $i = \mu k-3, j = \mu k-2$ to get a contradiction. Thus we may assume that there exists a β_s satisfying (25). Then by counting again the elements of U greater than or equal to $u_{\mu k-2, m-1}$ in two ways as earlier we get $2\mu k-2 = 2(m+1)k-2 = mk\epsilon_1 + J_5 + 1$. This is possible only when $\epsilon_1 = 2, k \geq 2$ since $0 \leq J_5 \leq mk-2$. Thus for $\beta_r = \beta_\mu, \beta_{\mu-1}$ we have $u_{\mu k-2, m-1} \leq \beta_r - (mk-1)d_2$ and (25) is satisfied for $s = \mu-2$. Since $2mk-\mu k = (m-1)k \geq 4$ and $\beta_\mu - \beta_{\mu-1} < d_2$, we observe that $\beta_\mu - (mk-2)d_2, \beta_{\mu-1} - (mk-2)d_2, \beta_\mu - (mk-1)d_2, \beta_{\mu-1} - (mk-1)d_2$ are all in the $(m-1)$ th column of Figure (2). Let $u_{i, m-1} = \beta_\mu - (mk-2)d_2$. Then we have the following possibilities for $(u_{i+1, m-1}, u_{i+2, m-1}, u_{i+3, m-1})$:

- (i) $(\beta_{\mu-1} - (mk-2)d_2, \beta_\mu - (mk-1)d_2, \beta_{\mu-1} - (mk-1)d_2)$
- (ii) $(\beta_{\mu-1} - (mk-2)d_2, \beta_\mu - (mk-1)d_2, \beta_{\mu-2})$
- (iii) $(\beta_{\mu-2} - J_7 d_2, \beta_{\mu-1} - (mk-2)d_2, \beta_\mu - (mk-1)d_2)$
- (iv) $(\beta_{\mu-1} - (mk-2)d_2, \beta_{\mu-2} - J_8 d_2, \beta_\mu - (mk-1)d_2)$

for some J_7, J_8 with $0 \leq J_7, J_8 \leq mk-1$. In the possibility (ii), we note that $u_{i+3, m-1} = \beta_{\mu-2}$. For, if $u_{i+3, m-1} = \beta_{\mu-2} - J_9 d_2$ for some J_9 with $0 < J_9 \leq mk-1$, then $\beta_\mu - (mk-2)d_2 > \beta_{\mu-2} - (J_9-1)d_2 > \beta_{\mu-2} - J_9 d_2$. Thus either $u_{i+1, m-1}$ or $u_{i+2, m-1}$ must be equal to $\beta_{\mu-2} - (J_9-1)d_2$ which is not possible. When (i) or (ii) holds, we observe that atleast two of $u_{i+2, m}, u_{i+1, m}, u_{i, m}$ belong to the same arithmetic progression with common difference d_2 since these three elements lie in atleast two arithmetic progressions with common difference d_2 containing β_μ and $\beta_{\mu-1}$. Thus $u_{i+2, m} - u_{i, m} \geq d_2$. Now, we apply Lemma 1 with $i = i, j = i+2$ to obtain a contradiction. A similar application of Lemma 1 with $i = i, j = i+3$ leads to a contradiction whenever (iii) or (iv) holds. Here, we need to observe that atleast two of $u_{i+3, m}, u_{i+2, m}, u_{i+1, m}, u_{i, m}$ belong to the same arithmetic progression with common difference d_2 since these four elements lie in atleast three arithmetic progressions with common difference d_2 containing $\beta_\mu, \beta_{\mu-1}$ and $\beta_{\mu-2}$. Thus the case $K_1 = 2, \mu = m+1$ does not hold. This completes the proof of Theorem 2. \square

Proof of Corollary. As in the proof of Theorem 2, we may assume that $|y| > c_1$. Further, by Theorem 2, we have $m \geq 3$ and $\mu \geq m+2$. As in (13),

we get for $\ell \geq 2$,

$$\sum_{h=1}^{\ell} t_{i,h} = \frac{\ell}{\mu}(\beta_1 + \cdots + \beta_{\mu}) - \frac{\ell}{2}(\ell k - 1)d_1 \quad \text{for } 1 \leq i \leq \mu k.$$

From the above equality with $i = \mu k$ and $t_{\mu k, \ell} = \beta_{\mu}$, we get

$$\begin{aligned} \beta_{\mu} - (\ell - 1)(\ell k - 1)d_1 &\leq \frac{\ell}{\mu}(\beta_1 + \cdots + \beta_{\mu}) - \frac{\ell}{2}(\ell k - 1)d_1 \\ &\leq \frac{\ell}{m+2}(\beta_1 + \cdots + \beta_{\mu}) - \frac{\ell}{2}(\ell k - 1)d_1 \end{aligned}$$

which implies that

$$\beta_{\mu} \leq \frac{\ell}{m - \ell + 2}(\beta_1 + \cdots + \beta_{\mu-1}) + \frac{(m+2)(\ell-2)(\ell k - 1)d_1}{2(m - \ell + 2)}.$$

This contradicts our assumption. For $\ell = 1$, we use (13) with $i = \mu k$ and $\mu \geq m+2$ to obtain $\beta_{\mu} \leq \frac{m}{2}(\beta_1 + \cdots + \beta_{\mu-1}) + \frac{(m^2-4)(mk-1)d_2}{4}$. This proves the Corollary. \square

3. Proof of Theorem 1

Denote by c_4, c_5, c_6 and c_7 effectively computable numbers depending only on $d_1, d_2, m, \mu, s_1, \dots, s_{\mu}$. As in the proof of Theorem 2, we may suppose that $|y| \geq c_4$ with c_4 sufficiently large and we shall arrive at a contradiction. In the notation of Theorem 2, we set $s_i = \beta_i, 1 \leq i \leq \mu$, $f(X) = g(X)$ if equation (1) holds with $+$ sign and $f(X) = g^2(X)$ if equation (1) holds with $-$ sign. By the assumption that $P_1(X) \cdots P_{\mu}(X)$ and $Q_1(Y) \cdots Q_{\mu}(Y)$ have simple roots, we have $|T| = \ell k \mu$ and $|U| = m k \mu$ so that the elements of T as well as U are distinct. Thus the assumptions of Theorem 2 are satisfied so that Figure (1), Figure (2), Lemma 1 and assertions of Theorem 2 are valid.

Let $m = 2$ or $\mu \in \{2, 3, 4\}$. Then we derive from Theorem 2 that $|y| \leq c_5$ which is not possible if c_4 is sufficiently large. It remains to prove Theorem 1 under the conditions (iii) and (iv) in (3).

(iii) Let $d_2 = 1$. In view of Theorem 1 (i), we may assume that $m \geq 3$. By Theorem 2(b), we need to consider $\mu > m+1 \geq 4$. Since $\beta_1, \dots, \beta_{\mu}$ are rational integers, we observe that the elements of U are ordered as

$$(27) \quad \begin{aligned} \beta_1 - (mk - 1) &< \beta_1 - (mk - 2) < \cdots < \beta_1 < \beta_2 - (mk - 1) \\ &< \cdots < \beta_2 < \cdots < \beta_{\mu} - (mk - 1) < \cdots < \beta_{\mu}. \end{aligned}$$

Further, from (27), we see that among three consecutive u 's in Figure (2), atleast two of them are consecutive integers. In particular, either

$$u_{\mu k-2, m-1} - u_{\mu k-1, m-1} = 1$$

or

$$u_{\mu k-1, m-1} - u_{\mu k, m-1} = 1.$$

We apply Lemma 1 with $i = \mu k - 2, j = \mu k - 1$ if the former equality holds and with $i = \mu k - 1, j = \mu k$ if the latter equality holds to get a contradiction.

(iv) Let $d_1 = 1$. From Theorem 1(i), we derive that $m \geq 3$. First, we take $\ell \geq 3$. Then, by Theorem 2(b), we may assume that $\mu \geq m + 2 \geq \ell + 3 \geq 6$. We use (11) and argue as in Lemma 1 to obtain $t_{i, \ell-1} - t_{j, \ell-1} > t_{j, \ell} - t_{i, \ell}$ for $1 \leq i < j \leq \mu k$. Then we apply the preceding inequality as in the case (iii) to get the assertion. Next, we consider $\ell = 2$ and $\mu \equiv 1 \pmod{2}$. Let $\mu = 2\delta + 1$. Then we observe from Figure (1) that $t_{1,1} = \beta_{\mu-\delta} - k, t_{1,2} = \beta_{\mu-\delta} - (k-1)$. We use (9) with $i = 1$ to obtain

$$(x - \beta_{\mu-\delta} + k)(x - \beta_{\mu-\delta} + k - 1) = (y - u_{1,1}) \cdots (y - u_{1,m})$$

which implies

$$x_2^2 = (y - u_{1,1}) \cdots (y - u_{1,m}) + \frac{1}{4}$$

where $x_2 = x + \frac{2k-1-2\beta_{\mu-\delta}}{2}$. We apply Theorem III of [3] to derive that the polynomial $4(Y - u_{1,1}) \cdots (Y - u_{1,m}) + 1$ is irreducible over \mathbb{Q} . Now, we apply a theorem of Baker [1] on hyper elliptic equations to conclude that $|y| < c_6$ which is not possible if c_4 is sufficiently large. Finally, we consider $\ell = 1, k \geq 2$. Then $t_{1,1} = \beta_1 - (k-1), t_{2,1} = \beta_1 - (k-2)$. Thus, from (9) with $i = 1, 2$, we get

$$\begin{aligned} x - \beta_1 + k - 1 &= (y - u_{1,1}) \cdots (y - u_{1,m}) \\ x - \beta_1 + k - 2 &= (y - u_{2,1}) \cdots (y - u_{2,m}) \end{aligned}$$

which implies

$$(x - \beta_1 + k - 1)(x - \beta_1 + k - 2) = (y - u_{1,1}) \cdots (y - u_{1,m})(y - u_{2,1}) \cdots (y - u_{2,m})$$

i.e.,

$$x_3^2 = (y - u_{1,1}) \cdots (y - u_{1,m})(y - u_{2,1}) \cdots (y - u_{2,m}) + \frac{1}{4}$$

where $x_3 = x + \frac{2k-3-2\beta_1}{2}$. Now, we apply the results of [3] and [1] as in the case $\ell = 2, \mu \equiv 1 \pmod{2}$ for deriving that $|y| < c_7$ and this completes the proof of Theorem 1. \square

Remark: The argument for the assertion in the beginning of the first paragraph on page 72 of [5] should be corrected as follows: Observe that $[\mathbb{Q}(t_{i,j}) : \mathbb{Q}(v_i)]$ for $1 \leq j \leq \ell$ and $[\mathbb{Q}(u_{i,j'}) : \mathbb{Q}(v_i)]$ for $1 \leq j' \leq m$ are equal to $\mu/[\mathbb{Q}(v_i) : \mathbb{Q}]$. Therefore, by (10) and (11), $\mu/[\mathbb{Q}(v_i) : \mathbb{Q}]$ divides ℓ and m and hence $[\mathbb{Q}(v_i) : \mathbb{Q}] = \mu$.

REFERENCES

- [1] A. Baker, *Bounds for the solutions of the hyperelliptic equation*, Proc. Camb. Phil. Soc. **65** (1969), 439–444.
- [2] A. Brauer and G. Ehrlich, *On the irreducibility of certain polynomials*, Bull. Amer. Math. Soc. **52** (1946), 844–856.
- [3] H.L. Dorwart and O. Ore, *Criteria for the irreducibility of polynomials*, Ann. of Math. **34** (1993), 81–94.
- [4] N. Saradha, T.N. Shorey and R. Tijdeman, *On arithmetic progressions with equal products*, Acta Arithmetica **68** (1994), 89–100.
- [5] N. Saradha, T.N. Shorey and R. Tijdeman, *On values of a polynomial at arithmetic progressions with equal products*, Acta Arithmetica **72** (1995), 67–76.
- [6] T.N. Shorey, *London Math. Soc. Lecture Note Series*, Number Theory, Paris 1992-3, éd. Sinnou David, **215** (1995), 231–244.

N. SARADHA
 School of Mathematics
 Tata institut of Fundamental Research
 Homi Bhabha Road
 Bombay 400 005
 INDIA
 e-mail: saradha@math.tifr.res.in