La contribution pour la minoration de θ ne provenant pas des $A(T, N_t)$ entiers est au moins égale à ce qu'elle serait si ces entiers étaient isolés, puisque $n_1+n_2+\ldots+n_{k-1}+\lambda \leqslant k\lambda$. Il en résulte que si t dépasse l'entier t_0 défini précédemment, alors:

$$M(K, N_t) \geqslant \frac{1}{2}\{M(L, N_t)+M(L', N_t)\}+\frac{a-2}{4(a-1)}-\varepsilon.$$

Bibliographie

[1] R. Béjian, *Minoration de la discrépance d'une suite quelconque sur T*, Annales de la Faculté des Sciences de Toulouse, Mathématiques, Université Paul Sabatier, Série 5, tome 1, fascicule 3, 1979, 79-éme volume de la collection, p. 201–213.
[2] H. Faure, *Discrépance des suites associées à un système de minoration*, a paraître.
[3] L. Kuipers and H. Niederreiter, *Uniform distribution of sequences*, J. Wiley and Sons, 1974, p. 107–109.
[4] P. Liardet, *Discrépance sur la cercle*, Primaths, n° 1; Université de Provence, 1979, p. 7–11.
[5] K. F. Roth, *On irregularities of distribution*, Mathematika 1 (1954), p. 73–79.
[6] W. M. Schmidt, *Irregularities of distribution VII*, Acta Arith. 21 (1972), p. 45–60.
[7] R. Tijdeman et G. Wagner, Résultat non publié.
[8] T. van Aardenne-Ehrenfest, *Proof of the impossibility of a just distribution*, Indag. Math. 11 (1949), p. 264–269.
[9] J. G. van der Corput, *Verteilungsfunktionnen*, Proc. Kon. Ned. V. Wetensch. 38 (1935), p. 813–821.

Reçu le 3.4.1980
et dans la forme modifiée le 2.6.1980 (1203)

ACTA ARITHMETICA
XLI (1982)

An application of Hilbert's irreducibility theorem to diophantine equations

by

A. Schinzel (Warszawa)

This paper is a sequel to [3]. That was a study of polynomials F with the property that for every integer t^* (or for some integer t^* from every arithmetic progression) the equation $F(x, y, t^*) = 0$ is solvable for integers x, y. It has been proved that under suitable conditions on F this property implies the solvability of $F(x, y, t) = 0$ for x, y in $Q[t]$. It has been shown also by an example that the result fails if t is replaced by a two-dimensional vector $\boldsymbol{t}$. In the present paper I show how to modify the assertion so that it remains true for vector $\boldsymbol{t}$ of any dimension. The principal tool is the classical Hilbert's irreducibility theorem in a slightly refined form given in [2].

I shall prove the following theorems.

Theorem 1. *Let $F \in Q[u, \boldsymbol{\tau}, t]$, $M \in Q[\boldsymbol{\tau}, t]$, $\boldsymbol{\tau} = \langle \tau_1, \ldots, \tau_r\rangle$. Suppose that for every r arithmetic progressions $P_1, \ldots, P_r$ there exist integers $\tau_1^*, \ldots, \tau_r^*$ and polynomials $x, y \in Q[t]$ such that $\tau_s^* \in P_s$ $(1 \leqslant s \leqslant r)$ and*

$$F(x(t), \boldsymbol{\tau}^*, t) = M(\boldsymbol{\tau}^*, t)y(t).$$

Then there exist polynomials $X \in Q(\boldsymbol{\tau})[t]$, $Y \in Q(\boldsymbol{\tau})[t]$ satisfying

$$F(X(t), \boldsymbol{\tau}, t) = M(\boldsymbol{\tau}, t)Y(t).$$

Theorem 2. *Let $F \in Q[u, \boldsymbol{\tau}, t]$ be of degree at most four in u, $M \in Q[\boldsymbol{\tau}, t]$. Suppose that for every $r+1$ arithmetic progressions $P_1, \ldots, P_{r+1}$ there exist integers $\tau_1^*, \ldots, \tau_r^*, t^*, x, y$ such that $\tau_i^* \in P_i$ $(1 \leqslant i \leqslant r)$, $t^* \in P_{r+1}$ and*

$$F(x, \boldsymbol{\tau}^*, t^*) = M(\boldsymbol{\tau}^*, t^*)y.$$

Then there exist polynomials $X, Y \in Q(\boldsymbol{\tau})[t]$ satisfying

$$F(X(t), \boldsymbol{\tau}, t) = M(\boldsymbol{\tau}, t)Y(t).$$

The proof of Theorem 1 is based on the two following lemmata.

Lemma 1. *Let $M \in Q[\boldsymbol{\tau}, t]$ be squarefree with respect to t, $F \in Q[x, \boldsymbol{\tau}, t]$ have the leading coefficient with respect to x prime to M. There exist a non-zero* *polynomial* $\Phi \in Q[u, \tau, t]$ *such that if* $\tau^* \in C^r$, $x \in C[t]$, *the degree of* x *with respect to* t *is less than the degree of* M *and*

$$F(x(t), \tau^*, t) \equiv 0 \bmod M(\tau^*, t)$$

then

$$\Phi(x(t), \tau^*, t) = 0.$$

Moreover the leading coefficient of Φ *with respect to* u *is independent of* t.

Proof. Let F be of degree f in x with the leading coefficient $a(\tau, t)$, M be of degree m in t with the leading coefficient $\mu(\tau)$. If $m = 0$ the condition on the degree of x implies $x = 0$, thus we can take $\Phi(u, \tau, t) = u$. If $m > 0$ let for indeterminates $x_0, \ldots, x_{m-1}$

$$F\Big(\sum_{i=0}^{m-1} x_i t^i, \tau, t\Big) = \sum_{j=0}^{h} A_j(x_0, \ldots, x_{m-1}, \tau) t^j \qquad (h \geqslant m-1)$$

and let $B_j(x_0, \ldots, x_{m-1}, \tau)$ be the homogeneous part of A_j of degree f with respect to $x_0, \ldots, x_{m-1}$, if A_j is of that degree, otherwise $B_j = 0$. Clearly

$$a(\tau, t)\Big(\sum_{i=0}^{m-1} x_i t^i\Big)^f = \sum_{j=0}^{h} B_j(x_0, \ldots, x_{m-1}, \tau) t^j.$$

We have for each $j \leqslant h$

$$\mu(\tau)^h t^j \equiv \sum_{i=0}^{m-1} a_{ij} t^i \bmod M(\tau, t), \qquad a_{ij} \in Q[\tau].$$

Hence in the ring $Q[\tau, t]$

$$(1) \quad \mu(\tau)^h F\Big(\sum_{i=0}^{m-1} x_i t^i, \tau, t\Big) \equiv \sum_{j=0}^{h} A_j \sum_{i=0}^{m-1} a_{ij} t^i \equiv \sum_{i=0}^{m-1} t^i \sum_{j=0}^{h} a_{ij} A_j \bmod M(\tau, t)$$

and similarly

$$(2) \qquad \mu(\tau)^h a(\tau, t)\Big(\sum_{i=0}^{m-1} x_i t^i\Big)^f \equiv \sum_{i=0}^{m-1} t^i \sum_{j=0}^{h} a_{ij} B_j \bmod M(\tau, t).$$

Let us consider the system of polynomials

$$(3a) \quad F_i(x_0, \ldots, x_m, \tau) = x_m^f \sum_{j=0}^{h} a_{ij} A_j\Big(\frac{x_0}{x_m}, \ldots, \frac{x_{m-1}}{x_m}, \tau\Big) \qquad (i = 0, \ldots, m-1),$$

$$F_m(x_0, \ldots, x_m, \tau, t, u) = \sum_{i=0}^{m-1} x_i t^i - x_m u$$

where u is a new indeterminate.

We assert that the resultant $R(u, \tau, t)$ of the above system with respect to $x_0, \ldots, x_m$ is non-zero. Indeed by a known property of resultants (see [1], p. 11) the cofactor of u^{f^m} in R is the resultant R_0 of the system

$$(3b) \quad F_i(x_0, \ldots, x_{m-1}, 0, \tau) = \sum_{j=0}^{h} a_{ij} B_j(x_0, \ldots, x_{m-1}, \tau) \qquad (i = 0, \ldots, m-1).$$

Now, if $R_0 = 0$ then by the fundamental property of resultants the system $F_i(x_0, \ldots, x_{m-1}, 0, \tau) = 0$ has a non-zero solution $(\xi_0, \ldots, \xi_{m-1})$ in the algebraic closure $\widehat{Q(\tau)}$ of $Q(\tau)$. From (2) and (3b) we get

$$\mu(\tau)^h a(\tau, t)\Big(\sum_{i=0}^{m-1} \xi_i t^i\Big)^f \equiv 0 \bmod M(\tau, t),$$

where the congruence is in the ring $\widehat{Q(\tau)}[t]$. But by the assumption $(a(\tau, t), M(\tau, t)) = 1$ and $M(\tau, t)$ is square-free with respect to t, hence

$$\sum_{i=0}^{m-1} \xi_i t^i \equiv 0 \bmod M(\tau, t)$$

and M being of degree m we get $\xi_i = 0$ $(0 \leqslant i < m)$, a contradiction. Thus $R_0 \neq 0$, R_0 is independent of t. We set

$$(4) \qquad \Phi(u, \tau, t) = \mu(\tau) R(u, \tau, t).$$

Clearly the leading coefficient of Φ with respect to u is μR_0 and is independent of t.

Suppose now that for a $\tau^* \in C^r$ and $x \in C[t]$ we have

$$x(t) = \sum_{i=0}^{m-1} \xi_i t^i \quad \text{and} \quad F(x(t), \tau^*, t) \equiv 0 \bmod M(\tau^*, t).$$

Then either $\mu(\tau^*) = 0$ and by (4) $\Phi(x(t), \tau^*, t) = 0$ or $\mu(\tau^*) \neq 0$ and then (1) implies

$$\sum_{j=0}^{h} a_{ij}(\tau^*) A_j(\xi_0, \ldots, \xi_{m-1}, \tau^*) = 0 \qquad (0 \leqslant i \leqslant m-1).$$

This gives by (3a)

$$F_i(\xi_0, \ldots, \xi_{m-1}, 1, \tau^*) = 0 \qquad (0 \leqslant i \leqslant m-1)$$

and also $F_m(\xi_0, \ldots, \xi_{m-1}, 1, \tau^*, t, x(t)) = 0$. Thus $R(x(t), \tau^*, t) = 0$ and by (4) $\Phi(x(t), \tau^*, t) = 0$.

Lemma 2. *Let* $P(\tau, t)$ *be a polynomial irreducible over* Q *of positive degree in* t, ν *a positive integer and let* $F_i \in Q[x, \tau, t]$ $(1 \leqslant i \leqslant k)$. *If for* *every r arithmetic progressions $P_1, \ldots, P_r$ there exist integers $\tau_1^*, \ldots, \tau_r^*$, an index $i \leqslant k$ and a polynomial $x \in Q[t]$ such that $\tau_s^* \in P_s$ $(s \leqslant r)$,*

$$F_i(x(t), \tau^*, t) \equiv 0 \bmod P(\tau^*, t)^\nu \tag{5}$$

then there exist an index $i \leqslant k$ and a polynomial $X \in Q(\tau)[t]$ such that

$$F_i(X(\tau, t), \tau, t) \equiv 0 \bmod P(\tau, t)^\nu . \tag{6}$$

Proof by induction on ν. For $\nu = 1$ we can at once dispose of the trivial case where for some i we have $F_i(0, \tau, t) \equiv 0 \bmod P(\tau, t)$. This case being excluded we represent F_i in the form

$$F_i(x, \tau, t) = G_i(x, \tau, t) + P(\tau, t) H_i(x, \tau, t) x^{d_i} \tag{7}$$

where the degree of G_i with respect to x is less than d_i, and the leading coefficient of G_i with respect to x is not divisible by P. Then we take in Lemma 1

$$F = \prod_{i=1}^{k} G_i(x, \tau, t), \qquad M = P(\tau, t). \tag{8}$$

Let $\Phi(u, \tau, t)$ be a polynomial, the existence of which is asserted in that lemma. Let further

$$\Phi(u, \tau, t) = \Phi_0(\tau, t) \prod_{\varrho=1}^{\varrho_1} \Phi_\varrho(u, \tau, t), \tag{9}$$

where $\Phi_0 \in Q[\tau, t]$, $\Phi_\varrho \in Q[u, \tau, t]$, Φ_ϱ is irreducible over Q $(1 \leqslant \varrho \leqslant \varrho_1)$ and is of degree 1 in u for $\varrho \leqslant \varrho_0$, of degree at least 2 in u for $\varrho > \varrho_0$. By Lemma 1 the leading coefficient of Φ with respect to u is independent of t hence

$$\Phi_0(\tau, t) = \Psi_0(\tau) \tag{10}$$

and we may denote by $\Psi_\varrho(\tau)$ the leading coefficient of Φ_ϱ with respect to u. If for all positive $\varrho \leqslant \varrho_0$ we have

$$H_\varrho(\tau, t) = \Psi_\varrho(\tau)^f F\left(-\frac{\Phi_\varrho(0, \tau, t)}{\Psi_\varrho(\tau)}, \tau, t\right) \not\equiv 0 \bmod P(\tau, t) \tag{11}$$

then the resultant R_ϱ of H_ϱ and P with respect to t is different from 0. In virtue of Theorem 1 of [2] there exist r arithmetic progressions $P_1, \ldots, P_r$ such that for all vectors $\tau^* \in P_1 \times \ldots \times P_r$ all polynomials $\Phi_\varrho(x, \tau^*, t)$ are irreducible $(1 \leqslant \varrho \leqslant \varrho_1)$ and

$$\prod_{\varrho=0}^{\varrho_1} \Psi_\varrho(\tau^*) \prod_{\varrho=1}^{\varrho_0} R_\varrho(\tau^*) \pi(\tau^*) \neq 0 \tag{12}$$

where $\pi(\tau)$ is the leading coefficient of P with respect to t. If we combine this with (5) we get a contradiction. Indeed for $\tau^* \in P_1 \times \ldots \times P_r$ from (5) and (7) we get

$$G_i(x(t), \tau^*, t) \equiv 0 \bmod P(\tau^*, t),$$

hence by (8)

$$F(x(t), \tau^*, t) \equiv 0 \bmod P(\tau^*, t).$$

Let $x(t) = P(\tau^*, t) y(t) + x_1(t)$, where the degree of x_1 with respect to t is less than the degree of P, $y \in Q[t]$.

We have

$$F(x_1(t), \tau^*, t) \equiv 0 \bmod P(\tau^*, t) \tag{13}$$

and by Lemma 1

$$\Phi(x_1(t), \tau^*, t) = 0.$$

Hence by (9)

$$\Phi_0(\tau^*, t) \prod_{\varrho=1}^{\varrho_1} \Phi_\varrho(x_1(t), \tau^*, t) = 0.$$

By (10) and (12) $\Phi_0(\tau^*, t) \neq 0$, moreover since $\Phi_\varrho(u, \tau^*, t)$ is irreducible of degree $\geqslant 2$ for $\varrho > \varrho_0$ we have $\Phi_\varrho(x_1(t), \tau^*, t) \neq 0$ for $\varrho > \varrho_0$. Thus there exists a $\varrho \leqslant \varrho_0$ such that

$$\Phi_\varrho(x_1(t), \tau^*, t) = 0$$

and then

$$x_1(t) = -\frac{\Phi_\varrho(0, \tau^*, t)}{\Psi_\varrho(\tau^*)}.$$

From (11) and (13) we get

$$H_\varrho(\tau^*, t) \equiv 0 \bmod P(\tau^*, t)$$

and $\pi(\tau^*) R_\varrho(\tau^*) = 0$ contrary to (12). The obtained contradiction proves that for a positive $\varrho \leqslant \varrho_0$ we have

$$\Psi_\varrho(\tau)^f F\left(-\frac{\Phi_\varrho(0, \tau, t)}{\Psi_\varrho(\tau)}, \tau, t\right) \equiv 0 \bmod P(\tau, t).$$

From (8) and the irreducibility of P it follows that for a certain $i \leqslant k$

$$G_i\left(-\frac{\Phi_\varrho(0, \tau, t)}{\Psi_\varrho(\tau)}, \tau, t\right) \equiv 0 \bmod P(\tau, t),$$

where the congruence is taken in the ring $Q(\tau)[t]$. Then by (7)

$$F_i(X(t),\tau,t)\equiv 0 \bmod P(\tau,t),\qquad X=-\frac{\Phi_\varrho(0,\tau,t)}{\Psi_\varrho(\tau)}\in Q(\tau)[t]$$

which shows (6) for $\nu=1$.

Now, let us suppose that the lemma is true for the modulus $P^{\nu-1}$ ($\nu>1$).

Let

$$(14)\qquad F_i(x,\tau,t)\equiv\prod_{j=1}^{J_i}\big(x-x_{ij}(\tau,t)\big)\cdot F_{i0}(x,\tau,t) \bmod P(\tau,t),$$

where $x_{ij}(\tau,t)\in Q(\tau)[t]$, $F_{i0}\in Q(\tau)[x,t]$. Choose $D_i\in Q[t]$ such that $D_iF_{i0}\in Q[x,\tau,t]$ and the congruence $F_{i0}(x,\tau,t)\equiv 0 \bmod P(\tau,t)$ is unsoluble for $x\in Q(\tau)[t]$. We have for each $j\leqslant J_i$ and a suitable $D_{ij}\in Q[\tau]$

$$(15)\qquad D_{ij}(\tau)F_i\big(x_{ij}(\tau,t)+P(\tau,t)y,\tau,t\big)=P(\tau,t)F_{ij}(y,\tau,t),\qquad F_{ij}\in Q[y,\tau,t].$$

In virtue of the already proved case $\nu=1$ of the lemma there exist arithmetic progressions $P_1,\ldots,P_r$ such that if $\tau_s^*\in P_s$ $(1\leqslant s\leqslant r)$ then none of the congruences $D_iF_{i0}(x,\tau^*,t)\equiv 0 \bmod P(\tau^*,t)$ $(1\leqslant i\leqslant k)$ is solvable. We may assume moreover choosing if necessary some subprogressions of $P_1,\ldots,P_r$ and using Theorem 1 of [2] that all progressions P_i have the same difference and that for $\tau^*\in P_1\times\ldots\times P_r$ the polynomial $P(\tau^*,t)$ is irreducible. For $\tau^*\in P_1\times\ldots\times P_r$ and for each $i\leqslant k$ the conditions (5) and (14) imply that $x(t)\equiv x_{ij}(\tau^*,t) \bmod P(\tau^*,t)$ for a certain $j\leqslant J_i$.

Hence $x(t)=x_{ij}(\tau^*,t)+P(\tau^*,t)y(t)$ and by (5) and (15) we get

$$F_{ij}\big(y(t),\tau^*,t\big)\equiv 0 \bmod P(\tau^*,t)^{\nu-1}.$$

Let $P_s=\{n\in Z:\ n\equiv b_s \bmod a\}$, $\boldsymbol{b}=\langle b_1,\ldots,b_r\rangle$. By the inductive assumptions applied to the set of polynomials $F_{ij}(y,a\tau+\boldsymbol{b},t)$ $(1\leqslant i\leqslant k, 1\leqslant j\leqslant J_i)$ we infer the existence of a pair (i,j) and of a polynomial $Y\in Q(\tau)[t]$ such that $1\leqslant i\leqslant k$, $1\leqslant j\leqslant J_i$,

$$F_{ij}\big(Y(\tau,t),\tau,t\big)\equiv 0 \bmod P(\tau,t)^{\nu-1}.$$

It follows now from (15) that (6) holds with

$$X(\tau,t)=x_{ij}(\tau,t)+P(\tau,t)Y(\tau,t).$$

Proof of Theorem 1. Assume first that $M\neq 0$ and let

$$M(\tau,t)=P_0(\tau)\prod_{l=1}^{m}P_l(\tau,t)^{\nu_l}$$

where for $l\geqslant 1$ the polynomials $P_l(\tau,t)$ are of positive degree in t, irreducible and prime to each other. For each $l\leqslant m$ the assumptions of Lemma 2 are satisfied with $k=1$, $P=P_l$, $\nu=\nu_l$; $F_1=F$. Hence by the said lemma there exist polynomials $X_l,Y_l\in Q(\tau)[t]$ such that

$$F\big(X_l(\tau,t),\tau,t\big)=P_l^{\nu_l}Y_l(\tau,t)$$

and it is enough to choose

$$X\equiv X_l \bmod P_l,\qquad Y\equiv Y_l \bmod P_l\qquad (1\leqslant l\leqslant m).$$

Assume now that $M=0$. Let

$$(16)\qquad F(x,\tau,t)=F_0(\tau,t)\prod_{\sigma=1}^{\sigma_1}F_\sigma(x,\tau,t)$$

where for $\sigma\geqslant 1$ the polynomials $F(x,\tau,t)$ are irreducible, moreover $F_\sigma(x,\tau,t)$ is of degree 1 in x for $\sigma\leqslant\sigma_0$ and of degree at least 2 in x for $\sigma>\sigma_0$. Let $\phi_\sigma(\tau,t)$ be the leading coefficient of F_σ with respect to x.

From the irreducibility of $F_\sigma(x,\tau,t)$ it follows for $\sigma\leqslant\sigma_0$ that $\big(\phi_\sigma(\tau,t),F_\sigma(0,\tau,t)\big)=1$ hence the resultant $R_\sigma(\tau)$ of $\phi_\sigma(\tau,t)$ and $F_\sigma(0,\tau,t)$ with respect to t is non-zero. If for a positive $\sigma\leqslant\sigma_0$ we have $\phi_\sigma\in Q[\tau]$ then we take $X=-\dfrac{F_\sigma(0,\tau,t)}{\phi_\sigma(\tau,0)}$, $Y=0$.

If for all positive $\sigma\leqslant\sigma_0$ we have $\phi_\sigma\notin Q[\tau]$ then let $\psi_\sigma(\tau)$ be the leading coefficient of ϕ_σ with respect to t $(0\leqslant\sigma\leqslant\sigma_0)$. In virtue of Theorem 1 of [2] there exist arithmetic progressions $P_1,\ldots,P_r$ such that for $\tau\in P_1\times\ldots\times P_r$ all polynomials $F_\sigma(x,\tau^*,t)$ are irreducible and

$$(17)\qquad \prod_{\sigma=0}^{\sigma_1}\psi_\sigma(\tau^*)\prod_{\sigma=1}^{\sigma_0}R_\sigma(\tau^*)\neq 0.$$

If we combine this with the condition

$$F\big(x(t),\tau^*,t\big)=0$$

we get a contradiction. Indeed by (16) we have for a positive $\sigma\leqslant\sigma_1$

$$F_\sigma\big(x(t),\tau^*,t\big)=0$$

and since for $\sigma>\sigma_0$ the polynomial $F_\sigma(x,\tau^*,t)$ is irreducible of degree at least 2 in x we get $\sigma\leqslant\sigma_0$. Hence

$$\phi_\sigma(\tau^*,t)x(t)+F_\sigma(0,\tau^*,t)=0,\qquad \phi_\sigma(\tau^*,t)\,|\,F_\sigma(0,\tau^*,t)$$

and since by (17) $R_\sigma(\tau^*)\neq 0$ it follows that $\phi_\sigma(\tau^*,t)\in Q$. This however is impossible because ϕ_σ is of degree at least 1 in t and $\psi_\sigma(\tau^*)\neq 0$.

For the proof of Theorem 2 we shall need one more lemma.

LEMMA 3. *Let $L \in Z[x, t]$ be of degree at most four in x, $P_0 \in Z[t]$ be irreducible. If for all sufficiently large primes p and all integers t^* such that $p \| P_0(t^*)$ the congruence $L(x, t^*) \equiv 0 \bmod p^\nu$ is solvable in Z then the congruence $L(x, t) \equiv 0 \bmod P_0(t)^\nu$ is solvable in $Q[t]$.*

Proof. For the case, where P_0 is primitive the lemma is proved in [3] as Lemma 6. In general let $P_0 = cP_1$, where P_1 is primitive. Since for all primes $p \nmid c$ the relations $p \| P_0(t^*)$ and $p \| P_1(t^*)$ are equivalent the general case follows from the special case mentioned earlier.

Proof of Theorem 2. If $M = 0$ the assertion follows from [2], Theorem 2. If $M \neq 0$ it is enough in virtue of the Chinese Remainder Theorem for the ring $Q(\boldsymbol{\tau})[t]$ to prove the assertion for the case $M = P(\boldsymbol{\tau}, t)^\nu$, where $P \in Z(\boldsymbol{\tau}, t)$ is an irreducible polynomial of positive degree in t. By Theorem 1 of [2] there exist arithmetic progression $P_1, \ldots$ $\ldots, P_r$ such that if $\boldsymbol{\tau}^* \in P_1 \times \ldots \times P_r$ then $P(\boldsymbol{\tau}^*, t)$ is irreducible in $Q[t]$. We may assume without loss of generality that $P_i = \{n \in Z\colon n \equiv b_i \bmod a\}$. Take an integral vector $\boldsymbol{\tau}^*$, an integer t^* and a prime p such that $p \| P(a\boldsymbol{\tau}^* + \boldsymbol{b}, t^*)$. By the assumption applied to the arithmetic progressions $p^\nu u + a\tau_1^* + b_1, \ldots, p^\nu u + a\tau_r^* + b_r, p^\nu u + t^*$ there exist integers $u_1, \ldots, u_{r+1}$, x, y such that

$$F(x, p^\nu \boldsymbol{u} + a\boldsymbol{\tau}^* + \boldsymbol{b}, p^\nu u_{r+1} + t^*) = P(p^\nu \boldsymbol{u} + a\boldsymbol{\tau}^* + \boldsymbol{b}, p^\nu u_{r+1} + t^*) y,$$

where we have put $\boldsymbol{u} = \langle u_1, \ldots, u_r \rangle$. Hence

$$F(x, a\boldsymbol{\tau}^* + \boldsymbol{b}, t^*) \equiv 0 \bmod p^\nu$$

and the assumptions of Lemma 3 are satisfied with $L = F(x, a\boldsymbol{\tau}^* + \boldsymbol{b}, t)$, $P_0 = P(a\boldsymbol{\tau}^* + \boldsymbol{b}, t)$. By that lemma the congruence

$$F(x, a\boldsymbol{\tau}^* + \boldsymbol{b}, t) \equiv 0 \bmod P(a\boldsymbol{\tau}^* + \boldsymbol{b}, t)^\nu$$

is solvable in $Q[t]$, i.e. there exist polynomials $x, y \in Q[t]$ such that

$$F\big(x(t), a\boldsymbol{\tau}^* + \boldsymbol{b}, t\big) = P(a\boldsymbol{\tau} + \boldsymbol{b}, t)^\nu y(t).$$

Since this holds for all integral vectors $\boldsymbol{\tau}^* \in Z^r$ Theorem 1 implies the existence of polynomials $X, Y \in Q(\boldsymbol{\tau})[t]$ such that

$$F\big(X_0(\boldsymbol{\tau}, t), a\boldsymbol{\tau} + \boldsymbol{b}, t\big) = P(a\boldsymbol{\tau} + \boldsymbol{b}, t)^\nu Y_0(\boldsymbol{\tau}, t)$$

and Theorem 2 follows with $X = X_0\left(\dfrac{\boldsymbol{\tau} - \boldsymbol{b}}{a}, t\right)$, $Y = Y_0\left(\dfrac{\boldsymbol{\tau} - \boldsymbol{b}}{a}, t\right)$.

References

[1] F. S. Macaulay, *The algebraic theory of modular systems*, Cambridge 1916, reprint New York 1964.

[2] A. Schinzel, *On Hilbert's Irreducibility Theorem*, Ann. Polon. Math. 16 (1965), pp. 333–340.

[3] — *Families of curves having each an integer point*, Acta Arith. 40 (1982), pp. 399–420.

Received on 14.5.1980
and in revised form on 2.6.1980 (1207)