ACTA ARITHMETICA
XL (1982)

Families of curves having each an integer point

by

A. Schinzel (Warszawa)

H. Davenport, D. J. Lewis and the writer [3] proved that if an equation with integral coefficients $F(x, y, t) = 0$ quadratic in x and y is solvable in rational x, y for at least one integer t from every arithmetic progression, then the equation is solvable in rational functions $x(t), y(t) \in Q(t)$. The question has been raised whether the solvability of $F(x, y, t) = 0$ in integers x, y for all integers t implies the solvability of the equation in polynomials. It is the aim of the present paper to study this question in a more general context. We shall prove

Theorem 1. *If $L \in Z[x, t]$ is of degree at most four in x, $M \in Z[t]$ and every arithmetic progression contains an integer t^* such that $L(x, t^*) = M(t^*)y$ is solvable in integers x, y, then there exist polynomials $X, Y \in Q[t]$ such that $L(X(t), t) = M(t)Y(t)$.*

The theorem is no longer true in general if the degree of L is greater than four. Also for L of degree non-exceeding four the conclusion cannot in general be strenghtened to assert the existence of integer valued polynomials X, Y. The relevant examples will be given after the proof of Theorem 1. Theorem 1 easily implies

Theorem 2. *If $F \in Z[x, y, t]$, the highest homogeneous part F_0 of F with respect to x, y is quadratic and singular and every arithmetic progression contains an integer t^* such that $F(x, y, t^*) = 0$ is solvable in integers x, y, then there exist polynomials $X, Y \in Q[t]$ such that $F(X(t), Y(t), t) = 0$.*

It seems likely that if we assume the solvability of $F(x, y, t) = 0$ in integers x, y for all $t^* \in Z$, the conclusion remains true provided F_0 is reducible over $Q(t)$. However, in general the conclusion fails as it is shown by the following

Theorem 3. *The equation $x^2 - (4t^2+1)^3 y^2 = -1$ is solvable in integers x, y for all $t^* \in Z$, but there exist no polynomials $X, Y \in Q[t]$ such that $X(t)^2 - (4t^2+1)^3 Y(t)^2 = -1$.*

Prompted by a question from Professor J. Leicht I have studied the possibility of modifying the assumptions of Theorem 1 so that they would

imply the existence of integer valued polynomials X, Y. The result is the following

THEOREM 4. *Let n be a positive integer $\not\equiv 0 \pmod 8$, $A, B, M \in Z[t]$. If every arithmetic progression contains an integer t^* such that $A(t^*)x^n + B(t^*) = M(t^*)y$ is solvable in integers x, y, then there exist integer valued polynomials X, Y such that $A(t)X(t)^n + B(t) = M(t)Y(t)$.*

The condition $n \not\equiv 0 \pmod 8$ cannot be relaxed, as I shall show by an example. For $n = 1$ Theorem 4 is contained in a more general result of Skolem [8] concerning polynomials in many variables. According to Skolem the polynomials A, B, M may have any number of variables provided A and M have no common zero. I shall show by an example that already for $n = 2$ the corresponding statement is false. The possibility of extending Theorems 1, 2, and 4 to polynomials in many variables will be studied in a subsequent paper.

For the proof of the above theorems we need several lemmata.

LEMMA 1. *Let D be a Dedekind domain, $f, g, h \in D[x]$, $\mathfrak{p}$ be a prime ideal of D, $f(x) \equiv g(x)h(x) \pmod{\mathfrak{p}}$. If g, h are relatively prime* mod $\mathfrak{p}$ *and the leading coefficient of g is 1, then for every integer $n \geqslant 0$ there exist polynomials $g_n, h_n \in D[x]$ such that*

$$f(x) \equiv g_n(x)h_n(x) \pmod{\mathfrak{p}^{n+1}}, \tag{1}$$

(2) *the degree of g_n equals the degree of g, the leading coefficients of g_n is 1,*

$$g_n(x) \equiv g(x), \quad h_n(x) \equiv h(x) \pmod{\mathfrak{p}}. \tag{3}$$

Proof. This lemma is closely related to Hensel's lemma and can be derived by following the proof of Hensel's lemma given by Hasse [6] up to the point where the solvability of the congruence

$$g_{n-1}z_n + h_{n-1}y_n \equiv f_n \pmod{\mathfrak{p}}, \quad f_n \in D[x]$$

in polynomials $y_n, z_n \in D[x]$ is needed. Then since g_{n-1}, h_{n-1} are relatively prime mod $\mathfrak{p}$ we use the fact that $D/\mathfrak{p}$ is a field.

LEMMA 2. *Let D be a principal ideal domain, $a, b, c \in D$, (p) be a prime ideal of D. If $p \nmid 2a$ and $\Delta = b^2 - 4ac$ the congruence*

$$ax^2 + bx + c \equiv 0 \pmod{p^\nu} \tag{4}$$

is solvable in $x \in D$ if and only if either $\operatorname{ord}_p d \geqslant \nu$ or $\operatorname{ord}_p d = \delta \equiv 0 \pmod 2$ and the congruence $z^2 \equiv dp^{-\delta} \pmod p$ is solvable in D.

Proof. The congruence (4) is equivalent to

$$(2ax + b)^2 \equiv d \pmod{4ap^\nu}$$

and since $p \nmid 2a$, it is solvable if and only if $y^2 \equiv d \pmod{p^\nu}$ is.

If $\delta = \operatorname{ord}_p d \geqslant \nu$ it is enough to take $y = 0$. If $\delta < \nu$, the congruence

implies $\delta = 2\operatorname{ord}_p y \equiv 0 \pmod 2$ and $y = p^{\delta/2}z$, $z^2 \equiv dp^{-\delta} \pmod{p^{\nu-\delta}}$. Thus the necessity of the condition given in the lemma follows. On the other hand, if the condition is satisfied and $z_0^2 \equiv d \pmod p$, $z_0 \in D$, we can apply Lemma 1 with

$$f(x) = x^2 - dp^{-\delta}, \quad g(x) = x - z_0, \quad h(x) = x + z_0, \quad n = \nu - \delta - 1.$$

The congruence

$$x^2 - dp^{-\delta/2} \equiv g_n(x)h_n(x) \pmod{p^{n+1}},$$

where $\deg g_n = \deg g = 1$ and the leading coefficient of g_n is 1, implies that $x^2 \equiv dp^{-\delta/2} \pmod{p^\delta}$ has solutions $\pm g_n(0)$. Multiplying by p^δ, we get

$$\left(p^{\delta/2}g_n(0)\right)^2 \equiv d \pmod{p^\nu}.$$

Remark. The lemma can easily be modified so that it would apply to all Dedekind domains. It is also possible, although not so easy, to prove analogous statements about congruences of degree three and four. For instance, if D is a principal ideal domain, $a, b \in D$, (p) is a prime ideal of D, $p \nmid 3$, then the congruence

$$x^3 + ax + b \equiv 0 \pmod{p^\nu}$$

is solvable in $x \in D$ if and only if either $\operatorname{ord}_p b \geqslant \nu$ or $2\operatorname{ord}_p b > 3\operatorname{ord}_p a$ or $3 \mid \beta = \operatorname{ord}_p b < \nu$, $2\beta \leqslant 3\operatorname{ord}_p a$ and the congruence $z^3 + ap^{-2\beta/3} + bp^{-\beta} \equiv 0 \pmod p$ is solvable.

LEMMA 3. *If $A, B \in Z[t]$, $(A, B) = 1$. For sufficiently large primes p the divisibility $p \mid A(t^*)$, $t^* \in Z$ implies $p \nmid B(t^*)$.*

Proof. Let R be the resultant of A and B. Since $(A, B) = 1$, we have $R \neq 0$ and there exist polynomials $U, V \in Z[t]$ such that $AU + BV = R$. Now, if $p \nmid R$ we have either $p \nmid A(t^*)$ or $p \nmid B(t^*)$.

LEMMA 4. *Let K be an algebraic number field, $F \in K[x]$ be of degree at most four. If the congruence $F(x) \equiv 0 \pmod{\mathfrak{p}}$ is solvable for almost all prime ideals of degree 1 in K then the equations $F(x) = 0$ is solvable in K.*

Proof. If $F(x)$ is irreducible in K then the lemma follows from the more general result of Hasse [5]. If $F(x)$ is reducible in K but has no zero there then its degree must be four. If now the congruence $F(x) \equiv 0 \pmod{\mathfrak{p}}$ is solvable for almost all ideals $\mathfrak{p}$ of K rather than for almost all prime ideals $\mathfrak{p}$ of degree 1 in K then the assertion holds in virtue of Proposition 2 in Fujiwara [4]. However, in the proof of this proposition only prime ideals of degree 1 are needed.

LEMMA 5. *Let $A_i, B_i, C_i \in Z[t] (i = 1, 2)$, let $P \in Z[t]$ be a primitive irreducible polynomial, $A_1A_2 \not\equiv 0 \pmod P$ and the polynomials $A_i(t)x^2 + B_i(t)x + C_i(t)$ $(i = 1, 2)$ be prime* mod $P(t)$. *If for all sufficiently large*

primes p and all integers t^* such that $p \| P(t^*)$ the congruence

$$\prod_{i=1}^{2} \left(A_i(t^*)x^2 + B_i(t^*)x + C_i(t^*)\right) \equiv 0 \pmod{p^\mu} \tag{5}$$

is solvable in $x \in Z$ then the congruence

$$\prod_{i=1}^{2} \left(A_i(t)x^2 + B_i(t)x + C_i(t)\right) \equiv 0 \pmod{P(t)^\mu} \tag{6}$$

is solvable in $Q[t]$.

Proof. Let $D_i(t) = B_i(t)^2 - 4A_i(t)C_i(t) = P(t)^{\delta_i}E_i(t)$, where $P_i \nmid E_i$ $(i = 1, 2)$. (If $D_1 = 0$ or $D_2 = 0$ (6) is clearly solvable.) If for an $i \leqslant 2$, $\delta_i \geqslant \mu$ the congruence $A_i(t)x^2 + B_i(t)x + C_i(t) \equiv 0 \pmod{P(t)^\mu}$ is solvable in virtue of Lemma 2 applied with $D = Q[t]$, hence (6) is solvable also.

Let $P(\vartheta) = 0$, $K = Q(\vartheta)$, $\mathfrak{p}$ be a prime ideal of degree 1 in K with norm p assumed sufficiently large. Choose $t^* \equiv \vartheta \pmod{\mathfrak{p}}$. Then $P(t^*) \equiv 0 \pmod{p}$, $P(t^*+p) \equiv 0 \pmod{p}$, $P(t^*+p) - P(t^*) \equiv pP'(t^*) \pmod{p^2}$. Since $(P', P) = 1$, we have by Lemma 3 $P'(t^*) \not\equiv 0 \pmod{p}$, thus $P(t^*) \not\equiv 0 \pmod{p^2}$ or $P(t^*+p) \not\equiv 0 \pmod{p^2}$. Replacing t^* by t^*+p if necessary we may assume that $P(t^*) \not\equiv 0 \pmod{p^2}$, and that (5) holds for a suitable $x = x^* \in Z$.

Let $R(t)$ be the resultant of $A_i(t)x^2 + B_i(t)x + C_i(t)$ $(i = 1, 2)$ with respect to x. By the assumption we have $(P(t), R(t)) = 1$ and by Lemma 3 $R(t^*) \not\equiv 0 \pmod{p}$. On the other hand, if we had

$$A_i(t^*)x^{*2} + B_i(t^*)x^* + C_i(t^*) \equiv 0 \pmod{p} \qquad (i = 1, 2)$$

it would follow that $R(t^*) \equiv 0 \pmod{p}$. Thus there exists an $i \leqslant 2$ such that

$$A_i(t^*)x^{*2} + B_i(t^*)x^* + C_i(t^*) \equiv 0 \pmod{p^\mu}.$$

Since $(P, E_i) = 1$, we have by Lemma 3 $p \nmid E_i(t^*)$. Thus $\operatorname{ord}_p D_i(t^*) = \delta_i$ and by Lemma 2 applied with $D = Z$ we have $\delta_i \equiv 0 \pmod{2}$ and $\left(\frac{D_i(t^*)p^{-\delta_i}}{p}\right) = 1$, whence $\left(\frac{E_i(t^*)}{p}\right) = 1$.

Now $E_i(t^*) \equiv E_i(\vartheta) \pmod{\mathfrak{p}}$ and we get $\left(\frac{E_i(\vartheta)}{\mathfrak{p}}\right) = 1$.

Take in Lemma 4

$$F(x) = \prod_{i=1}^{2} \left(\frac{1 + (-1)^{\delta_i}}{2} x^2 - E_i(\vartheta)\right).$$

We infer that for almost all prime ideals $\mathfrak{p}$ of degree 1 in K the congruence $F(x) \equiv 0 \pmod{\mathfrak{p}}$ is solvable in K. Hence by Lemma 4 $F(x)$ has a zero in K and since $E_1(\vartheta)E_2(\vartheta) \neq 0$, it follows that for an $i \leqslant 2$ we have $\delta_i \equiv 0 \pmod{2}$ and $E_i(\vartheta) = G(\vartheta)^2$ where $G \in Q[t]$. Hence

$$E_i(t) \equiv G(t)^2 \pmod{P(t)}$$

and by Lemma 2 the congruence $A_i(t)x^2 + B_i(t)x + C_i(t) \equiv 0 \pmod{P(t)^\mu}$ is solvable in $Q[t]$.

Lemma 6. *Let $L \in Z[x, t]$ be of degree at most 4 in x, let $P \in Z[t]$ be irreducible and primitive. If for all sufficiently large primes p and all integers t^* such that $p \| P(t^*)$ the congruence $L(x, t^*) \equiv 0 \pmod{p^\mu}$ is solvable in Z then $L(x, t) \equiv 0 \pmod{P(t)^\mu}$ is solvable in $Q[t]$.*

Proof (by induction on μ). We set $K = Q(\vartheta)$, where $P(\vartheta) = 0$.

$\mu = 1$. Let $\mathfrak{p}$ be a prime ideal to degree 1 in K with norm p assumed sufficiently large, $t^* \equiv \vartheta \pmod{\mathfrak{p}}$. The argument used in the proof of Lemma 5 shows that without loss of generality we may assume $p \| P(t^*)$. Hence $L(x^*, t^*) \equiv 0 \pmod{p}$ for an x^* in Z,

$$L(x^*, \vartheta) \equiv 0 \pmod{\mathfrak{p}}$$

and by Lemma 4 $L(x, \vartheta)$ has a zero in K. Denoting this zero by $X(\vartheta)$, $X \in Q[t]$, we infer from $L(X(\vartheta), \vartheta) = 0$ that

$$L(X(t), t) \equiv 0 \pmod{P(t)}.$$

The inductive step. Suppose that the lemma is true for exponents less than $\mu \geqslant 2$ and all polynomials L satisfying the assumptions. Let the congruence $L(x, t^*) \equiv 0 \pmod{p^\mu}$ be solvable in Z for all sufficiently large primes p and all integers t^* such that $p \| P(t^*)$. By the case $\mu = 1$, $L(x, \vartheta)$ has a zero in K. If $L(x, \vartheta) = 0$ identically then $L(x, t) = P(t)L_1(x, t)$, $L_1 \in Z[x, t]$. For all sufficiently large primes p and all integers t^* such that $p \| P(t^*)$ the congruence $L(x, t^*) \equiv 0 \pmod{p^{\mu-1}}$ is solvable. Hence by the inductive assumption there exists an $X \in Q[t]$ such that $L(X(t), t) \equiv 0 \pmod{P^{\mu-1}(t)}$ and then $L(X(t), t) \equiv 0 \pmod{P^\mu(t)}$. If $L(x, \vartheta)$ has a simple zero we have

$$L(x, \vartheta) = G(x, \vartheta)H(x, \vartheta)$$

where $G, H \in Q[x, t]$ both the degree and the leading coefficient of G with respect to x are 1 and $(G(x, \vartheta), H(x, \vartheta)) = 1$. Hence

$$L(x, t) \equiv G(x, t)H(x, t) \pmod{P(t)},$$

G, H relatively prime mod P and by Lemma 1 applied with $D = Q[t]$, $\mathfrak{p} = (P(t))$ we infer that

$$L(x, t) \equiv G_{\mu-1}(x, t)H_{\mu-1}(x, t) \pmod{P^\mu(t)},$$

where $G_{\mu-1}(x,t)$ is of degree 1 in x with the leading coefficient 1. Therefore $L\big(-G_{\mu-1}(0,t),t\big) \equiv 0 \pmod{P^{\mu}(t)}$.

If $L(x,\vartheta)$ is a product of two coprime quadratic factors we have $L(x,t) \equiv G(x,t)H(x,t) \pmod{P(t)}$, $G, H \in Q[x,t]$, where G, H are quadratic in x, relatively prime mod $P(t)$ and we may assume without loss of generality that the leading coefficient of G with respect to x is 1. By Lemma 1 applied with $D = Q[t]$, $\mathfrak{p} = (P(t))$ we have

$$L(x,t) \equiv G_{\mu-1}(x,t)H_{\mu-1}(x,t) \pmod{P^{\mu}(t)}, \tag{7}$$

where polynomials $G_{\mu-1}, H_{\mu-1} \in Q[t]$ are quadratic with respect to x and relatively prime mod $P(t)$, moreover their leading coefficients are not divisible by $P(t)$. For a suitable integer $d \neq 0$ we have

$$dG_{\mu-1}(x,t)\,dH_{\mu-1}(x,t) \in Z[x,t]$$

and

$$d^2P^{-\mu}(t)\big(L(x,t)-G_{\mu-1}(x,t)H_{\mu-1}(x,t)\big) \in Z[x,t].$$

Hence the solvability of the congruence $L(x,t^*) \equiv 0 \pmod{p^{\mu}}$, for $p \parallel P(t^*)$ implies the solvability of the congruence

$$dG_{\mu-1}(x,t^*)\,dH_{\mu-1}(x,t^*) \equiv 0 \pmod{p^{\mu}}.$$

In virtue of Lemma 5 there exists an $X \in Q[t]$ such that

$$dG_{\mu-1}\big(X(t),t\big)\,dH_{\mu-1}\big(X(t),t\big) \equiv 0 \pmod{P^{\mu}(t)}$$

and then by (7) $L\big(X(t),t\big) \equiv 0 \pmod{P(t)^{\mu}}$.

There remains only the case where $L(x,\vartheta) = c(x-a)^r$, $a, c \in K$, $c \neq 0$, $r \geqslant 2$.

Let $c = C(\vartheta)$, $a = A(\vartheta)$, where $A, C \in Q[t]$. We have

$$L(x,t) \equiv C(t)\big(x-A(t)\big)^r \pmod{P(t)}, \qquad (P,C) = 1$$

and the congruence $L(x^*,t^*) \equiv 0 \pmod{p}$ for $p \parallel P(t^*)$ implies $x^* \equiv A(t^*) \pmod{p}$. (Note that $C(t^*) \not\equiv 0 \pmod{p}$ by Lemma 3.) Hence $x^* \equiv A(t^*)+P(t^*)y^* \pmod{p^{\mu}}$, $y^* \in Z$ and we have

$$L\big(A(t^*)+P(t^*)y^*, t^*\big) \equiv 0 \pmod{p^{\mu}}. \tag{8}$$

Let $L_1(y,t) = L\big(A(t)+P(t)y,t\big)/P(t)$. We have for a suitable integer $l \neq 0$

$$lL_1(y,t) \in Z[y,t].$$

The congruence (8) together with $p \parallel P(t^*)$ implies that

$$lL_1(y^*,t^*) \equiv 0 \pmod{p^{\mu-1}}.$$

By the inductive assumption there exists a polynomial $Y \in Q[t]$ such that $lL_1\big(Y(t),t\big) \equiv 0 \pmod{P(t)^{\mu-1}}$ and then $L\big(A(t)+P(t)Y(t),t\big) \equiv 0 \pmod{P^{\mu}(t)}$.

Proof of Theorem 1. If $M(t) = 0$ the theorem follows from Theorem 1 of [2].

If $M(t) \neq 0$ let

$$M(t) = m\prod_{i=1}^{k} P_i(t)^{\mu_i}$$

be the canonical factorization of M into polynomials irreducible and primitive. Take an index $i \leqslant k$, a prime p and integer t_1^* such that $p \parallel P_i(t^*)$. The arithmetic progression $p^{\mu_i}u+t^*$ contains an integer t_1^* such that for suitable $x^*, y^* \in Z$ we have $L(x^*,t_1^*) = M(t^*)y^*$. Clearly $L(x^*,t^*) \equiv L(x^*,t_1^*) \equiv 0 \pmod{p^{\mu}}$. Hence by Lemma 6 there exists a polynomial $X_i \in Q[t]$ such that

$$L\big(X_i(t),t\big) \equiv 0 \pmod{P_i^{\mu_i}(t)}.$$

By the Chinese Remainder Theorem there exists a polynomial $X \in Q[t]$ satisfying $X \equiv X_i(t) \pmod{P_i^{\mu_i}(t)}$ $(1 \leqslant i \leqslant k)$. We get $L\big(X(t),t\big) \equiv 0 \pmod{\prod_{i=1}^{k} P_i^{\mu_i}(t)}$, hence

$$L\big(X(t),t\big) = M(t)\,Y(t), \qquad Y(t) \in Q[t].$$

Here is an example showing that Theorem 1 fails for polynomials L of degree 5 in x.

Example 1. Let $L(x,t) = (x^2+3)(x^3+3)$, $M(t) = 3t+1$. For every integer t^* we have $M(t^*) = \prod_{i=1}^{k} p_i^{\alpha_i}\prod_{j=1}^{l} q_j^{\beta_j}$, where p_i are primes $\equiv 1 \pmod 3$, q_j are primes $\equiv 2 \pmod 3$. The congruences $x^2+3 \equiv 0 \pmod{p_i^{\alpha_i}}$ and $x^3+3 \equiv 0 \pmod{q_j^{\beta_j}}$ are solvable for all $i \leqslant k$, $j \leqslant l$. Denoting their solutions by x_i and x_j', respectively, we can satisfy the equation $L(x,t^*) = M(t^*)\,y$ by taking $x \equiv x_i \pmod{p_i^{\alpha_i}}$, $x \equiv x_j' \pmod{q_j^{\beta_j}}$ $(1 \leqslant i \leqslant k, 1 \leqslant j \leqslant l)$. On the other hand, the equation $L\big(X(t),t\big) = M(t)\,Y(t)$ where $X, Y \in Q[t]$ would imply $X(-\frac{1}{3})^2+3 = 0$ or $X(-\frac{1}{3})^3+3 = 0$ hence $\sqrt{-3} \in Q$ or $\sqrt[3]{-3} \in Q$, which is impossible. (The idea comes from van der Waerden [12].)

The next example shows that the conclusion of Theorem 1 cannot be sharpened to assert the existence of integer valued polynomials $X(t)$, $Y(t)$ satisfying $L\big(X(t),t\big) = M(t)\,Y(t)$.

Example 2. Let $L(x,t) = (2x+1)(3x+1)$, $M(t) = 5t+1$. For every integer t^* we have $M(t^*) = 2^{\alpha}N$, N odd. The congruences $2x+1 \equiv 0 \pmod N$, $3x+1 \equiv 0 \pmod{2^{\alpha}}$ are both solvable. Denoting their solutions by x_1 and x_2 respectively we can satisfy the equation $L(x,t^*) = M(t^*)y$ by taking $x \equiv x_1 \pmod N$, $x \equiv x_2 \pmod{2^{\alpha}}$. Suppose now

that $X(t)$, $Y(t)$ are integer valued polynomials satisfying $L(X(t), t) = M(t)Y(t)$. Then clearly

$$(9) \qquad \text{either } 2X(t)+1 = (5t+1)Y_1(t) \quad \text{or } 3X(t)+1 = (5t+1)Y_2(t), \quad Y_1, Y_2 \in Q[t].$$

Let m be a positive integer such that $m_i Y_i \in Z[t]$ ($i = 1$ or 2) and let $2^{\delta_1} \| m_1$, $3^{\delta_2} \| m_2$. Solving the congruence $5t+1 \equiv 0 \pmod{2^{\delta_1+1}}$ if $i = 1$ or $5t+1 \equiv 0 \pmod{3^{\delta_2+1}}$ if $i = 2$, we get from (9) a contradiction (the idea comes from Skolem [10]).

Proof of Theorem 2. By the assumption we have

$$F(x, y, t) = C(t)\big(A(t)x+B(t)y\big)^2+D(t)x+E(t)y+F(0, 0, t)$$

where $A, B, C, D, E \in Z[t]$ and we can assume without loss of generality that $(A, B) = 1$.

Let R be the resultant of A and B and let $G, H \in Z[t]$ be such that

$$A(t)G(t)+B(t)H(t) = R.$$

We set

$$A(t)x+B(t)y = u, \qquad H(t)x+G(t)y = v$$

and obtain

$$RF(x, y, t) = RC(t)u^2+\big(D(t)G(t)+E(t)\big)u+ +\big(A(t)E(t)-B(t)D(t)\big)v+RF(0, 0, t) = 0.$$

Moreover, if $x, y \in Z$ we have $u, v \in Z$. The assumptions of Theorem 1 are satisfied with

$$L(u, t) = RC(t)u^2+\big(D(t)G(t)+E(t)H(t)\big)u+RF(0, 0, t),$$
$$M(t) = A(t)E(t)-B(t)D(t).$$

By the said theorem there exist polynomials $U, V \in Q[t]$ such that identically

$$L\big(U(t), t\big) = M(t)V(t).$$

Setting

$$X(t) = \frac{1}{R}\,[G(t)U(t)-B(t)V(t)],$$

$$Y(t) = \frac{1}{R}\,[H(t)U(t)-A(t)V(t)],$$

we get $X, Y \in Q[t]$ and $F\big(X(t), Y(t), t\big) = 0$.

Proof of Theorem 3. Setting

$$(2t^*+\sqrt{4t^{*2}+1}\,)^{4t^{*2}+1} = x+y(4t^{*2}+1)\sqrt{4t^{*2}+1},$$

we get for every integer t^* integers x, y satisfying

$$x^2-(4t^{*2}+1)^3y^2 = -1.$$

On the other hand, it has been proved already by Abel [1] that all solutions of an equation $U^2(t)-F(t)V^2(t) = \text{const} \neq 0$ are given by convergents of the continued fraction expansion of $\sqrt{F(t)}$. Since for $F(t) = 4t^2+1$

$$F(t) = 2t+\cfrac{1}{\left|4t\right.}+\cfrac{1}{\left|4t\right.}+\cdots,$$

we infer from the equation

$$X(t)^2-(4t^2+1)^3X(t)^2 = -1$$

that

$$X(t)+(4t^2+1)\sqrt{4t^2+1}\,Y(t) = c(2t\pm\sqrt{4t^2+1}\,)^n, \qquad n \geqslant 0.$$

Hence

$$n(2t)^{n-1} \equiv 0 \pmod{4t^2+1},$$

$n = 0$, $X(t) = c$, $Y(t) = 0$ and $c^2 = -1$ contradicting $X \in Q[t]$.

For the proof of Theorem 4 we need four lemmata.

Lemma 7. *Let $M(t) = m\prod_{i=1}^{k} P_i^{\mu_i}(t)$ where polynomials $P_i(t)$ are distinct irreducible and primitive. Under the assumptions of the theorem and the conditions $BM \neq 0$, $(A, M) = 1$ there exist polynomials $X_0, Y_0 \in Q[t]$ such that*

$$A(t)X_0(t)^n+B(t) = M(t)Y_0(t),$$

$$X_0(t) \equiv 0 \Big(\mathrm{mod}\prod_{i=1}^{k} P_i(t)^{-[-\beta_i/n]}\Big), \qquad \text{where} \qquad P_i(t)^{\beta_i} \| B(t).$$

Proof. By the assumption, $P_i \nmid A$ ($1 \leqslant i \leqslant k$). Set $B = P_i^{\beta_i}B_i$, where $P \nmid B$. By the Chinese Remainder Theorem for the ring $Q[t]$ it is sufficient to show the solvability in this ring of each congruence

$$(10) \qquad A(t)X(t)^n+B(t) \equiv 0 \big(\mathrm{mod}\, P_i^{\mu_i}(t)\big) \qquad (1 \leqslant i \leqslant k).$$

Let $P_i(\vartheta) = 0$, $K = Q(\vartheta)$ and let $\mathfrak{p}$ be a prime ideal of degree 1 in K with the norm p sufficiently large. We have $\vartheta \equiv t_0 \pmod{\mathfrak{p}}$ for a suitable $t_0 \in Z$ and $P_i(t_0) \equiv 0 \pmod{p}$. Choosing $t_1 = t_0$ or t_0+p we can achieve that every $t^* \equiv t_1 \pmod{p^2}$ satisfies $p \| P_i(t^*)$. Moreover, since p is sufficiently large we have by Lemma 3 $p \nmid AB_i(t^*)$, whence $p^{\beta_i} \| B(t^*)$. If $\beta_i \geqslant \mu_i$ the congruence (10) has the solution $X = 0$. If $\beta_i < \mu_i$ the equality

$$A(t^*)x^n+B(t^*) = M(t^*)y$$

implies that $\beta_i \equiv 0 \pmod n$, $x \equiv 0 \pmod{p^{\beta_i/n}}$ and

$$\left(x P_i(t^*)^{-\beta_i/n}\right)^n \equiv -B_i(t^*)/A(t^*) \pmod p.$$

However,

$$\frac{B_i(t^*)}{A(t^*)} \equiv \frac{B_i(\vartheta)}{A(\vartheta)} \pmod{\mathfrak{p}}$$

and thus $-B_i(\vartheta)/A(\vartheta)$ is an nth power residue for almost all prime ideals of degree 1 in K. In virtue of Flanders' theorem [3a] $-B_i(\vartheta)/A(\vartheta) = C(\vartheta)^n$, where $C \in Q[t]$ and thus

$$A(t)C(t)^n + B_i(t) \equiv 0 \pmod{P_i(t)}.$$

Hence

$$A(t)x^n + B_i(t) \equiv \left(x - C(t)\right)H(x,t) \pmod{P_i(t)}.$$

Clearly, $H\left(C(t), t\right) \not\equiv 0 \pmod{P_i(t)}$; thus by Lemma 1 applied with $D = Q[t]$ there exists a $C_{\mu_i - 1} \in Q[t]$ such that

$$A(t)C_{\mu_i-1}(t)^n + B_i(t) \equiv 0 \pmod{P_i^{\mu_i}(t)}.$$

Now we can satisfy (10) by taking

$$X(t) = C_{\mu_i-1}(t)P_i^{\beta_i/n}(t).$$

LEMMA 8. *Let under the assumptions of Lemma 7*

$$\Pi(t) = \prod_{i=1}^{k} P_i(t)^{\max\{-[-\mu_i/n],\, \mu_i + (n-1)[-\beta_i/n]\}},$$

$$X(t,v) = X_0(t) + v\Pi(t), \qquad Y(t,v) = \frac{A(t)X(t,v)^n + B(t)}{M(t)}.$$

If $d, e \in Z$, $dX_0 \in Z[t]$, $eY_0 \in Z[t]$ *then* $dX(t,v) \in Z[t,v]$, $[d^n m, e]\,Y(t,v) \in Z[t,v]$.

Proof. The statement concerning $X(t,v)$ is obvious and that concerning $Y(t,v)$ follows from the identity

$$Y(t,v) = Y_0(t) + \sum_{\nu=1}^{n} \binom{n}{\nu} A(t)X_0(t)^{n-\nu}\Pi(t)^\nu M(t)^{-1}v^\nu.$$

Indeed,

$$\operatorname{ord}_{P_i} X_0^{n-1}\Pi \geqslant -(n-1)[-\beta_i/n] + \max\{-[-\mu_i/n], \mu_i + (n-1)[-\beta_i/n]\} \geqslant \mu_i = \operatorname{ord}_{P_i} M,$$

$$\operatorname{ord}_{P_i} \Pi^n \geqslant n\max\{-[-\mu_i/n],\, \mu_i + (n-1)[-\beta_i/n]\} \geqslant \mu_i = \operatorname{ord}_{P_i} M;$$

hence for each $\nu = 1, 2, \ldots, n$

$$X_0(t)^{n-\nu}\Pi(t)^\nu P_i(t)^{-\mu_i} \in Q[t].$$

Since $dX_0 \in Z[t]$ and P_i is primitive we have $d^{n-\nu}X_0(t)^{n-\nu}\Pi(t)^\nu P_i(t)^{-\mu_i} \in Z[t]$,

$$md^{n-\nu}X_0(t)^{n-\nu}\Pi(t)^\nu M(t)^{-1} \in Z[t]. \tag{11}$$

LEMMA 9. *Let* $P \in Z[t]$ *be a primitive polynomial with discriminant* $D \neq 0$, $t^* \in Z$, p *a prime. If* $\operatorname{ord}_p D = d$, $\infty > \operatorname{ord}_p P(t^*) = e > 2d+1$ *then there exists a* $t_0 \equiv t^* \pmod{p^{e-d-1}}$ *such that*

$$\operatorname{ord}_p P(t_0) = \operatorname{ord}_p P(t^*) - 1.$$

Proof. If P is of degree 1 then $P(t^*) \equiv 0 \pmod p$ implies $P'(t^*) \not\equiv 0 \pmod p$, P being primitive. Therefore, it is enough to take $t_0 = t^* + p^{e-1}$.

If P is of degree > 1 then we have for suitable polynomials U, $V \in Z[t]$ $PU + P'V = D$ (see Rédei [7], Satz 275). Hence $e > 2d+1$ implies $\delta = \operatorname{ord}_p P'(t^*) \leqslant d$. Take $t_0 = t^* + p^{e-\delta-1}$. From the Taylor formula we get

$$P(t_0) \equiv P(t^*) + P'(t^*)p^{e-\delta-1} \pmod{p^{2(e-\delta-1)}}.$$

By the assumption $2(e-\delta-1) \geqslant 2(e-d-1) > e-1 = \operatorname{ord}_p P'(t^*)p^{e-\delta-1}$. Hence

$$\operatorname{ord}_p P(t_0) = e-1.$$

Remark. It may be that the lemma holds for $e > d+1$, but the writer could not prove it.

LEMMA 10. *Under the assumptions of Lemmata 7 and 8 for every prime* p *there exist an integer* e *and an integer valued function* $w(\tau)$ *defined on the set* $\{0, 1, \ldots, p^{2e}-1\}$ *such that if* $t^* \in Z$, $v^* \in Q$, $t^* \equiv \tau \pmod{p^{2e}}$, $p^e v^* \equiv w(\tau) \pmod{p^{2e}}$ *then* $X(t^*, v^*)$ *and* $Y(t^*, v^*)$ *are* p*-adic integers.*

Proof. Let nonnegative integers ξ, η be chosen so that $p^\xi X_0$, $p^\eta Y_0$ have integral p-adic coefficients. Let R_{ij} for $i, j = 1, \ldots, k$ be the resultant of P_i and P_j if $i \neq j$ and the discriminant of P_i if $i = j$. Moreover, let R_{i0} be the resultant of P_i and A, R_{ik+1} the resultant of P_i and $B_i = BP_i(t)^{-\beta_i}$ $(1 \leqslant i \leqslant k)$, $B_{k+1} = B\prod_{i=1}^{k} P_i(t)^{-\beta_i}$.

Put $\varrho_{ij} = \operatorname{ord}_p R_{ij}$. Clearly, $\varrho_{ij} = \varrho_{ji} \geqslant \min\left(\operatorname{ord}_p P_i(t^*), \operatorname{ord}_p P_j(t^*)\right)$ for every $t^* \in Z$ and $i \neq j$. Put further

$$c_i = \varrho_{i0} + \sum_{j=1}^{k} (2\beta_j + \mu_j)\varrho_{ij} + 2\varrho_{ik+1} + n\xi + 2\eta + 2\operatorname{ord}_p n + \operatorname{ord}_p m,$$

$$c = \sum_{i=1}^{k} c_i\mu_i + \xi + \operatorname{ord}_p m.$$

For every nonnegative integer $\tau < p^{2c}$ the arithmetic progression $\tau + p^{c-\xi+1}u$ contains an integer t_τ such that for suitable integers x_τ, y_τ we have

$$A(t_\tau)x_\tau^n + B(t_\tau) = M(t_\tau)y_\tau, \qquad M(t_\tau) \neq 0 \tag{12}$$

(integers t_τ, x_τ, y_τ are not determined uniquely, but any choice will do).

If for all $i \leqslant k$ we have $\operatorname{ord}_p P_i(\tau) \leqslant c_i$ then

$$o = \operatorname{ord}_p \Pi(\tau) \leqslant \sum_{i=1}^{k} \mu_i \operatorname{ord}_p P_i(\tau) \leqslant c - \xi.$$

We define

$$w(\tau) = p^{c-o-\xi}w,$$

where w is a root of the congruence

$$w\frac{\Pi(\tau)}{p^o} + p^\xi X_0(\tau) \equiv x_\tau p^\xi \pmod{p^c}.$$

If $t^* \equiv \tau \pmod{p^{2c}}$ and $p^c v^* \equiv w(\tau) \pmod{p^{2c}}$ then we have

$$\operatorname{ord}_p M(\tau) = \operatorname{ord}_p m + \sum_{i=1}^{k} \mu_i \operatorname{ord}_p P_i(t) \leqslant c - \xi,$$

hence

$$\operatorname{ord}_p M(t^*) = \operatorname{ord}_p M(\tau) = \operatorname{ord}_p M(t_\tau),$$

$$X(t^*, v^*) \equiv X_0(\tau) + \frac{w(\tau)}{p^c}\Pi(\tau) \pmod{p^c}.$$

By the definition of $w(\tau)$

$$X(t^*, v^*) = X_0(\tau) + \frac{w}{p^{o+\xi}}\Pi(\tau) = x_\tau \pmod{p^{c-\xi}},$$

$$A(t^*)X(t^*, v^*)^n + B(t^*) \equiv A(t_\tau)x_\tau^n + B(t_\tau) \equiv M(t_\tau)y_\tau \pmod{p^{c-\xi}},$$

hence

$$\operatorname{ord}_p\left(A(t^*)X(t^*, v^*)^n + B(t^*)\right) \geqslant \min\left(c-\xi, \operatorname{ord}_p M(t_\tau)\right) = \operatorname{ord}_p M(t^*).$$

This shows that $X(t^*, v^*)$ and $Y(t^*, v^*)$ are both p-adic integers.

If for a certain $i \leqslant k$ $\operatorname{ord}_p P_i(\tau) > c_i$ then since $c_i \geqslant \varrho_{ij}$ we have for all $j \neq i$ $(1 \leqslant j \leqslant k)$ $\operatorname{ord}_p P_j(\tau) \leqslant \varrho_{ij} < c_j$ thus i is uniquely determined. We have the following possibilities $\beta_i \geqslant \mu_i \equiv 0 \pmod n$, $\beta_i \geqslant \mu_i \not\equiv 0 \pmod n$ and $\beta_i < \mu_i$ which we consider successively.

1. $\beta_i \geqslant \mu_i \equiv 0 \pmod n$. Here we set $\zeta_i = \max\{\xi, \varrho_{i0}\}$,

$$\Pi_i(t) = \Pi(t)P_i^{-\mu_i/n}(t), \qquad X_{0i}(t) = X_0(t)P_i^{-\mu_i/n}(t),$$
$$M_i(t) = M(t)P_i(t)^{-\mu_i}.$$

We have

$$o_i = \operatorname{ord}_p \Pi_i(\tau) \leqslant \sum_{\substack{j=1 \\ j\neq i}}^{k} \mu_j \operatorname{ord}_p P_j(\tau) \leqslant \sum_{j=1}^{k} \mu_j \varrho_{ij} \leqslant c_i - \zeta_i \leqslant c - \zeta_i.$$

Moreover from (11) and $\beta_i \geqslant \mu_i$ we infer that

$$P_i^{\mu_i}(t_\tau) \mid A(t_\tau)x_\tau^n$$

and since

$$\operatorname{ord}_p P_i(t_\tau) \geqslant \min\left(\operatorname{ord}_p P_i(\tau), c-\xi+1\right) > c_i \geqslant \varrho_{i0},$$

we get

$$\operatorname{ord}_p A(t_\tau) \leqslant \varrho_{i0} \leqslant n\zeta_i,$$
$$n(\operatorname{ord}_p x_\tau + \zeta_i) \geqslant \mu_i \operatorname{ord}_p P_i(t_\tau).$$

We define

$$w(\tau) = p^{c-o_i-\zeta_i}w,$$

where w is a root of the congruence

$$\frac{\Pi_i(\tau)}{p^{o_i}}w + p^{\zeta_i}X_{0i}(\tau) \equiv \frac{x_\tau p^{\zeta_i}}{P_i^{\mu_i/n}(t_\tau)} \pmod{p^c}.$$

If $t^* \equiv \tau \pmod{p^{2c}}$, $p^c v^* \equiv w(\tau) \pmod{p^{2c}}$ we have

$$\operatorname{ord}_p M_i(\tau) = \operatorname{ord}_p m + \sum_{\substack{j=1 \\ j\neq i}}^{k} \mu_j \operatorname{ord}_p P_j(\tau) \leqslant c_i - \zeta_i \leqslant \mu_i(c_i - \zeta_i) \leqslant c - \mu_i\zeta_i - \xi,$$

hence $\operatorname{ord}_p M_i(t^*) = \operatorname{ord}_p M_i(\tau) = \operatorname{ord}_p M_i(t_\tau)$.

On the other hand, taking

$$X_i(t^*, v^*) = X_{0i}(t^*) + v^*\Pi_i(t^*),$$

we get

$$X_i(t^*, v^*) \equiv X_{0i}(\tau) + \frac{w(t)}{p^c}\Pi_i(\tau) \pmod{p^c}$$

and by the definition of $w(\tau)$

$$p^{\zeta_i}X_i(t^*, v^*) \equiv p^{\zeta_i}X_{0i}(\tau) + \frac{w}{p^{o_i}}\Pi_i(\tau) \equiv \frac{x_\tau p^{\zeta_i}}{P_i^{\mu_i/n}(t_\tau)} \pmod{p^c}.$$

Since

$$\operatorname{ord}_p P_i^{\mu_i/n}(t^*) \geqslant \min\left(\operatorname{ord}_p P_i(\tau), 2c\right) > c_i \geqslant \zeta_i$$

we infer that $X(t^*, v^*) = X_i(t^*, v^*)P_i^{\mu_i/n}(t^*)$ is a p-adic integer. Moreover

$$p^{n\zeta_i}\big(A(t^*)X_i(t^*, v^*)^n + P_i(t^*)^{\beta_i-\mu_i}B_i(t^*)\big) \equiv \frac{A(t_\tau)p^{n\zeta_i}x_\tau^n}{P_i^{\mu_i}(t_\tau)} + p^{n\zeta_i}P_i(t^*)^{\beta_i-\mu_i}B_i(t_\tau) \pmod{p^{c-\xi}}.$$

By (12) the right-hand side equals $p^{n\zeta_i}M_i(t_\tau)y$, hence

$$\operatorname{ord}_p\big(A(t^*)X_i(t^*, v^*)^n + P_i(t^*)^{\beta_i-\mu_i}B_i(t^*)\big) \geqslant \min\big(c-\xi-n\zeta_i, \operatorname{ord}_p M_i(t_\tau)\big) = \operatorname{ord}_p M_i(t^*)$$

and

$$\operatorname{ord}_p\big(A(t^*)X(t^*, v^*)^n + B(t^*)\big) \geqslant \mu_i\operatorname{ord}_p P_i(t^*) + \operatorname{ord}_p M_i(t^*) = \operatorname{ord}_p M(t^*).$$

Thus $Y(t^*, v^*)$ is a p-adic integer.

2. $\beta_i \geqslant \mu_i \not\equiv 0 \pmod n$. Here we set $w(\tau) = 0$.

If $\beta_i > \mu_i$ we have

$$X_0(t) \equiv 0 \big(\bmod P_i(t)^{-[-\beta_i/n]}\big), \qquad A(t)X_0(t)^n + B(t) \equiv 0 \big(\bmod P_i(t)^{\mu_i+1}\big),$$

hence $Y_0(t) \equiv 0 \big(\bmod P_i(t)\big)$. Moreover, since $P_i(t)$ is primitive, we have

$$p^\xi X_0(t)P_i(t)^{-1} \in Z_p[t], \qquad p^\eta Y_0(t)P_i(t)^{-1} \in Z_p[t], \tag{13}$$

where Z_p is the ring of p-adic integers.

If $t^* \equiv \tau \pmod{p^{2c}}$, $p^c v^* \equiv w(\tau) \pmod{p^{2c}}$ we have $v^* \equiv 0 \pmod{p^c}$,

$$X(t^*, v^*) \equiv X_0(t^*) \pmod{p^c},$$

$$Y(t^*, v^*) = Y_0(t^*) + \sum_{\nu=1}^{n}\binom{n}{\nu}\frac{A(t^*)X_0(t^*)^{n-\nu}\Pi(t^*)^\nu}{M(t^*)}v^{*\nu}.$$

Since $\operatorname{ord}P_i(t^*) > c_i \geqslant \max\{\xi, \eta\}$ we infer from (13) that

$$X_0(t^*),\ Y_0(t^*) \in Z_p.$$

On the other hand, by (12)

$$mp^{\xi(n-\nu)}\frac{X_0(t)^{n-\nu}\Pi(t)^\nu}{M(t)} \in Z_p[t] \qquad (\nu = 1, 2, \ldots, n).$$

Since $\operatorname{ord}_p v^\nu \geqslant c \geqslant \xi(n-1) + \operatorname{ord}_p m$ we conclude that $X(t^*, v^*)$, $Y(t^*, v^*)$ are p-adic integers.

If $\beta_i = \mu_i$ we have as before $X_0(t) \equiv 0 \big(\bmod P_i(t)\big)$. If $t^* \equiv \tau \pmod{p^{2c}}$, $p^c v^* \equiv w(\tau) \equiv 0 \pmod{p^{2c}}$, then $X(t^*, v^*) \equiv X_0(t^*) \pmod{p^c}$ is again a p-adic integer and $Y(t^*, v^*) \in Z_p$ if and only if $Y_0(t^*) \in Z_p$.

The latter condition is satisfied for all $t^* \equiv \tau \pmod{p^{2c}}$ if it is satisfied

for one such t^*. Since we cannot have $P_i(t^*) = 0$ for all $t^* \equiv \tau \pmod{p^{2c}}$ we may assume that $P_i(t^*) \neq 0$. If $\eta = 0$, $Y_0(t^*) \in Z_p$. If $\eta > 0$ we have $\operatorname{ord}_p P_i(t^*) > c_i \geqslant 2\varrho_{ii}+1$, hence by Lemma 9 there exists a $t_0 \equiv t^* \pmod{p^{c_i-\varrho_{ii}}}$ such that $\operatorname{ord}P_i(t_0) = \operatorname{ord}P_i(t^*) - 1$. On the other hand

$$\operatorname{ord}_p A(t^*) \leqslant \varrho_{i0} < c_i - \varrho_{ii},$$

$$\operatorname{ord}_p B_i(t^*) \leqslant \sum_{\substack{j=1\\ j\neq i}}^{k}\beta_j\varrho_{ij} + \varrho_{ik+1} < c_i - \varrho_{ii},$$

$$\operatorname{ord}_p M_i(t^*) \leqslant \operatorname{ord}_p m + \sum_{\substack{j=1\\ j\neq i}}^{k}\mu_j\varrho_{ij} < c_i - \varrho_{ii} - n\xi,$$

hence

$$\operatorname{ord}_p A(t_0) = \operatorname{ord}_p A(t^*) < \infty, \qquad \operatorname{ord}_p B_i(t_0) = \operatorname{ord}_p B_i(t^*) < \infty,$$

$$\operatorname{ord}_p M_i(t_0) = \operatorname{ord}_p M_i(t^*) < \infty.$$

Since $\mu_i \not\equiv 0 \pmod n$ we cannot have simultaneously

$$\mu_i\operatorname{ord}_p P_i(t^*) + \operatorname{ord}_p B_i(t^*) \equiv \operatorname{ord}_p A(t^*) \pmod n$$

and

$$\mu_i\operatorname{ord}_p P_i(t_0) + \operatorname{ord}_p B_i(t_0) \equiv \operatorname{ord}_p A(t_0) \pmod n$$

thus taking $t_1 = t^*$ or t_0 we can achieve that

$$\operatorname{ord}_p B(t_1) = \mu_i\operatorname{ord}_p P_i(t_1) + \operatorname{ord}_p B_i(t_1) \not\equiv \operatorname{ord}_p A(t_1) \pmod n,$$

$$\infty > \operatorname{ord}_p P_i(t_1) \geqslant c_i - \varrho_{ii},$$

$$a = \max\{\operatorname{ord}_p A(t_1), \operatorname{ord}_p B(t_1), \operatorname{ord}_p M(t_1)\} < \infty.$$

The arithmetic progression $t_1 + p^{a+1}u$ contains an integer t_2 such that for suitable integers x_2, y_2 we have

$$A(t_2)x_2^n + B(t_2) = M(t_2)y_2.$$

Since

$$\operatorname{ord}_p A(t_2) = \operatorname{ord}_p A(t_1), \qquad \operatorname{ord}_p P_i(t_2) = \operatorname{ord}_p P_i(t_1),$$
$$\operatorname{ord}_p B(t_2) = \operatorname{ord}_p B(t_1), \qquad \operatorname{ord}_p M(t_2) = \operatorname{ord}_p M(t_1),$$

we have

$$\operatorname{ord}_p A(t_2)x_2^n \equiv \operatorname{ord}_p A(t_2) \not\equiv \operatorname{ord}_p B(t_2) \pmod n.$$

It follows that

$$\operatorname{ord}_p B(t_2) \geqslant \operatorname{ord}_p M(t_2)y_2 \geqslant \operatorname{ord}_p M(t_2) \quad \text{and} \quad \operatorname{ord}_p B(t_1) \geqslant \operatorname{ord}_p M(t_1).$$

On the other hand we have $\operatorname{ord}_p P_i(t_1) \geqslant c_i - \varrho_{ii} > \varrho_{ij}$ for all $j \leqslant k+1$,

hence

$$\operatorname{ord}_p P_j(t_1) \leqslant \varrho_{ij}\ (j \neq i), \qquad \operatorname{ord}_p M_i(t_1) \leqslant \operatorname{ord}_p m + \sum_{\substack{j=1\\ j\neq i}}^{k} \varrho_{ij}\mu_j \leqslant c_i - n\xi - \varrho_{it};$$

$$\begin{aligned}\operatorname{ord}_p A(t_1)X_0(t_1)^n &\geqslant -n[-\beta_i/n]\operatorname{ord}_p P_i(t_1) - n\xi\\ &\geqslant (\mu_i+1)\operatorname{ord}_p P_i(t_1) - n\xi \geqslant \mu_i \operatorname{ord}_p P_i(t_1) + c_i - n\xi - \varrho_{it}\\ &\geqslant \mu_i \operatorname{ord}_p P_i(t_1) + \operatorname{ord}_p M_i(t_1) = \operatorname{ord}_p M(t_1).\end{aligned}$$

Since $A(t_1)X_0(t_1)^n + B(t_1) = M(t_1)Y_0(t_1)$ we get $\operatorname{ord}_p Y_0(t_1) \geqslant 0$. However $p^\eta Y_0(t_1) \equiv p^\eta Y_0(t^*) \pmod{p^{c_i-\varrho_{it}}}$. Since $c_i - \varrho_{it} \geqslant \eta$, $Y_0(t^*)$ is a p-adic integer and so is $Y(t^*, v^*)$.

3. $\beta_i < \mu_i$. Here we have $\beta_i \equiv 0 \pmod n$,

$$P_i(t)^{\beta_i/n} \| X_0(t), \qquad P_i(t)^{\mu_i - \frac{n-1}{n}\beta_i} \| \Pi(t).$$

Let

$$X_{0i}(t) = X_0(t)P_i(t)^{-\beta_i/n}, \qquad \Pi_i(t) = \Pi(t)P_i(t)^{\frac{n-1}{n}\beta_i - \mu_i},$$
$$M_i(t) = M(t)P_i(t)^{-\mu_i}.$$

We have

$$A(t)X_{0i}(t)^n + B_i(t) = P_i^{\mu_i-\beta_i}(t)M_i(t)Y_0(t)$$

and

$$\operatorname{ord}_p P_i(\tau) > c_i \geqslant \sum_{j=1}^{k} \beta_j \varrho_{ij} + \varrho_{ik+1} + \eta \geqslant \operatorname{ord}_p B_i(\tau) + \eta,$$

hence

$$\operatorname{ord}_p P_i^{\mu_i-\beta_i}(\tau)M_i(\tau)Y_0(\tau) > \operatorname{ord}_p B_i(\tau)$$

and

$$\operatorname{ord}_p A(\tau)X_{0i}(\tau)^n = \operatorname{ord}_p B_i(\tau).$$

We get

$$\operatorname{ord}_p X_{0i}(\tau) \leqslant \frac{1}{n}\operatorname{ord}_p B_i(\tau) \leqslant \frac{1}{n}\Big(\sum_{j=1}^{k}\beta_j\varrho_{ij} + \varrho_{ik+1}\Big)$$

and

$$(14)\qquad o_i = \operatorname{ord}_p \frac{nX_{0i}(\tau)^{n-1}\Pi_i(\tau)}{M_i(\tau)}$$
$$\leqslant \operatorname{ord}_p n + \sum_{j=1}^{k}\beta_j\varrho_{ij} + \varrho_{ik+1} - \operatorname{ord}_p m \leqslant c_i - \eta \leqslant c - \eta.$$

We define

$$w(\tau) = p^{c-o_i-\eta}w,$$

where w is a root of the congruence

$$\frac{nX_{0i}(\tau)^{n-1}\Pi_i(\tau)}{M_i(\tau)p^{o_i}}\,w + p^\eta Y_0(\tau) \equiv 0 \pmod{p^\eta}.$$

If $t^* \equiv \tau \pmod{p^{2c}}$ and $p^c v^* \equiv w(\tau) \pmod{p^{2c}}$ we have

$$\operatorname{ord}_p P_i(t^*) > c_i \geqslant \sum_{j=1}^{k}\beta_j\varrho_{ij} + \varrho_{ik+1} + \eta.$$

If $P_i(t^*) \neq 0$ then

$$(15)\qquad \operatorname{ord}_p B(t^*) \leqslant \beta_i \operatorname{ord}_p P_i(t^*) + \sum_{j=1}^{k}\beta_j\varrho_{ij} + \varrho_{ik+1} < \mu_i \operatorname{ord}_p P_i(t^*) - \eta$$
$$\leqslant \operatorname{ord}_p M(t^*) \leqslant \operatorname{ord}_p M(t^*)Y_0(t^*).$$

Therefore,

$$(16)\qquad \operatorname{ord}_p B(t^*) = \operatorname{ord}_p A(t^*)X_0(t^*)^n.$$

Moreover, $A(t^*)B(t^*)M(t^*) \neq 0$.

Let $b = \max\{\operatorname{ord}_p A(t^*), \operatorname{ord}_p B(t^*), \operatorname{ord}_p M(t^*)\}$ and let t_0 be an integer in the arithmetic progression $t^* + p^{b+1}u$ such that for suitable $x_0, y_0 \in Z$

$$A(t_0)x_0^n + B(t_0) = M(t_0)y_0.$$

We have $\operatorname{ord}_p A(t_0) = \operatorname{ord}_p A(t^*)$, $\operatorname{ord}_p B(t_0) = \operatorname{ord}_p B(t^*)$, $\operatorname{ord}_p M(t_0) = \operatorname{ord}_p M(t^*)$ and by (15) $\operatorname{ord}_p B(t_0) < \operatorname{ord}_p M(t_0) \leqslant \operatorname{ord}_p M(t_0)y_0$. Hence

$$\operatorname{ord}_p B(t_0) = \operatorname{ord}_p A(t_0)x_0^n$$

and by (16)

$$(17)\qquad \operatorname{ord}_p X_0(t^*) = \operatorname{ord}_p x_0 \geqslant 0.$$

If $P_i(t^*) = 0$ there exists a $t' \equiv t^* \pmod{p^{2c}}$ such that $P_i(t') \neq 0$. Since

$$X_0(t^*) \equiv X_0(t') \pmod{p^{2c-\xi}}$$

we have (17) in every case. On the other hand

$$\operatorname{ord}_p v^*\Pi(t^*) \geqslant \min\Big\{c, \operatorname{ord}_p \frac{w(\tau)}{p^c}\Pi(\tau)\Big\}$$
$$\geqslant \min\{c, \operatorname{ord}_p\Pi(\tau) - o_i - \eta\} \geqslant \min\{c, c_i - o_i - \eta\} \geqslant 0,$$

hence

$$\operatorname{ord}_p X(t^*, v^*) \geqslant 0.$$

It remains to prove that $Y(t^*, v^*)$ is a p-adic integer. We have

$$Y(t^*, v^*) = Y_0(t^*) + \frac{nX_{0i}(t^*)^{n-1}\Pi_i(t^*)}{M_i(t^*)}\, v^* + \sum_{\nu=2}^{n}\binom{n}{\nu}\frac{X_{0i}(t^*)^{n-\nu}\Pi_i(t^*)^\nu}{M_i(t^*)}\, P_i(t^*)^{(\nu-1)(\mu_i-\beta_i)} v^{*\nu}.$$

Now

$$p^\eta Y_0(t^*) \equiv p^\eta Y_0(\tau) \pmod{p^{2c}},$$

$$p^{(n-1)\xi} X_{0i}(t^*)^{n-1}\Pi_i(t^*) \equiv p^{(n-1)\xi} X_{0i}(\tau)^{n-1}\Pi_i(\tau) \pmod{p^{2c}},$$

$$M_i(t^*) \equiv M_i(\tau) \pmod{p^{2c}},$$

(18)

$$\operatorname{ord}_p M_i(\tau) \leqslant \sum_{j=1}^{k} \mu_j \varrho_{ij} + \operatorname{ord}_p m < c_i - n\xi + \operatorname{ord}_p m < 2c.$$

Hence

$$p^\eta \frac{nX_{0i}(t^*)^{n-1}\Pi_i(t^*)}{M_i(t^*)}\, v^* \equiv p^\eta \frac{nX_{0i}(\tau)^{n-1}\Pi_i(\tau)}{M_i(\tau)}\frac{w(\tau)}{p^c} \bmod p^{c-(n-1)\xi+\eta-\operatorname{ord}_p M_i(\tau)}$$

and since $c \geqslant c_i + \operatorname{ord}_p m$ we have by the definition of $w(\tau)$

$$p^\eta Y_0(t^*) + p^\eta \frac{nX_{0i}(t^*)^{n-1}\Pi_i(t^*)}{M_i(t)^*}\, v^* \equiv p^\eta Y_0(\tau) + \frac{nX_{0i}(\tau)^{n-1}\Pi_i(\tau)}{M_i(\tau)p^{c_i}} w \equiv 0 \pmod{p^\eta}.$$

Thus

$$Y_0(t^*) + \frac{nX_{0i}(t^*)^{n-1}\Pi_i(t^*)}{M_i(t^*)}\, v^*$$

is a p-adic integer.

Now take $\nu \geqslant 2$ and consider the term

$$E_\nu(t^*, v^*) = \binom{n}{\nu}\frac{X_{0i}(t^*)^{n-\nu}\Pi_i(t^*)^\nu}{M_i(t^*)}\, P_i(t^*)^{(\nu-1)(\mu_i-\beta_i)} v^{*\nu}.$$

We have by (18)

$$\operatorname{ord}_p \frac{X_{0i}(t^*)^{n-\nu}\Pi_i(t^*)^\nu}{M_i(t^*)} \geqslant -(n-\nu)\xi - \sum_{j=1}^{k}\mu_j\varrho_{ij} - \operatorname{ord}_p m,$$

while by the congruence $p^c v^* \equiv w(\tau) \pmod{p^{2c}}$, by the definition of $w(\tau)$ and by (14)

$$\operatorname{ord}_p v^* \geqslant -c_i - \eta \geqslant -\operatorname{ord}_p n - \sum_{j=1}^{k}\beta_j\varrho_{ij} - \varrho_{ik+1} + \operatorname{ord}_p m - \eta,$$

finally

$$\operatorname{ord}_p P_i(t^*)^{\mu_i-\beta_i} > c_i \geqslant \sum_{j=1}^{k}(2\beta_j+\mu_j)\varrho_{ij} + 2\varrho_{ik+1} + n\xi + 2\eta + 2\operatorname{ord}_p n.$$

Hence

$$\begin{aligned}\operatorname{ord}_p E_\nu(t^*, v^*) > {} & -(n-\nu)\xi - \sum_{j=1}^{k}\mu_j\varrho_{ij} - \operatorname{ord}_p m - \nu\operatorname{ord}_p n - \nu\sum_{j=1}^{k}\beta_j\varrho_{ij} - \\ & - \nu\varrho_{ik+1} + \nu\operatorname{ord}_p m - \nu\eta + (\nu-1)\sum_{j=1}^{k}(2\beta_j+\mu_j)\varrho_{ij} + \\ & + 2(\nu-1)\varrho_{ik+1} + (\nu-1)n\xi + 2(\nu-1)\eta + 2(\nu-1)\operatorname{ord}_p n \\ = {} & n(\nu-2)\xi + \nu\xi + (\nu-2)\sum_{j=1}^{k}(\beta_j+\mu_j)\varrho_{ij} + (\nu-1)\operatorname{ord}_p m + \\ & + (\nu-2)\operatorname{ord}_p n + (\nu-2)\varrho_{ik+1} + (\nu-2)\eta + (\nu-2)\operatorname{ord}_p n \geqslant 0.\end{aligned}$$

Thus $E_\nu(t^*, v^*)$ is a p-adic integer and so is $Y(t^*, v^*)$.

Proof of Theorem 4. Suppose first that $BM \neq 0$, $(A, M) = 1$. Let X_0, Y_0 have the meaning of Lemma 7 and let d be chosen so that $dX_0 \in Z[t]$, $dY_0 \in Z[t]$. Let further $X(t, v)$, $Y(t, v)$ have the meaning of Lemma 8.

In virtue of Lemma 10 for every prime $p \mid dm$ there exists an integer c_p and an integer valued function $w_p(\tau)$ defined on the set $\{0, 1, \ldots, p^{c_p} - 1\}$ such that for all $t^* \in Z$, $v^* \in Q$ the congruences $t^* \equiv \tau \pmod{p^{2c_p}}$, $p^c v^* \equiv w_p(\tau) \pmod{p^{2c_p}}$ imply that $X(t^*, v^*)$ and $Y(t^*, v^*)$ are p-adic integers. By a result of Skolem [8] there exists an integer valued polynomial $W_p(t)$ such that $t^* \equiv \tau \pmod{p^{2c_p}}$ implies $W_p(t^*) \equiv w_p(\tau) \pmod{p^{2c_p}}$. Now take

$$V(t) = \sum_{p \mid dm} \frac{W_p(t)}{p^{c_p}} \prod_{\substack{q \mid dm \\ q \neq p}} q^{\varphi(p^{2c_p})\varrho_q}$$

where p, q run over primes and set

$$X(t) = X\big(t, V(t)\big), \qquad Y(t) = Y\big(t, V(t)\big).$$

We assert that $X(t)$, $Y(t)$ are integer valued polynomials. Indeed, by Lemma 8,

$$dX(t, v) \in Z[t, v], \qquad d^n m Y(t, v) \in Z[t, v].$$

Moreover, since

$$V(t)\prod_{p\mid dm} p^{c_p} \in Z[t]$$

and $X(t, v)$, $Y(t, v)$ are in v of degrees 1 and n respectively, we have

$$X(t)d\prod_{p\mid dm} p^{c_p} \in Z[t], \qquad Y(t)d^n m\prod_{p\mid dm} p^{nc_p} \in Z[t].$$

Thus for $t^* \in Z$ the values $X(t^*)$ and $Y(t^*)$ are p-adic integers for each $p \nmid dm$. On the other hand if $p \mid dm$ and $t^* \equiv \tau \pmod{p^{2c_p}}$, $0 \leqslant \tau < p^{2c_p}$ we have

$$p^{c_p} V(t^*) \equiv p^{c_p} \sum_{\substack{q_1^{c_{q_1}} \mid dm \\ q_1 \neq p}} \frac{W_{q_1}(t^*)}{q_1^{c_{q_1}}} \prod_{\substack{q_2^{c_{q_2}} \mid dm \\ q_2 \neq q_1}} q_2^{\varphi(q_1^{2c_{q_1}})c_{q_2}} + W_p(t^*) \prod_{\substack{q^{c_q} \mid dm \\ q \neq p}} q^{\varphi(q^{2c_q})c_q}$$

$$\equiv W_p(t^*) \equiv W_p(\tau) \pmod{p^{2c_p}},$$

hence by the property of the polynomials $X(t, v)$, $Y(t, v)$ stated above

$$X(t^*) = X\big(t^*, V(t^*)\big), \qquad Y(t^*) = Y\big(t^*, V(t^*)\big)$$

are p-adic integers.

Suppose now that $BM \neq 0$ and $(A, M) \neq 1$. Then there exists a primitive polynomial $D \in Z[t]$ such that $A = DA_1$, $M = DM_1$, $A_1, M_1 \in Z[t]$ and $(A_1, M_1) = 1$. Every arithmetic progression contains an integer t^* such that $A(t^*)x^n + B(t^*) = M(t^*)y$ is solvable in integers x, y hence $D(t^*) \mid B(t^*)$. It follows that $D \mid B$ and since D is primitive $B = DB_1$, where $B_1 \in Z[t]$. Every arithmetic progression P contains a progression P_1 such that $D(t^*) \neq 0$ for $t \in P_1$. Therefore, for $t^* \in P_1$

$$A(t^*)x^n + B(t^*) = M(t^*)y \quad \text{implies} \quad A_1(t^*)x^n + B_1(t^*) = M_1(t^*)y$$

and from the already proved case of the theorem we infer the existence of integer valued polynomials X, Y such that $A_1(t)X(t)^n + B_1(t) = M_1(t)Y(t)$. Clearly, $A(t)X(t)^n + B(t) = M(t)Y(t)$. It remains to consider the case $BM = 0$. If $B = 0$ we can take $X = Y = 0$. If $B \neq 0$ and $M = 0$ Theorem 1 of [2] implies the existence of a polynomial $X \in Q[t]$ such that $A(t)X(t)^n + B(t) = 0$. By the assumption every arithmetic progression contains an integer t^* such that either $B(t^*) = 0$ or $X(t^*)^n$ is an integer. Since $B \neq 0$, the former term of the alternative can be omitted. Let a positive integer d be chosen so that $dX \in Z[t]$ and let τ be an arbitrary integer. The arithmetic progression $\tau + du$ contains an integer t^* such that $X(t^*)$ is an integer. We have $dX(\tau) \equiv dX(t^*) \pmod{d}$, hence $d \mid dX(\tau)$ and $X(\tau)$ is an integer. Thus X is an integer-valued polynomial and the proof is complete. Now we shall show by an example

that the condition $n \not\equiv 0 \pmod 8$ cannot be omitted from the assumptions of Theorem 4.

Example 3. Take $n = 8$, $A(t) = 1$, $B(t) = -16$, $M(t) = 2t+1$. For every integer t^* we have $M(t^*) = \pm\prod_{i=1}^{k} p_i^{\alpha_i}$, where p_i are odd primes. For every $i \leqslant k$ the congruence

$$x^8 \equiv 16 \pmod{p_i^{\alpha_i}}$$

is solvable (cf. Trost [11]). Denoting a solution of this congruence by x_i and using the Chinese Remainder Theorem we find $x \equiv x_i \pmod{p_i^{\alpha_i}}$ $(1 \leqslant i \leqslant k)$, which satisfies $x^8 - 16 \equiv 0 \pmod{2t^*+1}$. On the other hand, the existence of polynomials $X, Y \in Q[t]$ satisfying $X(t)^8 - 16 = (2t+1)Y(t)$ would imply $X(-\frac{1}{2})^8 = 16$, $X(-\frac{1}{2})^2 = 2$, a contradiction.

The next example shows that in Theorem 4 polynomials in one variable cannot be replaced by polynomials in two variables even if $A = 1$ and M is irreducible.

Example 4. Take $n = 2$, $A(t, u) = B(t, u) = 1$, $M(t, u) = u^2 + (4t^2+1)^2$. For every pair of integers t^*, u^* the congruence $x^2 + 1 \equiv 0 \pmod{P(t^*, u^*)}$ is solvable. Indeed, we have $M(t^*, u^*) = 2^a \prod p_i^{\alpha_i}$, where $a = 0$ or 1 and $p_i \equiv 1 \pmod 4$. On the other hand suppose that polynomials $X, Y \in Q[t, u]$ satisfy

$$X(t, u)^2 + 1 = M(t, u)Y(t, u).$$

We get $u^2X(t, u)^2 \equiv (4t^2+1)^2 \pmod{M(t, u)}$ and since M is irreducible

$$uX(t, u) \equiv \pm(4t^2+1) \pmod{M(t, u)}.$$

The substitution $u = 0$ gives

$$4t^2 + 1 \equiv 0 \pmod{(4t^2+1)^2},$$

a contradiction.

References

[1] N. H. Abel, *Über die Integration der Differential Formel $\varrho dx/\sqrt{R}$ wenn R und ϱ ganze Functionen sind*, J. Reine Angew. Math. 1 (1826), pp. 185–221, French translation in *Oeuvres choisies*, Christiania 1881, T. I. pp. 104–144.

[2] H. Davenport, D. J. Lewis, and A. Schinzel, *Polynomials of certain special types*, Acta Arith. 9 (1964), pp. 107–116.

[3] — — — *Quadratic Diophantine equations with a parameter*, ibid. 11 (1966), pp. 353–358.

[3a] H. Flanders, *Generalization of a theorem of Ankeny and Rogers*, Ann. of Math. (2) 57(1953), pp. 392–400.

[4] M. Fujiwara, *Hasse principle in algebraic equations*, Acta Arith. 22 (1973), pp. 267–276.

[5] H. Hasse, *Zwei Bemerkungen zu der Arbeit „Zur Arithmetik der Polynome" von U. Wegner in den Math. Ann. 105,S. 628–631*, Math. Ann. 106 (1932), pp. 455–456.
[6] – *Zahlentheorie*, Berlin 1969.
[7] L. Rédei, *Algebra I*, Leipzig 1959.
[8] T. Skolem, *Über die Lösbarkeit gewisser linearer Gleichungen in Bereiche der ganzwertigen Polynome*, Kong. Norsle. Vid. Selsk. Forh. 9 (1937), no 34.
[9] – *Einige Sätze über Polynome*, Avh. Norske Vid. Akad. Oslo I 1940, no 4.
[10] – *Unlösbarkeit von Gleichungen, deren entsprechende Kongruenz für jeden Modul lösbar ist*, ibid. 1942, no 4.
[11] E. Trost, *Zur Theorie von Potenzresten*, Nieuw Arch. Wisk. 18 (1934), pp. 58–61.
[12] B. L. van der Waerden, *Noch eine Bemerkung zu der Arbeit „Zur Arithmetik der Polynome" von U. Wegner in Math. Ann. 105, S. 628–631*, Math. Ann. 109 (1934), pp. 679–680.

Received on 18.1.1980 (1194)

ACTA ARITHMETICA
XL (1982)

Conspectus materiae tomorum XXXI–XL (1976–1982)