[4] L. Carlitz, *Generalized Dedekind sums*, Math. Zeitschr. 85 (1964), pp. 83–90.
[5] — *A theorem on generalized Dedekind sums*, Acta Arith. 11 (1965), pp. 253–260.
[6] — *A three-term relation for Dedekind–Rademacher sums*, Publ. Math., Debrecen, 14 (1967), pp. 119–124.
[7] — *The reciprocity theorem for Dedekind–Rademacher sums*, Acta Arith. 29 (1976), pp. 309–313.
[8] L. J. Mordell, *Lattice points in a tetrahedron and generalized Dedekind sums*, J. Indian Math. Soc. 15 (1951), pp. 41–46.
[9] H. Rademacher, *Generalization of the reciprocity formula for Dedekind sums*, Duke Math. J. 21 (1954), pp. 391–398.
[10] — *Some remarks on certain generalized Dedekind sums*, Acta Arith. 9 (1964), pp. 97–105.
[11] H. Rademacher and E. Grosswald, *Dedekind sums*, The Mathematical Association of America, Washington, D. C., 1972.

Received on 17. 6. 1977 (953)

ACTA ARITHMETICA
XXXVII (1980)

Quadratic diophantine equations with parameters

by

D. J. Lewis* (Ann Arbor, Mich.) and A. Schinzel* (Warszawa)

To the memory of Paul Turán

1. In an earlier paper [3] written in collaboration with the late Harold Davenport we proved:

Theorem A. *Let $a(t)$, $b(t)$ be polynomials with integral coefficients. Suppose that every arithmetical progression contains an integer τ such that the equation $a(\tau)x^2+b(\tau)y^2 = z^2$ has a solution in integers x, y, z, not all 0. Then there exist polynomials $x(t)$, $y(t)$, $z(t)$ in $Z[t]$, not all identically 0, such that $a(t)x(t)^2+b(t)y(t)^2 \equiv z(t)^2$ identically in t.*

From this result we derived:

Theorem B. *Let $F(x, y, t)$ be a polynomial with integral coefficients which is of degree at most 2 in x and y. Suppose that every arithmetical progression contains an integer τ such that the equation $F(x, y, \tau) = 0$ is soluble in rational numbers for x and y. Then there exist rational functions $x(t)$, $y(t)$ in $Q(t)$ such that $F(x(t), y(t), t) \equiv 0$ identically in t.*

Earlier, one of us asked [6] whether a result similar to Theorem B holds if $F(x, y, t)$ is replaced by *any* polynomial $F(x, y, t_1, \ldots, t_r)$ and the stronger assumption is made that for all integral r-tuples $\tau_1, \ldots, \tau_r$, the equation $F(x, y, \tau_1, \ldots, \tau_r) = 0$ is soluble in the rational numbers for x and y. The stronger assumption is needed since the hypothesis analogous to the one of Theorem B involving arithmetical progressions is not sufficient already for $F(x, y, t) = x^2-y^3-t$. We shall show here that if F is of degree at most 2 in x and y a hypothesis analogous to the one of Theorem B suffices for any number of parameters t_i. We shall also indicate an equation of an elliptic curve over $Q(t)$ for which the stronger assumption involving all integers t does not seem to suffice.

* This paper was written while the authors were partially supported by an NSF grant.

As for allowing more variables, we note that in virtue of Gauss's theorem, for every integer τ, the equation

$$x^2+y^2+z^2 = 28\tau^2+1$$

is soluble in integers x, y, z, but there do not exist rational functions $x(t), y(t), z(t)$ in $\boldsymbol{Q}(t)$ such that

$$x(t)^2+y(t)^2+z(t)^2 \equiv 28t^2+1$$

identically in t, since 28 is not the sum of three rational squares. A. Pfister has shown us a more refined example of the equation

$$x^2+y^2+z^2 = 5t^2+13$$

which for all rational values of t is soluble with x, y, z in $\boldsymbol{Q}$, without being soluble with x, y, z in $\boldsymbol{Q}(t)$.

We now turn to the crucial lemma from which the generalization of Theorems A and B in the case of several parameters will be deduced in § 3.

2. LEMMA. *Let $a(t_1, \ldots, t_r)$, $b(t_1, \ldots, t_r)$, $c(t_1, \ldots, t_r) \not\equiv 0$ be polynomials with integral coefficients. Suppose that for all r-tuples of integers $\tau_1, \ldots, \tau_r$ such that $c(\tau_1, \ldots, \tau_r) \neq 0$ the equation*

$$(1)\qquad a(\tau_1, \ldots, \tau_r)x^2+b(\tau_1, \ldots, \tau_r)y^2 = z^2$$

has a solution in integers x, y, z, not all 0. Then there exist polynomials $x(t_1, \ldots, t_r)$, $y(t_1, \ldots, t_r)$, $z(t_1, \ldots, t_r)$ with integral coefficients, not all identically 0, such that

$$(2)\qquad a(t_1, \ldots, t_r)x(t_1, \ldots, t_r)^2+b(t_1, \ldots, t_r)y(t_1, \ldots, t_r)^2 \equiv z(t_1, \ldots, t_r)^2$$

identically in $t_1, \ldots, t_r$.

Proof. The proof is by induction on r. For $r = 1$ the result follows from Theorem A since clearly every arithmetic progression contains an integer τ for which $c(\tau) \neq 0$. Alternatively, with the stronger hypothesis of our lemma one can give a simpler direct proof for the case $r = 1$ following the arguments of Theorem A.

Suppose the lemma is true for fewer than r parameters. We can obviously suppose that neither $a(t_1, \ldots, t_r)$ nor $b(t_1, \ldots, t_r)$ is identically 0, since otherwise the conclusion follows trivially. Denote the degree of a polynomial q in t_r by $|q|$. We now proceed by induction on the degree of ab with respect to t_r. If $|a|+|b| = 0$, the hypothesis of the lemma holds for $c'(t_1, \ldots, t_{r-1}) = c(t_1, \ldots, t_{r-1}, \tau)$, where τ is an integer so chosen that $c' \not\equiv 0$; and, hence, the lemma is true from our induction assumption. Suppose the result holds for all a, b, c satisfying $|a|+|b| < n$ and $c \neq 0$ where n is some positive integer; we have to prove the result for polynomials a, b, c when $|a|+|b| = n$ and $c \neq 0$. We can suppose, without loss of generality, that $|a| \geqslant |b|$, and, so, in particular $|a| > 0$.

Suppose first that $a(t_1, \ldots, t_r)$ is not square free as a polynomial in t_r, say

$$a(t_1, \ldots, t_r) = k(t_1, \ldots, t_r)^2 a_1(t_1, \ldots, t_r),$$

where k has integral coefficients and $|k| \geqslant 1$. The hypothesis of the lemma regarding a, b, c insures that this hypothesis also holds for the polynomials

$$a_1(t_1, \ldots, t_r),\ b(t_1, \ldots, t_r) \text{ and } c_1(t_1, \ldots, t_r) = k(t_1, \ldots, t_r)c(t_1, \ldots, t_r).$$

Indeed, if $\tau_1, \ldots, \tau_r$ are integers such that $c_1(\tau_1, \ldots, \tau_r) \neq 0$, then the hypothesis for a, b, c asserts there are integers x, y, z, not all 0, satisfying (1). But then

$$a_1(\tau_1, \ldots, \tau_r)x^2+b(\tau_1, \ldots, \tau_r)y^2 = z^2$$

has $xk(\tau_1, \ldots, \tau_r), y, z$, as a nontrivial integral solution. Since $|a_1|+|b| < |a|+|b| = n$, the inductive hypothesis implies the existence of polynomials $x_1(t_1, \ldots, t_r), y_1(t_1, \ldots, t_r), z_1(t_1, \ldots, t_r)$ with integer coefficients and not all identically 0, such that

$$a_1(t_1, \ldots, t_r)x_1(t_1, \ldots, t_r)^2+b(t_1, \ldots, t_r)y_1(t_1, \ldots, t_r)^2 = z_1(t_1, \ldots, t_r)^2.$$

On taking

$$x(t_1, \ldots, t_r) = x_1(t_1, \ldots, t_r),$$
$$y(t_1, \ldots, t_r) = y_1(t_1, \ldots, t_r)k(t_1, \ldots, t_r),$$
$$z(t_1, \ldots, t_r) = z_1(t_1, \ldots, t_r)k(t_1, \ldots, t_r),$$

we obtain an identical solution of (2).

Hence we can suppose that $a(t_1, \ldots, t_r)$ is square free as a polynomial in t_r and hence its discriminant $D(t_1, \ldots, t_{r-1})$ with respect to t_r is not identically 0. Let $a_0(t_1, \ldots, t_{r-1})$, $c_0(t_1, \ldots, t_{r-1})$ be the leading coefficient of a and c with respect to t_r; taking $c_0 = c$ if $|c| = 0$. Let $\mathscr{T}$ be the set of points $\boldsymbol{t} = (t_1, \ldots, t_{r-1})$ in $(r-1)$-dimensional affine space defined by the inequality

$$a_0(t_1, \ldots, t_{r-1})c_0(t_1, \ldots, t_{r-1})D(t_1, \ldots, t_{r-1}) \neq 0,$$

and let T be the set of all integral $r-1$ tuples $\boldsymbol{\tau} = (\tau_1, \ldots, \tau_{r-1})$ in the set $\mathscr{T}$. For every $\boldsymbol{\tau}$ in T the polynomial $c_{\boldsymbol{\tau}}(t_r) = c(\boldsymbol{\tau}, t_r) \not\equiv 0$. Our hypothesis on a, b, c asserts that for every integer τ_r such that $c_{\boldsymbol{\tau}}(\tau_r) \neq 0$ the equation

$$a(\boldsymbol{\tau}, \tau_r)x^2+b(\boldsymbol{\tau}, \tau_r)y^2 = z^2$$

is soluble nontrivially in integers x, y, z. Hence for each $\boldsymbol{\tau}$ in T, by the case $r = 1$ of our theorem, there exist polynomials $x_{\boldsymbol{\tau}}(t_r), y_{\boldsymbol{\tau}}(t_r), z_{\boldsymbol{\tau}}(t_r)$ with integral coefficients, not all identically 0, such that

$$(3)\qquad a(\boldsymbol{\tau}, t_r)x_{\boldsymbol{\tau}}(t_r)^2+b(\boldsymbol{\tau}, t_r)y_{\boldsymbol{\tau}}(t_r)^2 \equiv z_{\boldsymbol{\tau}}(t_r)^2$$

identically in t_r. We can suppose that $(x_\tau(t_r), y_\tau(t_r), z_\tau(t_r)) = 1$. Since $a_0(\tau)D(\tau) \not\equiv 0$, $a(\tau, t_r)$ has no multiple factors, thus setting

$$d_\tau(t_r) = (a(\tau, t_r), y_\tau(t_r))$$

we get successively from (3): $d_\tau(t_r)|z_\tau(t_r)^2$, $d_\tau(t_r)|z_\tau(t_r)$, $d_\tau(t_r)^2|a(\tau, t_r)x_\tau(t_r)^2$, $d_\tau(t_r)|x_\tau(t_r)$ and hence $d_\tau(t_r) \equiv 1$. Therefore, for τ in T we have

$$(4)\qquad b(\tau, t_r) \equiv \left(\frac{z_\tau(t_r)}{y_\tau(t_r)}\right)^2 \equiv \beta_\tau(t_r)^2 \bmod a(\tau, t_r),$$

where β_τ is in $Q(t_r)$ and $|\beta_\tau| < |a|$ or $\beta_\tau = 0$.

In order to exploit the congruence (4) we note that for all nonnegavite integers h,

$$t_r^h \equiv \sum_{l=0}^{|a|-1} a_{hl}(\mathfrak{t}) t_r^l \bmod a(\mathfrak{t}, t_r),$$

where $a_{hl}(\mathfrak{t})$ are rational functions of $t_1, \ldots, t_{r-1}$ with powers of $a_0(\mathfrak{t})$ in the denominator. For τ in T we have $a_0(\tau) \neq 0$, hence $a_{hl}(\tau)$ are defined. Let

$$(5)\qquad \beta_\tau = \sum_{i=0}^{|a|-1} \xi_i t_r^i, \qquad \xi_i \in Q.$$

From (4) we get for τ in T,

$$b(\tau, t_r) \equiv \sum_{l=0}^{|a|-1} t_r^l \sum_{i,j=0}^{|a|-1} \xi_i \xi_j a_{i+j,l}(\tau) \bmod a(\tau, t_r),$$

and if

$$b(\mathfrak{t}, t_r) = \sum_{i=0}^{|a|} b_i(\mathfrak{t}) t_r^i, \qquad b_i(\mathfrak{t}) \text{ in } Z[\mathfrak{t}]$$

we get

$$(6)\qquad b_l(\tau) + b_{|a|}(\tau) a_{|a|,l}(\tau) = \sum_{i,j=0}^{|a|-1} \xi_i \xi_j a_{i+j,l}(\tau) \quad \text{for } l \leqslant |a|-1.$$

Let u be a new indeterminate and $R(\mathfrak{t}, t_r, u)$ be the resultant of the system of polynomials

$$(7)\qquad \begin{gathered} \big(b_l(\mathfrak{t}) + b_{|a|}(\mathfrak{t}) a_{|a|,l}(\mathfrak{t})\big) x_{|a|}^2 - \sum_{i,j=0}^{|a|-1} x_i x_j a_{i+j,l}(\mathfrak{t}) \qquad (0 \leqslant l < |a|), \\ \sum_{i=0}^{|a|-1} x_i t_r^i - x_{|a|} u \end{gathered}$$

with respect to the variables $x_0, \ldots, x_{|a|}$. We shall prove that $R(\mathfrak{t}, t_r, u) \neq 0$.

By a known property of resultants (see [4], p. 11) the coefficient of $u^{2|a|}$ in R is the resultant R_0 of the system obtained from (7) by substitution $x_{|a|} = 0$. If R_0 were 0, the system of homogeneous equations

$$(8)\qquad \sum_{i,j=0}^{|a|-1} \xi_i^* \xi_j^* a_{i+j,l}(\mathfrak{t}) = 0$$

would have nontrivial solutions ξ_i^* in the algebraic closure of $Q(\mathfrak{t})$. However, it then follows from (4), (5), (6), and (8) that

$$(9)\qquad 0 \equiv \Big(\sum_{i=0}^{|a|-1} \xi_i^* t_r^i\Big)^2 \bmod a(\mathfrak{t}, t_r).$$

Since $a(\mathfrak{t}, t_r)$ is square free, (9) implies

$$\sum_{i=0}^{|a|-1} \xi_i^* t_r^i \equiv 0 \bmod a(\mathfrak{t}, t_r);$$

which is impossible since $|a(\mathfrak{t}, t_r)| = |a|$.

Therefore $R_0 \neq 0$ and moreover $R_0 \in Q(\mathfrak{t})$. Let m be chosen so that

$$G(\mathfrak{t}, t_r, u) = a_0(\mathfrak{t})^m R(\mathfrak{t}, t_r, u) \in Z[\mathfrak{t}, t_r, u].$$

Then $a_0(\mathfrak{t})^m R_0(\mathfrak{t})$ is the leading coefficient of G with respect to u.

Let

$$G(\mathfrak{t}, t_r, u) = g_0(\mathfrak{t}) \prod_{\varrho=1}^{q} G_\varrho(\mathfrak{t}, t_r, u)$$

where $g_0 \in Z[\mathfrak{t}]$, $G_\varrho \in Z[\mathfrak{t}, t_r, u]$ and G_ϱ are irreducible over Q of positive degree and with leading coefficient $g_\varrho(\mathfrak{t})$ with respect to u. We can order G_ϱ so that G_ϱ is of degree 1 in u for $\varrho \leqslant p$ and of degree at least 2 for $\varrho > p$. If for all $\varrho \leqslant p$ we have

$$H_\varrho(\mathfrak{t}, t_r) = G_\varrho(\mathfrak{t}, t_r, 0)^2 - b(\mathfrak{t}, t_r) g_\varrho(\mathfrak{t})^2 \not\equiv 0 \bmod a(\mathfrak{t}, t_r)$$

then let the leading coefficient of the remainder from division of H_ϱ by $a(\mathfrak{t}, t_r)$ in the ring $Q(\mathfrak{t})[t_r]$ be $f_\varrho(\mathfrak{t}) a_0(\mathfrak{t})^{-m_\varrho}$, where $f_\varrho \in Z[\mathfrak{t}]$. By Hilbert's irreducibility theorem there exist integers $\tau_1^0, \ldots, \tau_{r-1}^0$ such that the polynomials $G_\varrho(\tau^0, t_r, u)$ are irreducible and

$$a_0(\tau^0) c_0(\tau^0) D(\tau^0) \prod_{\varrho=1}^{p} f_\varrho(\tau^0) \prod_{\varrho=0}^{q} g_\varrho(\tau^0) \neq 0.$$

Clearly τ^0 is in T. It follows from (5) and (6) that for $\mathfrak{t} = \tau^0$, $u = \beta_{\tau^0}(t_r)$ the system of polynomials (7) has a common zero

$$(\xi_0, \ldots, \xi_{|a|-1}, 1).$$

Since this zero is non-trivial we get successively

$$R(\tau^0, t_r, \beta_{\tau^0}(t_r)) = 0, \quad G(\tau^0, t_r, \beta_{\tau^0}(t_r)) = 0$$

and $G_\varrho(\tau^0, t_r, \beta_{\tau^0}(t_r)) = 0$ for a certain $\varrho \leqslant q$. Since $G_\varrho(\tau^0, t_r, u)$ is irreducible of degree at least 2 in u for $\varrho > p$ we get $\varrho \leqslant p$

$$g_\varrho(\tau^0)\beta_0(t_r) + G_\varrho(\tau^0, t_r, 0) = 0.$$

Hence by (4)

$$g_\varrho(\tau^0)^2 b(\tau^0, t_r) - G_\varrho(\tau^0, t_r, 0)^2 \equiv 0 \bmod a(\tau^0, t_r)$$

and $f_\varrho(\tau^0) = 0$ contrary to the choice of τ^0. The obtained contradiction shows that for a certain $\varrho \leqslant p$

$$g_\varrho(\mathbf{t})^2 b(\mathbf{t}, t_r) - G_\varrho(\mathbf{t}, t_r, 0)^2 \equiv 0 \bmod a(\mathbf{t}, t_r).$$

Reducing $G_\varrho(\mathbf{t}, t_r, 0) g_\varrho(\mathbf{t})^{-1}$ modulo $a(\mathbf{t}, t_r)$ in the ring $Q(\mathbf{t})[t_r]$ we find a $\beta(\mathbf{t}, t_r) \in Q(\mathbf{t})[t_r]$ such that

(10) $$b(\mathbf{t}, t_r) \equiv \beta(\mathbf{t}, t_r)^2 \bmod a(\mathbf{t}, t_r)$$

and

(11) $$|\beta| < |a| \quad \text{or} \quad \beta = 0.$$

We write

$$\beta^2(\mathbf{t}, t_r) - b(\mathbf{t}, t_r) = h^{-2}(\mathbf{t}) a(\mathbf{t}, t_r) A(\mathbf{t}, t_r)$$

where $h(\mathbf{t}) \in Z[\mathbf{t}]$ and $A \in Z[\mathbf{t}, t_r]$. In particular $h(\mathbf{t})\beta(\mathbf{t}, t_r) \in Z[\mathbf{t}, t_r]$.

If $A(\mathbf{t}, t_r) \equiv 0$ identically, we can satisfy (2) by taking

$$x(\mathbf{t}, t_r) = 0, \quad y(\mathbf{t}, t_r) = h(\mathbf{t}), \quad z(\mathbf{t}, t_r) = h(\mathbf{t})\beta(\mathbf{t}, t_r).$$

If $A(\mathbf{t}, t_r)$ is not identically 0, we have by (11) that $|A| < |a|$. We now drove the hypotheses of the lemma are satisfied for the polynomials

$$A(\mathbf{t}, t_r), \quad b(\mathbf{t}, t_r), \quad C(\mathbf{t}, t_r) = a(\mathbf{t}, t_r) h(\mathbf{t}) c(\mathbf{t}, t_r) A(\mathbf{t}, t_r).$$

We know that for all integers $\tau_1, \ldots, \tau_r$ such that $C(\boldsymbol{\tau}, \tau_r) \neq 0$, the equation (1) has a solution in integers x, y, z, not all 0. Taking

$$X = a(\boldsymbol{\tau}, \tau_r)x, \quad Y = h(\boldsymbol{\tau})\big(z - y\beta(\boldsymbol{\tau}, \tau_r)\big), \quad Z = h(\boldsymbol{\tau})\big(b(\boldsymbol{\tau}, \tau_r)y - \beta(\boldsymbol{\tau}, \tau_r)z\big)$$

we obtain

$$A(\boldsymbol{\tau}, \tau_r)X^2 + b(\boldsymbol{\tau}, \tau_r)Y^2 - Z^2 = h(\boldsymbol{\tau})^2\big(\beta(\boldsymbol{\tau}, \tau_r)^2 - b(\boldsymbol{\tau}, \tau_r)\big)(ax^2 + by^2 - z^2) = 0.$$

Also X, Y, Z are integers not all 0, since $a(\boldsymbol{\tau}, \tau_r)h(\boldsymbol{\tau})A(\boldsymbol{\tau}, \tau_r) \neq 0$. The inductive hypothesis applies to the polynomials

$$A(\mathbf{t}, t_r), \quad b(\mathbf{t}, t_r), \quad C(\mathbf{t}, t_r) \quad \text{since} \quad |A| + |b| < |a| + |b| = n.$$

Hence there exist polynomials $X(\mathbf{t}, t_r)$, $Y(\mathbf{t}, t_r)$, $Z(\mathbf{t}, t_r)$ with integral coefficients and not all identically zero, such that

$$A(\mathbf{t}, t_r)X(\mathbf{t}, t_r)^2 + b(\mathbf{t}, t_r)Y(\mathbf{t}, t_r)^2 \equiv Z(\mathbf{t}, t_r)^2$$

identically in $\mathbf{t}, t_r$. Putting

$$x(\mathbf{t}, t_r) = A(\mathbf{t}, t_r)X(\mathbf{t}, t_r),$$
$$y(\mathbf{t}, t_r) = h(\mathbf{t})\big(\beta(\mathbf{t}, t_r)Y(\mathbf{t}, t_r) + Z(\mathbf{t}, t_r)\big),$$
$$z(\mathbf{t}, t_r) = h(\mathbf{t})\big(b(\mathbf{t}, t_r)Y(\mathbf{t}, t_r) + \beta(\mathbf{t}, t_r)Z(\mathbf{t}, t_r)\big)$$

we obtain (2). Further $x(\mathbf{t}, t_r)$, $y(\mathbf{t}, t_r)$, $z(\mathbf{t}, t_r)$ do not all vanish identically since neither $A(\mathbf{t}, t_r)$ nor $b(\mathbf{t}, t_r) - \beta^2(\mathbf{t}, t_r)$ vanish identically.

Remark. The argument following formula (11) is implicit in Skolem's paper [8].

3. THEOREM 1. *Let $a(t_1, \ldots, t_r)$, $b(t_1, \ldots, t_r)$ be polynomials with integral coefficients. Suppose that for all r-tuples of arithmetic progressions $P_1, \ldots, P_r$ there exist integers $\tau_i \in P_i$ such that the equation* (1) *has a solution in integers x, y, z not all 0. Then there exist polynomials $x(t_1, \ldots, t_r)$, $y(t_1, \ldots, t_r)$, $z(t_1, \ldots, t_r)$ with integral coefficients, not all identically 0, such that* (2) *holds identically in $t_1, \ldots, t_r$.*

Proof. It is enough to show that the assumption of the theorem implies the assumption of the lemma. Now take any r-tuple of integers $\tau_1, \ldots, \tau_r$, an arbitrary prime p and a positive integer m. By the assumption of the theorem the arithmetic progressions $p^m t + \tau_1, \ldots, p^m t + \tau_r$ contain integers $\tau_1^0, \ldots, \tau_r^0$ respectively such that the equation

$$a(\tau_1^0, \ldots, \tau_r^0)x^2 + b(\tau_1^0, \ldots, \tau_r^0)y^2 = z^2$$

has a solution in integers not all 0. Hence it has a solution x_0, y_0, z_0 with $(x_0, y_0, z_0) = 1$ and we get

$$a(\tau_1, \ldots, \tau_r)x_0^2 + b(\tau_1, \ldots, \tau_r)y_0^2 \equiv z_0^2 (\bmod p^m).$$

By Theorem 2 of §5 of [1] it follows that (1) is soluble nontrivially in the field of p-adic numbers. By Lemma 2 in §7 ibidem it follows that (1) is soluble nontrivially also in real numbers, hence by Theorem 1 of §7 ibidem it is soluble nontrivially in integers.

Added in proof. Slightly different proof of Theorem 1 valid for arbitrary number fields will appear in a forthcoming book [7] of the second author.

THEOREM 2. *Let $F(x, y, t_1, \ldots, t_r)$ be any polynomial with integral coefficients which is of degree at most 2 in x and y. Suppose that for all r-tuples of arithmetic progressions $P_1, \ldots, P_r$ there exist integers $\tau_i \in P_i$ such that the equation*

$$F(x, y, \tau_1, \ldots, \tau_r) = 0$$

is soluble in rationals x, y. Then there exist rational functions $x(t_1, \ldots, t_r)$, $y(t_1, \ldots, t_r)$ *with rational coefficients such that*

$$F\big(x(t_1, \ldots, t_r),\ y(t_1, \ldots, t_r),\ t_1, \ldots, t_r\big) \equiv 0$$

identically in $t_1, \ldots, t_r$.

Proof. Theorem 2 follows from Theorem 1 for $r > 1$ in exactly the same way as Theorem B was derived from Theorem A (see [3]). In the argument (page 357) where the Corollary to Theorem 1 of [2] is used, one has instead to apply Theorem 2 of [6].

M. Fried has observed that Theorem B implies an analogous result for curves of genus 0 defined over $Q(t)$. The remark applies, *mutatis mutandis*, to Theorem 2.

One can moreover extend it to equations that define a finite union of curves of genus 0 over the algebraic closure of $Q(t)$. As to the curves of genus 1 it follows from the so-called Selmer's conjecture in the theory of rational points on such curves that for every integer t there is a rational solution of the equation

$$x^4-(8t^2+5)^2 = y^2 \tag{12}$$

(see [9]). On the other hand, suppose that rational functions $x(t)$, $y(t)$ in $Q(t)$ satisfy (12). There exist infinitely many integer pairs $\langle u, v\rangle$ such that $5u^2+8v^2$ is a prime p. Take u, v such that for $\tau = 5u/8v$, $x(\tau)$, $y(\tau)$ are defined. The equation (12) gives

$$\big(4vx(\tau)\big)^4-100p^2 = \big(16v^2y(\tau)\big)^2.$$

But, by a theorem of Nagell [5] the diophantine equation

$$X^4-100p^2 = Y^2 \quad (p \text{ prime} \equiv 1 \bmod 4)$$

has no rational solution.

References

[1] Z. I. Borevič and I. R. Šafarevič, *Number theory*, New York–London 1966.
[2] H. Davenport, D. J. Lewis, 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.
[4] F. S. Macaulay, *The algebraic theory of modular systems*, reprint, New York and London 1964.

[5] T. Nagell, *Zahlentheoretische Notizen I–IV*, Vid. Skrifter, I Mat. Naturv. Kl. 1923, No 13, Kristiania 1924.
[6] A. Schinzel, *On Hilbert's irreducibility theorem*, Ann. Polon. Math. 16 (1965), pp. 333–340.
[7] — *Selected topics on polynomials*, to be published by the University of Michigan Press.
[8] Th. Skolem, *Über die Lösung der unbestimmten Gleichung* $ax^2+by^2+cz^2 = 0$ *in einigen einfachen Rationalitätsbereichen*, Norsk Mat. Tidsskr. 10 (1928), pp. 50–62.
[9] N. M. Stephens, *Congruence properties of congruent numbers*, Bull. London Math. Soc. 7 (1975), pp. 182–184.

Received on 1. 7. 1977 (959)