where $h(x)$ is a polynomial over K. By the hypothesis of the theorem, taking x to be a suitable integer, we infer that a is the norm of an element α of K. Putting $\omega(x) = \alpha h(x)$, we obtain $f(x) = N_{K/Q}(\omega(x))$, identically, q. e. d.

References

[1] M. Bauer, *Zur Theorie der algebraischen Zahlkörper*, Math. Ann. 77 (1916), pp. 353-356.

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

[3] W. Feit and J. G. Thompson, *Solvability of groups of odd order*, Pacific J. Math. 13 (1963), pp. 775-1029.

[4] M. Hall, *The Theory of Groups*, New York 1959.

[5] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper II*, Jahresber. der Deutschen Math. Vereinigung 6 (1930).

[6] O. Haupt, *Einführung in die Algebra II*, Leipzig 1954.

[7] H. Mann, *Introduction to Algebraic Number Theory*, Columbus 1955.

[8] A. Schinzel, *On a theorem of Bauer and some of its applications*, Acta Arith., this volume, pp. 333-344.

[9] H. Zassenhaus, *The Theory of Groups*, (second edition), New York 1958.

Reçu par la Rédaction le 12. 3. 1965

ACTA ARITHMETICA
XI (1966)

Quadratic Diophantine equations with a parameter

by

H. Davenport (Cambridge), D. J. Lewis (Ann Arbor, Mich.)
and A. Schinzel (Warszawa)

We have proved in [2] the following result: Let $f(t)$ be a polynomial with integral coefficients and suppose that every arithmetical progression contains an integer t such that $F(x, y, t) = x^2+y^2-f(t) = 0$. Then $F(x(t), y(t), t) = 0$ identically, where $x(t)$ and $y(t)$ are polynomials with integral coefficients. This can be extended to $F(x, y, t) = x^2+Ay^2-f(t)$ provided $x(t), y(t)$ are allowed to have rational coefficients. An example is given in [5] showing that an analogous theorem does not hold for a general polynomial $F(x, y, t)$ even if we assume solubility for all integers t, and the question is raised there of the connection between the solubility of $F(x, y, t) = 0$ in rationals x, y for a suitable t from every arithmetical progression and the solubility in rational functions $x(t), y(t)$ (cf. also [4], Problems 5 and 6). In this paper we prove (Theorem 2) that such a connection does exist if $F(x, y, t)$ is of degree at most two in x and y. Whether, under the last assumption, the solubility in integers implies the solubility in polynomials with rational coefficients we do not know even in the simple case

$$F(x, y, t) = a(t)xy+b(t)x+c(t)$$

(a solution in polynomials with integral coefficients need not exist as is shown by the example $a(t) = 0$, $b(t) = 2$, $c(t) = t(t+1)$). On the other hand, it is easy to deduce from our Theorem 2 the result on sums of two squares mentioned at the beginning.

We start with a theorem on quadratic forms over $Q(t)$, where Q denotes the rational field.

Theorem 1. *Let $a(t)$, $b(t)$ be polynomials with integral coefficients. Suppose that every arithmetical progression contains some integer t such that the equation*

$$a(t)x^2+b(t)y^2 = z \tag{1}$$

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

$$a(t)x(t)^2+b(t)y(t)^2 = z(t)^2 \tag{2}$$

identically in t.

Proof. We can obviously suppose that neither $a(t)$ nor $b(t)$ is identically 0, since then the conclusion holds trivially. We can also suppose that $a(t)$ and $b(t)$ are not both constant, since then the conclusion is contained in the hypothesis. Thus if $|a|, |b|$ denote the degrees of the polynomials a, b, we can suppose that $|a|+|b| > 0$.

We proceed by induction on $|a|+|b|$. We suppose that the result holds for all polynomials $a(t), b(t)$ satisfying $|a|+|b| < k$, where k is some positive integer, and we have to prove the result when $|a|+|b| = k$. We can suppose without loss of generality that $|a| \geqslant |b|$.

If $a(t)$ is not square-free, say $a(t) = k^2(t)a_1(t)$, then the hypothesis is satisfied for the polynomials $a_1(t), b(t)$, since every arithmetical progression contains infinitely many integers t (cf. [2], p. 109) for which (1) is properly soluble in x, y, z, and among these there are at most finitely many for which $k(t) = 0$. Since $|a_1|+|b| < k$, the inductive hypothesis implies that there exist polynomials $x_1(t), y_1(t), z_1(t)$, not all identically 0, such that

$$a_1(t)x_1(t)^2+b(t)y_1(t)^2 = z_1(t)^2.$$

On taking

$$x(t) = x_1(t), \quad y(t) = k(t)y_1(t), \quad z(t) = k(t)z_1(t),$$

we obtain an identical solution of (2). Hence we can suppose that $a(t)$ is square-free.

Now $a(t)$ and $a'(t)$ are relatively prime, and therefore there exist polynomials $M(t)$, $N(t)$ with integral coefficients such that

$$M(t)a(t)+N(t)a'(t) = D, \tag{3}$$

where D is a non-zero integer.

Let

$$a(t) = a_0p_1(t)\dots p_m(t), \tag{4}$$

where a_0 is an integer and $p_1(t), p_2(t), \dots, p_m(t)$ are distinct irreducible polynomials with rational coefficients and highest coefficient 1. Let $p(t)$ be any one of the polynomials $p_i(t)$ and let θ be one of its zeros. There are infinitely many prime ideals $\mathfrak{q}$ of the first degree in the field $Q(\theta)$ generated by θ, and for all but a finite number of them, $q = N\mathfrak{q}$ does not divide a_0D. Since $\mathfrak{q}$ is of first degree and does not divide the denominator of θ (because it does not divide a_0), there exists a rational integer t_0 such that $t_0 \equiv \theta \pmod{\mathfrak{q}}$, and therefore

$$a(t_0) \equiv 0 \pmod{q}.$$

On noting that q cannot divide $a'(t_0)$ by (3), we see that by choosing t_1 to be either t_0 or t_0+q, we can ensure that

$$a(t_1) \equiv 0 \pmod{q}, \quad a(t_1) \not\equiv 0 \pmod{q^2}.$$

By hypothesis the arithmetical progression $t \equiv t_1 \pmod{q^2}$ contains an integer t_2 such that the equation

$$a(t_2)x_2^2+b(t_2)y_2^2 = z_2^2$$

has a solution in integers x_2, y_2, z_2, not all 0. These integers can be taken relatively prime. Since $a(t_2)$ is divisible by q but not by q^2, we have $y_2 \not\equiv 0 \pmod{q}$, whence

$$b(t_2) \equiv w^2 \pmod{q}$$

or some integer w. Since $t_2 \equiv \theta \pmod{\mathfrak{q}}$, this implies

$$b(\theta) \equiv w^2 \pmod{\mathfrak{q}}.$$

This holds, with some w depending on $\mathfrak{q}$, for all but a finite number of the prime ideals of the first degree in $Q(\theta)$. It follows from a known theorem(1) on the density of the prime ideals for which a given number of the field has a prescribed quadratic character, that

$$b(\theta) = \beta(\theta)^2,$$

where $\beta(t)$ is a polynomial with rational coefficients. Since θ is a zero of $p(t)$, this implies that

$$b(t) \equiv \beta^2(t) \big(\mathrm{mod}\, p(t)\big).$$

We apply this to each of the factors $p_i(t)$ in (4). Since the polynomials $p_i(t)$ are distinct and irreducible, it follows that for some polynomial $\beta(t)$ with rational coefficients we have

$$b(t) \equiv \beta^2(t) \big(\mathrm{mod}\, a(t)\big).$$

We write(2)

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

(1) See [3], Satz 169. The theorem as stated does not assert that the prime ideals are of the first degree, but this is apparent from the nature of the proof, since prime ideals of higher degree contribute only a bounded amount to $L(s)$ as $s \to 1$. Further, the theorem as stated is for an integer of the field, and $b(\theta)$ may be fractional; but we can put $b(\theta) = c(\theta)/d^2$, where $c(\theta)$ is integral and d is a positive integer, and apply the theorem (with $m = 1$) to $c(\theta)$.

(2) The argument which follows is due essentially to Legendre; see, for example [1], pp. 156-158.

where h is a suitable positive integer and A has integral coefficients. In particular, $h\beta(t)$ has integral coefficients.

Since we can plainly suppose that either $\beta(t) = 0$ identically or $|\beta| < |a|$, we have either $A(t) = 0$ identically or $|A| < |a|$. If $A(t) = 0$ identically we can satisfy (2) by taking $x(t) = 0$, $y(t) = h$, $z(t) = h\beta(t)$, so we can suppose that $A(t)$ is not identically 0.

We now prove that the hypotheses of the theorem are satisfied for the polynomials $A(t)$, $b(t)$. We know that every arithmetical progression contains infinitely many integers t such that the equation (1) has a solution in integers x, y, z, not all 0. Taking $X = ax$, $Y = h(-\beta y+z)$, $Z = h(by-\beta z)$, we obtain

$$AX^2+bY^2-Z^2 = h^2(\beta^2-b)(ax^2+by^2-z^2) = 0.$$

Also X, Y, Z are integers not all 0 provided $a(t)\big(\beta(t)^2-b(t)\big) \neq 0$, which holds for t sufficiently large. This proves the assertion.

The inductive hypothesis applies to the polynomials $A(t)$, $b(t)$, since $|A|+|b| < |a|+|b| = k$. Hence there exist polynomials $X(t)$, $Y(t)$, $Z(t)$ with integral coefficients, not all identically 0, such that

$$A(t)X^2(t)+b(t)Y^2(t) = Z^2(t).$$

Putting

$$x(t) = A(t)X(t), \quad y(t) = h\big(\beta(t)Y(t)+Z(t)\big),$$
$$z(t) = h\big(b(t)Y(t)+\beta(t)Z(t)\big),$$

we obtain the identity (2). Further, $x(t)$, $y(t)$, $z(t)$ do not all vanish identically since neither $A(t)$ nor $b(t)-\beta^2(t)$ vanishes identically.

THEOREM 2. *Let $F(x, y, t)$ be any polynomial with integral coefficients which is of degree at most 2 in x and y. Suppose that every arithmetical progression contains an integer t such that the equation*

$$F(x, y, t) = 0 \tag{5}$$

is soluble in rationals x, y. Then there exist two rational functions $x(t)$, $y(t)$ with rational coefficients such that

$$F\big(x(t), y(t), t\big) = 0 \tag{6}$$

identically in t.

Proof. If F is of degree at most 1 in both x and y, the conclusion is immediate. If F is of degree 2 in one of the variables, say x, it can be expressed either in the form

$$F(x, y) = A(t)\big(x+a(t)y+\beta(t)\big)^2+B(t)\big(y+\gamma(t)\big)^2+C(t),$$

or in the form

$$F(x, y) = A(t)\big(x+a(t)y+\beta(t)\big)^2+B_1(t)y+C(t),$$

where A, B, B_1, C, a, β, γ are rational functions of t and AB_1 is not identically 0, but BC may be. In the second case, there is an identical solution

$$Y = -\frac{C(t)}{B_1(t)}, \quad X = a(t)\frac{C(t)}{B_1(t)}-\beta(t).$$

In the first case, by an obvious change of variables, which does not affect the hypothesis or the conclusions, it will be sufficient to prove the result for

$$F(x, y) = A(t)x^2+B(t)y^2+C(t).$$

We can suppose that $C(t)$ is not identically 0, since then there is the obvious identical solution $x(t) = y(t) = 0$.

We write

$$A(t)C(t) = -\frac{a(t)}{D^2(t)}, \quad B(t)C(t) = -\frac{b(t)}{D^2(t)},$$

where a, b, D are polynomials with integral coefficients. It follows from the hypothesis that every arithmetical progression contains an integer t such that the equation

$$a(t)\xi^2+b(t)\eta^2 = \zeta^2$$

has a solution in integers ξ, η, ζ, not all 0. By Theorem 1 there exist polynomials $\xi(t)$, $\eta(t)$, $\zeta(t)$ with integral coefficients such that

$$a(t)\xi^2(t)+b(t)\eta^2(t) = \zeta^2(t)$$

identically, and $\xi(t)$, $\eta(t)$, $\zeta(t)$ are not all identically 0.

If $\xi(t)$ and $\zeta(t)$ are both identically 0 then $b(t)$ is identically 0, and so is $B(t)$. The hypothesis then implies that every arithmetical progression contains an integer t such that $-C(t)/A(t)$ is a square. This implies[3] that $-C(t)/A(t)$ is the square of a rational function of t, and this gives the desired identical solution of (6).

If $\zeta(t)$ is identically 0 but $\xi(t)$ is not, we take

$$x(t) = \frac{C(t)+A(t)}{2A(t)}, \quad y(t) = \frac{C(t)-A(t)}{2A(t)}\cdot\frac{\eta(t)}{\xi(t)},$$

and since $A(t)\xi^2(t)+B(t)\eta^2(t) = 0$ we obtain

$$A(t)x^2(t)+B(t)y^2(t) = C(t)$$

identically.

---

[3] See the Corollary to Theorem 1 of [2]. This must be applied to the polynomial obtained from $-C(t)/A(t)$ by multiplying by the square of a suitable polynomial.

Finally, if $\zeta(t)$ is not identically 0, we take

$$x(t) = \frac{C(t)}{D(t)} \cdot \frac{\xi(t)}{\zeta(t)}, \qquad y(t) = \frac{C(t)}{D(t)} \cdot \frac{\eta(t)}{\zeta(t)}$$

and obtain the same identity.

References

[1] H. Davenport, *The Higher Arithmetic*, London 1952.

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

[3] E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen*, Leipzig 1923.

[4] A. Schinzel, *Some unsolved problems on polynomials*, Matematicka Biblioteka 25 (1963), pp. 67-70.

[5] — *On Hilbert's irreducibility theorem*, Ann. Polon. Math. 16 (1965), pp. 333-340.

Reçu par la Rédaction le 19. 3. 1965

ACTA ARITHMETICA
XI (1966)

Sur un résultat de Jarník

par

J. Lesca (Grenoble)

Dans cet article, tous les nombres considérés sont réels. Dans l'article suivant, nous étudierons des problèmes analogues p-adiques.

I. Introduction. Dans un article [1] paru en 1959, V. Jarník démontre l'existence, dans certains cas, de systèmes libres(1) admettant une approximation continuelle donnée; il obtient:

„Etant donnés deux entiers m et $n \geqslant 1$, $m+n > 2$ et une fonction d'approximation $\varphi(t)$, soit M_{mn} l'ensemble des (n, m)-systèmes Θ tels que:

Θ est libre,

Θ admet l'approximation continuelle $\varphi(t)$.

Alors M_{mn} n'est pas vide dans les cas suivants:

$m \geqslant 2$,

$m = 1$ et $\lim\limits_{t\to\infty} \{t\varphi(t)\} = +\infty$.

Plus précisément, dans chacun des cas précédents, si G est un ouvert non vide de $\mathscr{R}^{mn}$, la projection sur chacun des axes de $G \cap M_{mn}$ a la puissance du continu".

Dans le cas d'une signature $(m, 1)$ $(m \geqslant 2)$, nous démontrons un résultat qui complète le précédent.

Théorème. *Etant donnés un entier $n > 1$ et une fonction d'approximation $\varphi(t)$ telle que $\limsup\limits_{t\to\infty} \{t\varphi(t)\} = +\infty$, soit M_n l'ensemble des $(1, n)$-systèmes Θ tels que:*

Θ est libre,

Θ admet l'approximation continuelle $\varphi(t)$.

Alors M_n n'est pas vide; plus précisément si G est un ouvert non vide de $\mathscr{R}^n$ la projection sur chacun des axes de $M_n \cap G$ a la puissance du continu.

---

(1) Pour les définitions et notations, se reporter au § II.