ACTA ARITHMETICA
XXI (1972)

On a diophantine equation

by

E. TROST (Zürich)

Let $r \neq 0$ be an element of a field K with characteristic $p \geqslant 0$ and $n \geqslant 2$ an integer. In this note we consider the diophantine equation

$$(1)\qquad D(n, r) = \begin{vmatrix} x_1 & x_2 & \ldots & x_n \\ x_2 & x_3 & \ldots & rx_1 \\ \cdot & \cdot & \cdot & \cdot \\ x_n & rx_1 & \ldots & rx_{n-1} \end{vmatrix} = 0.$$

(1) is said to be *solvable* in K if there is a solution $(x_1, x_2, \ldots, x_n) \neq (0, 0, \ldots, 0)$, $x_i \in K$ $(i = 1, 2, \ldots, n)$. In the real field (1) is solvable if $r^{1/n}$ is real. Putting in this case $x_1 = x_2 = \ldots = x_{n-1} = 1$ we get for x_n the equation (see [3], p. 99)

$$(x_n - r)^n - r(x_n - 1)^n = 0 \quad \text{yielding} \quad x_n = (r \mp r^{1/n})(1 \mp r^{1/n})^{-1}.$$

For $r < 0$ and even n there are equations (1) without non-trivial real solutions, for example $rx_1^2 - x_2^2 = 0$.

THEOREM 1. (1) *is solvable in* K *in two cases*;

$$(2)\qquad \begin{cases} 1)\ r = s^d,\ d\,|\,n,\ d > 1,\ s \in K, \\ 2)\ r = -4t^4,\ 4\,|\,n,\ t \in K. \end{cases}$$

Proof. Let $K[x]$ be the ring of polynomials with coefficients in K. $K[x]$ contains $f(x) = x^n - r$. Let R denote the quotient ring $K[x]/(f(x))$. We take from R the elements

$$a = x_n + x_{n-1}x + \ldots + x_1 x^{n-1}, \quad b = y_1 + y_2 x + \ldots + y_n x^{n-1}$$

and suppose

$$(3)\qquad ab = 0, \quad (x_1, x_2, \ldots, x_n) \neq (0, 0, \ldots, 0).$$

(3) leads to the following system of n linear equations with n unknowns $y_1, y_2, \ldots, y_n$

$$(4)\qquad \begin{aligned} x_1 y_1 + x_2 y_2 + \ldots + x_n y_n &= 0, \\ \cdots\cdots\cdots\cdots & \\ x_n y_1 + r x_1 y_2 + \ldots + r x_{n-1} y_n &= 0. \end{aligned}$$

The determinant of the system (4) is $D(n, r)$. (4) has a non-trivial solution if and only if $D(n, r) = 0$. In this case a, b are zero divisors in R. Whenever $f(x)$ is irreducible in K, R is a field and has therefore no zero divisors. Thus the solvability of (1) implies the reducibility of $f(x)$ in K. By Capelli's theorem (see [4], p. 662) $f(x)$ is reducible in K if and only if (2) holds (1). Now we give a solution in each of the cases (2).

1) $x_{km+i} = s^k$, $s \in K$, $m = nd^{-1}$, $i = 1, 2, \ldots, m$, $k = 0, 1, \ldots, d-1$. Setting these values in (1) and denoting the kth row of the resulting determinant by the vector Z_k we have $sZ_1 = Z_{m+1}$. Thus the determinant vanishes.

2) $x_i = 0$, $x_{m+i} = 1$, $x_{2m+i} = -2t$, $x_{3m+i} = 2t^2$, $t \in K$, $m = n/4$, $i = 1, 2, \ldots, m$. In this case we observe the relation $tZ_1 + Z_{m+1} = -(2t)^{-1} Z_{2m+1}$. Thus the determinant vanishes.

We can give the complete solution of a solvable equation (1) whenever n is a prime number and K the field Q of rational numbers. In this case we have $r = s^n$.

THEOREM 2. *In Q the complete solution of*

$$D(n, s^n) = 0, \quad n \text{ a prime}, \; s \in Q, \tag{5}$$

is given by $(a, as, \ldots, as^{n-1})$, $a \in Q$, *and* $s^{n-1}x_1 + s^{n-2}x_2 + \ldots + x_n = 0$.

Proof. Let A_n denote the cyclic determinant

$$\begin{vmatrix} y_1 & y_2 & \cdots & y_n \\ y_2 & y_3 & \cdots & y_1 \\ \cdot & \cdot & \cdots & \cdot \\ y_n & y_1 & \cdots & y_{n-1} \end{vmatrix}.$$

By setting $x_i = s^{i-1}y_i$ $(i = 1, 2, \ldots, n)$ in (5) we get $D(n, s^n) = s^{n(n-1)}A_n$. It is known (see [1], p. 160) that

$$A_n = (-1)^{(n-1)(n-2)/2} \prod_{\nu=0}^{n-1} [y_1 + y_2\xi^\nu + \ldots + y_n \xi^{(n-1)\nu}], \qquad \xi = e^{2\pi i/n}.$$

From $A_n = 0$ we infer

$$\sum y_i = 0 \quad \text{or} \quad \sum y_i \xi^{(i-1)\nu} = 0 \quad (\nu = 1, 2, \ldots, n-1).$$

The first relation yields $\sum s^{1-i}x_i = 0$ or, by multiplying by s^{n-1}, $\sum s^{n-i}x_i = 0$. Since the cyclotomic polynomial $1 + z + z^2 + \ldots + z^{n-1}$ is irreducible in Q from each of the remaining $n-1$ relations follows $y_1 = y_2 = \ldots = y_n = a$. Therefore we have the solution $(a, as, \ldots, as^{n-1})$.

(1) This part of the proof was given in [5].

It is an interesting question whether local solvability of a diophantine equation implies global solvability (i.e. solution in integers). In the case of (1) for n a prime and r an integer p-adic fields are not required. It suffices to suppose solvability for almost all (2) finite fields F_p of residues modulo a prime p.

THEOREM 3. *Let r be an integer $\neq 0$ and n a prime. The equation $D(n, r) = 0$ is solvable in integers if and only if the congruence $D(n, r) \equiv 0 \pmod{p}$ is solvable for almost all primes p with $(x_1, x_2, \ldots, x_n, p) = 1$.*

Proof. From the solvability of $D(n, r) = 0$ in F_p $(p \neq n)$ follows by Theorem 1 that r is a nth power residue modulo p. If r has this property for almost all primes there exists a rational integer s such that $r = s^n$ [6]. Applying again Theorem 1 completes the proof.

In [2] L. J. Mordell remarks that it is very difficult to prove the non-existence of integer solutions of the general equation

$$ax^3 + by^3 + cz^3 - dxyz = 0.$$

By setting $n = 3$ in (1) we get an equation of this type with $a = r^2$, $b = r$, $c = 1$, $d = 3r$. It is obvious that the impossibility of this equation for $r \neq s^3$ can easily be shown by divisibility considerations.

(2) "Almost all" primes means that the sequence of exceptional primes has Kronecker-density zero.

Added in proof (12. 4. 1972): (1) is a special case of an equation treated 1895 by E. Maillet by means of the theory of recurring series (see L. E. Dickson, *History of the Theory of Numbers*, vol. II, p. 695, New York 1966).

In chapter 7, § 2 of his monograph *The Jacobi–Perron Algorithm, its Theory and Applications* (Lecture Notes in Mathematics No. 207, Springer 1971) L. Bernstein deals with the equation $D(n, r) = \pm 1$ where r is a positive integer.

References

[1] W. Gröbner, *Matrizenrechnung*, München 1956.
[2] L. J. Mordell, *Diophantine Equations*, London 1969.
[3] G. Pólya und G. Szegö, *Aufgaben und Lehrsätze aus der Analysis II*, New York 1945.
[4] L. Rédei, *Algebra*, Leipzig 1959.
[5] E. Trost, *Problem 550*, Solution by the Proposer, El. Math. 23 (1968), p. 66.
[6] — *Zur Theorie der Potenzreste*, Nieuw Archief voor Wiskunde 18 (1934), pp. 58–61.

Received on 27. 12. 1970 (130)