THEOREM. *Let $f_1(x_1, \ldots, x_r), \ldots, f_k(x_1, \ldots, x_r)$ denote polynomials with coefficients in F that satisfy* (3). *Then the f_j are equivalent under the group $\boldsymbol{T}$ to a set of polynomials in at most $r-s$ indeterminates.*

References

[1] James Ax, *Zeroes of polynomials over finite fields*, Amer. Journ. Math. 86 (1964), pp. 255-261.

[2] L. Carlitz, *Invariant theory of systems of equations in a finite field*, Journ. Analyse Math. 3 (1953/54), pp. 382-413.

Reçu par la Rédaction le 13. 5. 1968

ACTA ARITHMETICA
XV (1969)

The diophantine equation $dy^2 = ax^4+bx^2+c$

by

L. J. MORDELL (Cambridge)

It is well known and easily proved that the equation

$$dy^2 = ax^4+bx^2+c, \tag{1}$$

where $a > 0$, b, c, $d > 0$ are integers, $b^2-4ac \neq 0$, has only a finite number of integer solutions. Thus write (1) as

$$dy^2 = ax^4+bx^2z+cz^2, \quad z = 1. \tag{2}$$

Then the general solution of (2) is given by a finite number of expressions of the form

$$x^2 = a_1p^2+b_1pq+c_1q^2, \tag{3}$$

$$z = 1 = a_2p^2+b_2pq+c_2q^2, \tag{4}$$

where p, q are integers.

The general solution of (3) is given by a finite number of expressions of the form

$$p = a_3r^2+b_3rs+c_3s^2, \quad q = a_4r^2+b_4rs+c_4s^2, \tag{5}$$

where r, s are integers.

Substituting in (4), we have a finite number of equations of the form

$$Ar^4+Br^3s+Cr^2s^2+Drs^3+Es^4 = 1. \tag{6}$$

By Thue's theorem, such equations have only a finite number of integer solutions. In general, it is very difficult to find these, and much detail and advanced technique are often required. There are, however, some classes of equations (1) all of whose integer solutions can be found by elementary means. This idea had been previously [1] applied to equations of the form

$$y^2 = ax^3+bx^2+cx+d.$$

---

[1] L. J. Mordell, *The diophantine equation $y^2 = ax^3+bx^2+cx+d$ or fifty years after*, Journ. Lond. Math. Soc. 38 (1963), pp. 454-458. *The diophantine equation $y^2 = ax^3+bx^2+cx+d$*, Rend. Circ. Mat. Palermo (II) 13 (1964), pp. 1-8.

Write the equation (1) as

$$dy^2 = a_1a_2x^4 - bx^2 + c, \quad a = a_1a_2, \quad a_1 > 0, \ a_2 > 0, \tag{7}$$

where we may suppose $x \geqslant 0, y \geqslant 0$.

Suppose it can be written in the form

$$dy^2 + kl^2 = (a_1x^2 - p)(a_2x^2 - q), \tag{8}$$

where k, l, p, q are integers at present undefined.

Then

$$pa_2 + qa_1 = b, \tag{9}$$

$$pq = c + kl^2, \tag{10}$$

and so

$$(pa_2 - qa_1)^2 = b^2 - 4a(c + kl^2),$$

and, say

$$4akl^2 + m^2 = b^2 - 4ac, \tag{11}$$

where

$$m = pa_2 - qa_1. \tag{12}$$

Hence (7) can be written in the form (8) if (11) has an integer solution l, m for which both

$$(b+m)/2a_2, \quad (b-m)/2a_1 \tag{13}$$

are integers.

The equation (8) imposes conditions on the quadratic character of $a_1x^2 - p \pmod{dk}$, and a contradiction may arise for appropriate k, l. We take $d = 1$, and consider the cases when $k = 1, 2$.

Suppose first that $k = 1$, and that l has no prime factors $\equiv 3 \pmod 4$. We investigate conditions under which there are no solutions with $a_1x^2 > p$, and $a_2x^2 > q$. Then we can exclude $x \equiv 0 \pmod 2$ if either $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$. Also $x \equiv 1 \pmod 2$ can be excluded if either $a_1 - p \equiv 3, 6, 7 \pmod 8$ or $a_2 - q \equiv 3, 6, 7 \pmod 8$. The equations so found may perhaps be easily proved impossible by direct congruence considerations applied to (7). This can be avoided by constructing equations which actually have solutions with $a_1x^2 - p < 0$. Thus, solutions $(x, y) = (0, y_0)$, $(1, y_1)$ exist if

$$y_0^2 + l^2 = pq, \quad y_1^2 + l^2 = (p - a_1)(q - a_2).$$

It is of course possible that other solutions exist with $a_1x^2 - p < 0$, and these can be found by inspection.

A simple instance is

$$y^2 + l^2 = (px^2 - p - 1 - 4q)(rx^2 - s), \tag{14}$$

where $p > 0$, $q \geqslant 0$, $s > r > 0$, and l has no odd factors $\equiv 3 \pmod 4$. The first factor excludes $x \equiv 1 \pmod 2$, and the second factor excludes $x \equiv 0 \pmod 2$ if $s \equiv 1 \pmod 4$. This is obviously satisfied by the existence of a solution with $x = 0$.

For solutions with $x = 0, 1, 2$, we have

$$y_0^2 + l^2 = s(p + 1 + 4q),$$

$$y_1^2 + l^2 = (s - r)(4q + 1),$$

$$y_2^2 + l^2 = (s - 4r)(4q - 3p + 1).$$

Hence

$$s = \frac{y_0^2 + l^2}{p + 1 + 4q}, \quad r = s - \frac{y_1^2 + l^2}{4q + 1}, \tag{15}$$

$$y_2^2 + l^2 = (4q - 3p + 1)\left(\frac{4y_1^2 + 4l^2}{4q + 1} - \frac{3y_0^2 + 3l^2}{p + 1 + 4q}\right). \tag{16}$$

There is no difficulty in finding integer values for p, q, l, r, s. Consider the special case $l = 1$, $p = 4$, $q = 3$. Then

$$s = \frac{y_0^2 + 1}{17}, \quad r = \frac{y_0^2 + 1}{17} - \frac{y_1^2 + 1}{13}.$$

We can take $y_0 = 13$, $s = 10$, $y_1 = 5$, $r = 8$. Then

$$y^2 + 1 = (4x^2 - 17)(8x^2 - 10)$$

has only the solutions $x = 0$, $x = \pm 1$.

It is more difficult to find equations with a third solution. Now (16) becomes

$$y_2^2 + 1 = \frac{4y_1^2 + 4}{13} - \frac{3y_0^2 + 3}{17}.$$

We require integer solutions with $r > 0$, that is

$$\frac{y_0^2 + 1}{17} > \frac{y_1^2 + 1}{13}.$$

The solution $y_0 = 4$, $y_2 = 2$, $y_1 = 5$ does not satisfy this condition.

Dr. R. F. Churchhouse of the Atlas computer laboratory has kindly given me a large number of solutions. It suffices to mention only

$$y_0 = 132, \ y_1 = 112, \ y_2 = 28.$$

The corresponding equation is

$$y^2 + 1 = (4x^2 - 17)(60x^2 - 1025),$$

and so this has only the non-negative integer solutions

$$x_0 = 0,\ x_1 = 1,\ x_2 = 2.$$

It might be of interest to find similar equations with four or more solutions.

An instance when $k = 2$ is given by

$$(17)\quad y^2+2l^2 = \big((8p+2)x^2-8q-3\big)(rx^2-s),\quad p \geqslant 0,\ q \geqslant 0,\ r>0,\ s>0,$$

where we suppose l has no prime factors $\equiv 5, 7 \pmod 8$. The first factor if positive excludes both $x \equiv 0 \pmod 2$ and $x \equiv 1 \pmod 2$.

If $(x, y) = (0, y_0), (1, y_1)$ are solutions, then

$$y_0^2+2l^2 = (8q+3)s,\quad y_1^2+2l^2 = (8q-8p+1)(s-r).$$

Hence

$$s = \frac{y_0^2+2l^2}{8q+3},\quad r = s-\frac{y_1^2+2l^2}{8q-8p+1}.$$

Take $l = 1, p = q = 0, y_0 = 8, s = 22, r = 20-y_1^2$. Then

$$y^2+2 = (2x^2-3)\big((20-y_1^2)x^2-22\big)$$

has only the solutions $(x, y) = (0, \pm 8), (\pm 1, \pm y_1)$.

ST. JOHN'S COLLEGE
Cambridge, England

Reçu par la Rédaction le 4. 6. 1968

ACTA ARITHMETICA
XV (1969)

On ratio sets of sets of natural numbers

by

T. Šalát (Bratislava)

Let us denote by N (C and R^+ respectively) the set of all natural numbers (all integral numbers and all positive rational numbers respectively). If $A \subset N$, $A \neq \emptyset$, then we put

$$D(A) = \{x \in C;\ \exists_{c,d \in A}\ x = c-d\},$$

$$R(A) = \Big\{x \in R^+;\ \exists_{c,d \in A}\ x = \frac{c}{d}\Big\}.$$

$D(A)$ is the set of differences of numbers of the set A and $R(A)$ is the ratio set of the set A.

In the paper [3] it is proved that $D(A) = C$ if the upper asymptotic density of the set A is greater than $1/2$. It is even proved in that paper that in this case (that is if the upper asymptotic density of A is greater than $1/2$) the following holds: for each $x \in C$ there exists an infinite number of pairs (c, d) of numbers of the set A such that $x = c-d$.

Let us remark that the condition $\delta_2(A) > 1/2$ ($\delta_2(A)$ denotes the upper asymptotic density of the set A) it is only a sufficient condition for the equality $D(A) = C$ to be true. E.g. if $A = \{1, 2, 4, \ldots, 2n, \ldots\}$, then we have obviously $\delta_2(A) = 1/2$ ($= \delta(A)$, $\delta(A)$ denotes the asymptotic density of the set A) and simultaneously $D(A) = C$.

We shall prove in this paper a theorem on the ratio sets which is analogous to the above mentioned theorem of Professor W. Sierpiński (see Theorem 1) and then we shall study some properties of $A \subset N$ which quarantee the density of $R(A)$ in the interval $\langle 0, +\infty)$.

Theorem 1. *Let $\delta_2(A) = 1$. Then for each $x \in R^+$ there exists an infinite number of pairs (c, d) of numbers of the set A such that $x = c/d$.*

Corollary. *If $\delta_2(A) = 1$, then $R(A) = R^+$.*

Proof of the theorem. Let $\delta_2(A) = 1$. Let us suppose that the assertion of the theorem is not true. Then there exists a positive rational number $r = \frac{p}{q} \neq 1$, $(p, q) = 1$ such that $r = \frac{c}{d}$ only for a finite number of pairs (c, d) of numbers of the set A.