ACTA ARITHMETICA
XV (1969)

A theorem on sets of polynomials over a finite field*

by

L. CARLITZ (Durham, North Carolina)

Let $F = \mathrm{GF}(q)$ denote the finite field of order $q = p^n$, where p is a prime and $n \geqslant 1$. Let

$$f_j(x_1, \ldots, x_r) \quad (j = 1, \ldots, k) \tag{1}$$

denote polynomials in the indeterminates $x_1, \ldots, x_r$ with coefficients in F and let N denote the number of solutions in F of the system

$$f_j(x_1, \ldots, x_r) = 0 \quad (j = 1, \ldots, k). \tag{2}$$

Ax [1] has proved that N is divisible by q^s, provided

$$r > s \sum_{j=1}^{k} \deg f_j. \tag{3}$$

Moreover he gave an example that shows that this result is best possible.

The writer [2] has discussed the equivalence of sets of polynomials in r indeterminates over F under the group $\boldsymbol{T}$ of (polynomial) transformations

$$y_j = \varphi_j(x_1, \ldots, x_r) \quad (j = 1, \ldots, r)$$

possessing an inverse. In particular he proved ([2], Theorem 4.9) that the set of polynomials (1) is equivalent (under $\boldsymbol{T}$) to a set of polynomials in $r-s$ indeterminants if and only if the number of solutions of the system

$$f_j(x_1, \ldots, x_r) = c_j \quad (j = 1, \ldots, r) \tag{4}$$

is divisible by q^s for all $c_j \in F$.

If in (2) we replace f_j by $f_j - c_j$ it is clear that (3) is unaltered. Application of Ax's result therefore leads to the following

* Supported in part by NSF grant GP-5174.

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.