

Row-reduction and invariants of Diophantine equations

N J WILDBERGER

School of Mathematics, University of New South Wales, Sydney 2052 Australia

MS received 30 March 1993; revised 9 February 1994

Abstract. To any Diophantine equation with integral coefficients we associate a finitely generated abelian group. The analysis of this group by row-reduction generally leads to simpler equations which are equivalent to the original but often dramatically easier to solve. This method of studying equations is useful over finite fields as well as over \mathbb{Q} . Some applications and an example are discussed.

Keywords. Diophantine equations; row-reduction.

Introduction

Let f be a polynomial in the variables X_1, \dots, X_n with integral coefficients and consider the problem of finding all rational solutions of the equation

$$f(X_1, \dots, X_n) = 0. \quad (1)$$

Historically work on this problem has focused on particular equations of low degree with a few variables. General results that apply to all polynomials or even large classes of polynomials are few and are mostly concerned with the existence of non-zero solutions, where a solution (s_1, \dots, s_n) of (1) is called non-zero if at least one of the s_i is non-zero.

For an arbitrary large non-homogeneous polynomial f , however, it would seem that this basic problem is hopelessly difficult. We hope to show in this paper that this is not so; specifically we will present a method to modify the general equation (1) which often results in a drastic simplification of the equation and sometimes to a complete determination of all solutions. It will be seen that this method can be useful when trying to solve (1) over any field, and in particular over a finite field it is surprisingly powerful considering its simplicity.

Before presenting the method in detail, we make a comment on the relevance of non-zero solutions of (1). Consider the following elementary method of obtaining such solutions. Suppose that $n \geq 2$. If one of the variables X_i occurs in each term of f , set $X_i = 0$ and let the other variables be arbitrary with at least one of them non-zero; this is a non-zero solution. Otherwise, pick one of the variables, set it to zero and examine the resulting equation for a variable which occurs in each term. If one occurs and the number of variables still exceeds 1, then we have a non-zero solution as before, otherwise we continue. We eventually get a non-zero solution or arrive at an equation with exactly one variable. If we can find a non-zero solution to this one-variable equation, we have a non-zero solution to the original equation.