SOME THEOREMS AND CONJECTURES IN DIOPHANTINE EQUATIONS

BY SERGE LANG

The theory of diophantine equations may be regarded as the natural continuation of algebraic geometry proper: Having once obtained a general theory of algebraic equations in several variables over essentially arbitrary ground fields (or rings), one tries to get statements depending on the special arithmetic structure of the coefficient domain. By definition, this becomes diophantine analysis. We shall list a few of the theorems and conjectures which arise in this direction.

Let k be a field, and $f(X_1, \cdots, X_n)$ a polynomial, also written $f(X)$, with coefficients in k. The equation $f=0$ defines an algebraic set, i.e. the set of all n-tuples $(x_1, \cdots, x_n)$ in some algebraically closed field containing k, such that $f(x)=0$. Such a point (x) in n-space is said to be a zero of f. It is said to be a rational point in k if all x_i lie in k. If f is a form (i.e. a homogeneous polynomial) then one views f as defining an algebraic set in projective space, and one considers nontrivial zeros, that is zeros such that not all x_i are 0. A nontrivial zero then defines a point in projective space, which is rational over k if again the coordinates can be chosen in k.

More generally, one considers systems of equations, or varieties (meaning an absolutely irreducible algebraic set). If V is a variety defined over a field k, then a point in it is rational over k if it has a set of coordinates in k.

The basic coefficient domain is that of the rational numbers $\boldsymbol{Q}$ or the integers $\boldsymbol{Z}$. It is but a step from this to a finite extension k of $\boldsymbol{Q}$ (called a number field) or the ring of integers I_k of k instead of $\boldsymbol{Z}$. We have primes $\mathfrak{p}$ associated with such fields: They are the absolute values which either induce the ordinary absolute value on $\boldsymbol{Q}$ (called archimedean primes) or the p-adic absolute value, defined by a prime number p:

$$|p^r m/n|_{\mathfrak{p}} = 1/p^r$$

if $m, n \in \boldsymbol{Z}$, $mn \neq 0$, and $p \nmid mn$. The latter are called finite primes. One can then form the completion $k_{\mathfrak{p}}$ under the prime $\mathfrak{p}$, which is called a $\mathfrak{p}$-adic field, and is the field of real or complex numbers if $\mathfrak{p}$ is

An address delivered before the February Meeting of the Society in New York on February 27, 1960 by invitation of the Committee to Select Hour Speakers for Eastern Sectional Meetings; received by the editors March 16, 1960.