DIOPHANTINE PROBLEMS IN GEOMETRY AND ELLIPTIC TERNARY FORMS

By Gerald B. Huff

It is a familiar fact that many interesting questions in diophantine analysis occur in a natural way in elementary geometry and that some of these remain unanswered [1]. In particular, for a, b rational numbers such that $a^2 \neq b^2$, consider the problem of determining:

(a) the rational points on the ellipse, $x = a \cos \theta$, $y = b \sin \theta$, which are at rational distances from the center;

(b) the rational values of x for which $(x, 0)$ is at rational distances from $(0, \pm a)$ and $(0, \pm b)$; or

(c) the solutions of the indeterminate trigonometric equation, $a \tan \theta = b \tan \phi$, in angles θ, ϕ whose sines and cosines are rational.

It is clear that (a) and (b) are each equivalent to (c). From the formula $2rs/(r^2 - s^2)$ for the tangent of an angle with rational sine and cosine, problem (c) is equivalent to determining the rational points of the elliptic cubic

$$C(z): \qquad az_1(z_2^2 - z_3^2) - bz_2(z_1^2 - z_3^2) = 0.$$

Poincaré [5], Hurwitz [3], Mordell [4], and others [6], [7], [9] have proved a number of theorems concerning the rational solutions of $F(z_1, z_2, z_3) = 0$; where $F = 0$ represents a plane elliptic cubic with coefficients in an algebraic field k and a point (z_1, z_2, z_3) is said to be *rational* if z_1, z_2, z_3 are proportional to numbers in k. If P and Q are rational points of $F = 0$, distinct or not, the third intersection of the line PQ with the cubic is also rational. When $P = Q$, this point is the *tangential* of P. A set S of rational points of $F = 0$ is said to be *complete* if for each P, Q in S, the line PQ meets $F = 0$ in a point of S. If all the points of S may be constructed from $P_1, P_2, \cdots, P_r$, then $P_1, P_2, \cdots, P_r$ is said to form a *basis* for S. If S has a basis of r points, but no basis of $r - 1$ points, then r is said to be the rank of S. The set of all rational points of $F = 0$ is a complete set and its rank is the *rank of the cubic*. The celebrated result of Mordell [4] is that the rank of any elliptic cubic is finite.

In this article, the cubics of type $C(z)$ are given a geometric characterization and studied for different fields. The principal tool is the rather stringent arithmetical conditions imposed on a point that it be the tangential of a rational point. When k is the field of rational numbers, there are several specific results, including a necessary and sufficient condition that C have an infinite number of rational points. Finally, applications are made to the problems in geometry.

Received January 21, 1948; presented to the American Mathematical Society, December 30, 1947.