PACIFIC JOURNAL OF MATHEMATICS
Vol. 43, No. 1, 1972

THE DIOPHANTINE PROBLEM $Y^2 - X^3 = A$ IN A POLYNOMIAL RING

DENNIS L. JOHNSON

Let $C[z]$ be the ring of polynomials in z with complex coefficients; we consider the equation $Y^2 - X^3 = A$, with $A \in C[z]$ given, and seek solutions of this with $X, Y \in C[z]$ i.e. we treat the equation as a "polynomial diophantine" problem. We show that when A is of degree 5 or 6 and has no multiple roots, then there are exactly 240 solutions (X, Y) to the problem with $\deg X \leqq 2$ and $\deg Y \leqq 3$.

It is possible that, A being of degree 6, solutions (X, Y) exist with $\deg X > 2$ or $\deg Y > 3$. We "normalize" the problem so as to remove these from our consideration, and give the following definitions: if A is any polynomial of degree d, we shall permit its *formal degree* to be any integer *divisible by* 6 and greater or equal to d. Given A of formal degree $6k$, we require the solutions X, Y of the equation to be of formal degrees $2k, 3k$ resp., i.e. $\deg X \leqq 2k$, $\deg Y \leqq 3k$. This problem will be called the *problem of order* k. The restriction on the degrees of X, Y causes no loss in generality, for if k is chosen large enough, it will exceed $1/2 \deg X$ and $1/3 \deg Y$. Furthermore, the classification by k has a natural geometric interpretation. We confine our attention to the problem of order 1. The order restriction enables us to projectivize the equation to an equation of degree $6k$, with $\deg A = 6k$, $\deg X = 2k$, $\deg Y = 3k$.

Suppose then that A has formal degree 6, and (X, Y) is a solution of proper formal degree, $\deg X \leqq 2$, $\deg Y \leqq 3$. The projective curve $K: w^3 - 3Xw + 2Y = 0$ has the z-discriminant $Y^2 - X^3 = A$, so the function $z: K \to S^2$ (proj. line) has its branches among the roots of A, for finite z. At $z = \infty$ we introduce $\tilde{z} = 1/z$, $\tilde{w} = w/z = \tilde{z}w$ and get

$$\tilde{z}^3 w^3 - 3\tilde{z}^3 X\left(\frac{1}{\tilde{z}}\right)w + 2\tilde{z}^3 Y\left(\frac{1}{\tilde{z}}\right) = 0 :$$

If $X = a_0 z^2 + \cdots$, $Y = b_0 z^3 + \cdots$, then

$$F = \tilde{w}^3 - 3(a_0 + a_1\tilde{z} + a_2\tilde{z}^2)\tilde{w} + 2(b_0 + b_1\tilde{z} + \cdots) = 0$$

and

$$\frac{\partial F}{\partial \tilde{w}} 3\tilde{w}^2 - 3(a_0 + \cdots) .$$

Now at $\tilde{z} = 0$ (i.e. $z = \infty$) z has a branch point if and only if $\partial F/\partial \tilde{w} = 0$;