ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 22, Number 1, Winter 1992

A GENERALIZATION OF A RESULT OF HURWITZ AND MORDELL ON THE TORSION SUBGROUPS OF CERTAIN ELLIPTIC CURVES

CHRIS CALDWELL

1. Introduction. Let k be an algebraic number field. For any elements a, b, c, d of k with $abc(d^3 - 27abc) \neq 0$, define an irreducible nonsingular cubic curve (over the field of complex numbers) by

$$F : aX^3 + bY^3 + cZ^3 = dXYZ.$$

Whenever the set of k-rational points $F(k)$ (points P in the projective plane with $P = (x, y, z)$ for some integers x, y, z of k) is not empty, F is an elliptic curve over k and $F(k)$ is an abelian group. We consider the problem of finding the torsion subgroup of $F(k)$. We also give an infinite family of elliptic curves over the rational numbers $\mathbf{Q}$ with rank at least two.

The rank of these curves has been very well studied, see [**1, 2, 3, 6, 12, 13, 14, 16**]. Yet previously the only general result about the torsion subgroup of $F(k)$, denoted here by $\operatorname{tor}(F(k))$, were the theorems of Hurwitz [**8**] and Mordell [**10,11**]. These authors did not use the modern language of elliptic curves, but their results may be written as follows

Theorem 1.1. (Hurwitz-Mordell) *Let a, b and c be squarefree nonzero rational integers, relatively prime in pairs. Let d be an integer such that $d^3 \neq 27abc$. Suppose that $F(\mathbf{Q})$ is not empty, and make F an elliptic curve over k by choosing any element of $F(\mathbf{Q})$ as the origin of F.*

(i) *If at most one of a, b, c is ± 1, then the only torsion point is the origin and the rank of $F(\mathbf{Q})$ is positive.*

(ii) *If $a = b = 1$, $c \neq \pm 1$, then $F(\mathbf{Q})$ has one or three torsion points. $F(\mathbf{Q})$ has three torsion points if and only if $d = c \pm 2$ or $4c \pm 1$.*

(iii) *If $a = b = c = 1$ and $d \neq -1, 5$, then $F(\mathbf{Q})$ has three torsion points.*

Received by the editors on October 15, 1988.