BULLETIN OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 81, Number 1, January 1975

DIOPHANTINE EQUATIONS AND MODULAR FORMS

BY A. P. OGG

An *elliptic curve* over a field K may be defined to be a nonsingular projective plane cubic curve in standard form, which for characteristic $\neq 2, 3$ is

$$E: y^2 = 4x^3 - g_2x - g_3, \tag{1}$$

where $g_2, g_3 \in K$; that E is nonsingular means that the discriminant $\Delta = g_2^3 - 27g_3^2$ is not 0. (A slightly modified cubic equation is required in characteristic 2 or 3.) E has a natural group law, written additively, with the unique point at infinity, $0 = (\infty, \infty)$, as zero, defined by the rule that three points on E add up to 0 if and only if they are collinear. E is then an abelian variety of dimension 1 defined over K. Let $E(K)$ denote the group of points of E with coordinates in K.

Over $K = \boldsymbol{C}$, the field of complex numbers, if we are given a complex torus $\boldsymbol{C}/L$, where $L = \boldsymbol{Z}\omega_1 \oplus \boldsymbol{Z}\omega_2$ is a lattice, then we have an analytic isomorphism

$$\begin{aligned} \boldsymbol{C}/L &\cong E: y^2 = 4x^3 - g_2x - g_3, \\ u &\mapsto (x, y) = (\wp(u), \wp'(u)) \end{aligned} \tag{2}$$

defined by the Weierstrass $\wp$-function. Here g_2 and g_3 depend on the lattice L. The isomorphism carries the natural group law on $\boldsymbol{C}/L$ onto the above geometrically defined group law on E, by the addition theorem for the $\wp$-function. Viewing E as $\boldsymbol{C}/L$, it is clear that the group of N-division points, $E_N = \{P \in E: N \cdot P = 0\}$, is isomorphic to $C_N \times C_N$, where C_N is the cyclic group of order N.

If $K = \boldsymbol{Q}$ is the field of rational numbers, then, by a celebrated theorem of Mordell, the group $E(\boldsymbol{Q})$ is finitely generated:

$$E(\boldsymbol{Q}) = \boldsymbol{Z}^r \times F, \tag{3}$$

where $F = E(\boldsymbol{Q})^t$, the torsion subgroup of $E(\boldsymbol{Q})$, is finite. In practice, for a given elliptic curve E, one can determine the torsion subgroup F rather

---

A talk presented to the American Mathematical Society at its November, 1973 meeting in Tucson. This paper was written in June, 1974, and contains some things which were not known at the time of the meeting; received by the editors June 28, 1974.

AMS (MOS) subject classifications (1970). Primary 10B02, 10D10, 14G05.

Key words and phrases. Elliptic curve, modular curve, rational torsion, descent, Jacobian, isogeny, involution.