Miyawaki, I.
Osaka J. Math.
10 (1973), 309-323

ELLIPTIC CURVES OF PRIME POWER CONDUCTOR WITH Q-RATIONAL POINTS OF FINITE ORDER

ISAO MIYAWAKI

(Received August 4, 1972)

Introduction

Let $\boldsymbol{E}$ be an elliptic curve (an abelian variety of dimension one) defined over the rational number field $\boldsymbol{Q}$. After Weil [9], we can define the conductor of $\boldsymbol{E}$. But, in general, it would be difficult to find all the curves of given conductor. But it seems to be easier to find all the curves of given conductor having $\boldsymbol{Q}$-rational points of finite order >2.

In this paper we determine all the curves of prime power conductor which have at least three rational points of finite order. There are only finitely many such curves up to $\boldsymbol{Q}$-isomorphism. They are listed in the table at the end of the paper.

Since each of them has $\boldsymbol{Q}$-rational points of finite order, we can take a special cubic equation as a global minimal model for it. Further, since that curve has a prime power conductor, the coefficients of that equation must be a solution of a certain diophantine equation. Therefore, the determination of such curves is reduced to elementary diophantine problems.

Some of them have no complex multiplication and non-integral invariants. Let $\boldsymbol{E}$ be one of them and $\boldsymbol{Q}(\boldsymbol{E}_n)$ be the field generated by the coordinates of the n-division points of $\boldsymbol{E}$ over $\boldsymbol{Q}$. Then we can determine the Galois group of $\boldsymbol{Q}(\boldsymbol{E}_l)$ over $\boldsymbol{Q}$ for all prime l.

1. Integrality of rational points of finite order

Let $\boldsymbol{E}$ be an elliptic curve defined over $\boldsymbol{Q}$. A Weierstrass model for $\boldsymbol{E}$ over $\boldsymbol{Q}$ is plane cubic equation of the form

$$y^2+a_1xy+a_3y+x^3+a_2x^2+a_4x+a_6=0 \tag{1}$$

with $a_j\in\boldsymbol{Q}$, the zero of $\boldsymbol{E}$ being the point at infinity. We define auxiliary quantities by

$$\beta_2=a_1^2-4a_2$$
$$\beta_4=2a_4-a_1a_3$$