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

$$(1)\qquad y^2+a_1xy+a_3y+x^3+a_2x^2+a_4x+a_6=0$$

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

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

$$\beta_6 = a_3^2 - 4a_6$$
$$\beta_8 = a_4^2 - a_1a_3a_4 + a_1^2a_6 + a_2a_3^2 - 4a_2a_6 \,.$$

The discriminant Δ is defined by

$$\Delta = \beta_2^2\beta_8 - 8\beta_4^3 - 27\beta_6^2 + 9\beta_2\beta_4\beta_6$$

and the invariant J is defined by

$$J = (\beta_2^2 - 24\beta_4)^3/\Delta \,.$$

This model is minimal at a prime p if each a_j is integral at p, and $\mathrm{ord}_p(\Delta)$ is as small as possible. Since the ring $\boldsymbol{Z}$ of rational integers is a principal ideal domain, it is easy to see that we can find a global minimal Weierstrass model for $\boldsymbol{E}$ over $\boldsymbol{Q}$, i.e., a cubic equation as above with each $a_j \in \boldsymbol{Z}$, which is simultaneously minimal at all p. For a detailed discussion of minimal models of elliptic curves, see Néron [2]. It should be noted that the conductor N of $\boldsymbol{E}$ and the discriminant Δ of the global minimal model for $\boldsymbol{E}$ have same prime divisors.

Lemma 1. *Suppose that each a_j is a rational integer in* (1). *If $t_0 = (x_0, y_0)$ is a rational point on* (1) *of finite order $m > 2$, then x_0 and y_0 are integers.*

Proof. After the transformation

$$(2) \qquad \begin{aligned} 6^2x &= X + 3a_1^2 - 12a_2 \\ 6^3y &= Y - 3a_1(X + 3a_1^2 - 12a_2) - 4\cdot 3^3a_3 \,, \end{aligned}$$

we get

$$(3) \qquad Y^2 + X^3 + AX + B = 0$$

where

$$\begin{aligned} A &= 3(3a_1^2 - 12a_2)^2 + 2(6^2a_2 - 3^2a_1^2)(3a_1^2 - 12a_2) + 6^4a_4 - 2^3\cdot 3^4a_1a_3 \\ B &= (3a_1^2 - 12a_2)^3 + (6^2a_2 - 3^2a_1^2)(3a_1^2 - 12a_2)^2 + 6^6a_6 - 2^4\cdot 3^6a_3^2 \\ &\quad + (6^4a_4 - 2^33^4a_1a_3)(3a_1^2 - 12a_2). \end{aligned}$$

Hence $3^3 | A$, $3^3 | B$ and $4A^3 + 27B^2 = -2^8\cdot 3^{12}\Delta$.
Let (X_0, Y_0) be the transform of (x_0, y_0) by (2). Then by Theorem 22.1 of Cassels [1] X_0 and Y_0 are integers. Hence 6^2x_0 and 6^3y_0 are integers. By the assumption we have $Y_0 \neq 0$. So the tangent of (3) at $(X_0. Y_0)$ is

$$Y - Y_0 = -(3X_0^2 + A)(2Y_0)^{-1}(X - X_0) \,.$$

Put $(X_1, Y_1) = -2(X_0, Y_1)$, then X_1 and Y_1 are also integers, and we have

$$(4) \qquad (3X_0^2 + A)^2/(2Y_0)^2 = -(2X_0 + X_1) \,.$$

Hence

$$(5) \qquad (3X_0^2+A)/(2Y_0)\in Z\,.$$

First, we shall show that $\mathrm{ord}_2(x_0)$ and $\mathrm{ord}_2(y_0)$ are non-negative. If X_0 is odd, then A is odd by (5), so is a_1. Hence 6^2x_0 is even by (2). If X_0 is even, then A is even by (5), so is a_1. Hence 6^2x_0 is even by (2). In either case, we have $\mathrm{ord}_2(x_0)\geqslant -1$. Multiplying (1) by 2^4, we see that 2^2y_0 is integral at 2, hence $\mathrm{ord}_2(y_0)\geqslant -2$. Hence $\mathrm{ord}_2(y_0^2)\geqslant -3$ by (1), i.e., $\mathrm{ord}_2(y_0)\geqslant -1$. This implies $\mathrm{ord}_2(x_0^3)\geqslant -2$, i.e., $\mathrm{ord}_2(x_0)\geqslant 0$ and $\mathrm{ord}_2(y_0)\geqslant 0$.

Next, we shall show that $\mathrm{ord}_3(x_0)$ and $\mathrm{ord}_3(y_0)$ are non-negative. If we suppose $X_0\not\equiv 0 \bmod 3$, then $Y_0\not\equiv 0 \bmod 3$ by (3), hence $X_0\equiv -1 \bmod 3$. Hence we have $X_1\equiv -1 \bmod 3$ by (4). Further we can easily see $X_0\neq X_1$ by (4). The points $-(X_0, Y_0)-(X_1, Y_1)$ and $-(X_0, Y_0)-(X_1, -Y_1)$ on (3) are also integral. Hence, by the same reasoning as above, we have

$$(Y_0-Y_1)/(X_0-X_1)\in Z$$
$$(Y_0+Y_1)/(X_0-X_1)\in Z\,.$$

Since $X_0-X_1\equiv 0 \bmod 3$, we have

$$Y_0-Y_1\equiv Y_0+Y_1\equiv 0 \bmod 3 \text{ i.e. } Y_0\equiv 0 \bmod 3\,,$$

which is a contradiction. Hence $X_0\equiv 0 \bmod 3$ i.e., $\mathrm{ord}_3(x_0)\geqslant -1$ by (2). By the same method as above we have $\mathrm{ord}_3(x_0)\geqslant 0$ and $\mathrm{ord}_3(y_0)\geqslant 0$. This completes the proof of the lemma.

REMARK. Assumption being as in Lemma 1, we obtain the x-coordinates of 2-division points on (1) as the roots of the equation

$$(a_1x+a_3)^2-4(x^3+a_2x^2+a_4x+a_6)=0$$

Hence, if (x_0, y_0) is a rational point on (1) of order 2, then we have $2^2x_0\in \boldsymbol{Z}$ and $2^3y_0\in \boldsymbol{Z}$. Moreover, if the other 2-division points, say (x_1, y_1) and (x_2, y_2), are also rational points, then we have

$$x_0x_1x_2=-(a_6-a_3^2/4)\,.$$

Hence, at least one of them is an integral point.

Lemma 2. *Let $\boldsymbol{E}$ be an elliptic curve defined over a finite field k with q-elements and N be the number of k-rational points of $\boldsymbol{E}$.*

Then we have

$$N=1-a+q\,,$$

where

$$|a| \leqslant 2\sqrt{q}\ .$$

This is the "Riemann hypothesis" for elliptic curves.

2. Determination of curves of prime power conductor with Q-rational points of finite order

In this section, we shall determine all the elliptic curves of prime power conductor having at least three rational points of finite order. Since all the curves of 2-power conductor have been determined in Ogg [3], we shall deal with the curves of odd prime power conductor. So we shall always mean by p an odd prime integer. Let E be such a curve and F be the group of rational points of finite order on E. By Mordell-Weil theorem, F is a finite group. Let $E(l)$ be the reduction of E at a prime l. Since E has a good reduction at 2, $E(2)$ is also an elliptic curve defined over the field $GF(2)$. Hence $E(2)$ has at most five $GF(2)$-rational points by Lemma 2. It is well-known that the reduction map of F into the group of $GF(2)$-rational points on $E(2)$ is a homomorphism and the order of its kernel is 2-power. Therefore the order of F is 2^λ, $2^\lambda\cdot 3$ or $2^\lambda \cdot 5$.

As was shown in Ogg [3], we note that there is no curve with $\Delta=\pm 1$.

Theorem 1. *There are nine elliptic curves having rational points of order* 3 *and they have no rational point of order* 2.

Proof. Let E be such a curve and (1) be a global minimal model of E. By Lemma 1, we may assume that $a_6=0$ and $t=(0, 0)$ is a point of order 3, hence a_3 is not zero. Since $2(0,0)+(0,0)=0$, we have

$$(-a_4/a_3)^2+a_1(-a_4/a_3)+a_2 = 0\ .$$

Hence a_4/a_3 is an integer. Put $a_4=a_3a_4'$, then

$$\Delta = a_3^3\{-8(2a_4'-a_1)^3-27a_3+9(a_1^2-4a_2)(2a_4'-a_1)\}\ .$$

By $\Delta=\pm p^m$, we see that a_3 is odd. Hence a_1 is even. Hence by the transformation $y\to y-(a_1/2)x$, we can take $a_1=0$. Hence we get the global minimal model of E of the form

$$y^2+a_3y+x^3+a_2x^2+a_3a_4x = 0 \tag{6}$$

with

$$a_j \in Z$$
$$a_4^2+a_2 = 0\ , \quad \Delta = a_3^3(8a_4^3-27a_3) = \pm p^m\ , \quad a_3>0\ .$$

(I) The case $a_3=1$

In this case, we have

$$8a_4^3-27=(2a_4-3)(4a_4^2+6a_4+9)=\pm p^m$$

If $2a_4-3=\pm 1$, then we get $a_4=1$ or 2, curves 1, 2. Next we shall consider the cases $2a_4-3=\pm p^n$ $(n>0)$. If $p\neq 3$ we have $a_4\not\equiv 0 \bmod p$, hence $4a_4^2+6a_4+9=(2a_4-3)^2+18a_4=\pm 1$. This contradicts with $a_4\in \boldsymbol{Z}$. Hence $p=3$. If $n=1$, then we get

$$2\mathrm{a}_4=3\pm 3\,,\quad (2a_4-3)^2+18a_4=9(1+3\pm 3)=\pm 3^{m'}\,.$$

Hence we get $a_4=0$, the curve 3. If $n=2$, then we have

$$2a_4=3\pm 9\,,\quad (2a_4-3)^2+18a_4=27(3+1\pm 3)=\pm 3^{m'}\,.$$

Hence we get $a_4=-3$, the curve 4. If $n\geqslant 3$, then we have

$$2a_4=3\pm 3^n\,,\quad (2a_4-3)^2+18a_4=3^{2n}+9(3\pm 3^n)=\pm 3^{m'}\,.$$

But this is impossible.

(II) The case $a_3=p$

First, we shall consider the case $p=3$. Then we have

$$8a_4^3-3^4=\pm 3^{m'}\,.$$

If $m'=0$, then $8a_4^3-3^4=\pm 1$. But this is impossible. Hence a_4 is divisible by 3. Put $a_4=3a_4'$, then we have

$$8a_4'^3-3=\pm 3^{m''}\,.$$

If $m''=0$, then $8a_4'^3=3\pm 1$. This is impossible. Hence a_4' is divisible by 3. Put $a_4'=3a_4''$, then we have

$$8\cdot 3^2 a_4''^3-1=\pm 1\,.$$

Hence we get $a_4=0$, the curve 5.

Next, we shall consider the case $p\neq 3$. If a_4 were divisible by p, we would have

$$8(a_4/p)^3p^2-27=\pm 1\,.$$

But this is impossible. Hence $8a_4^3-27p=\pm 1$, and we have

$$27p=8a_4^3\pm 1=(2a_4\pm 1)\{(2a_4\pm 1)^2\mp 6a_4\}\,.$$

If $2a_4\pm 1$ is divisible by p, then we get $(2a_4\pm 1)^2\mp 6a_4=\pm 3, \pm 9$. This implies $2a_4\pm 1=\pm 3$. But this contradicts with $2a_4\pm 1\equiv 0 \bmod p$. Hence $2a_4\pm 1$ is not divisible by p. This implies $2a_4\pm 1=\pm 3, \pm 9$. We can easily see $2a_4\pm 1=9$, then we get curves 6,7.

(III) The case $a_3=p^2$

First, we shall consider the case $p\neq 3$. If a_4 were divisible by p, we would have

$$8(a_4/p)^3p-27=\pm 1\,.$$

But this is impossible. Hence a_4 is not divisible by p, i.e., $8a_4^3-27p^2=\pm 1$. Hence we get $27p^2=8a_4^3\pm 1=(2a_4\pm 1)\{(2a_4\pm 1)^2\mp 6a_4\}$. But we can easily see by the same method as in (II) that this is impossible. So we suppose $p=3$. Then we have

$$8a_4^3-3^5=\pm 3^{m'}\,.$$

It can be easily seen that m' is not zero. Put $a_4=3a_4'$. Then we have

$$8a_4'^3-3^2=\pm 3^{m''}\,.$$

If $m''=0$, then we get $a_4'=1$, the curve 8. If $m''>0$, put $a_4'=3a_4''$, then we have

$$3\cdot 8a_4''^3-1=\pm 1\,.$$

Hence we get $a_4''=0$, the curve 9.

(IV) The case $a_3=p^n$ $(n\geqslant 2)$

If a_4 is divisible by p, then a_2 is divisible by p^2. But this implies that (6) is not a minimal model. Hence we have $8a_4^3-27p^n=\pm 1$, i.e., $27p^n=(2a_4\pm 1)\{(2a_4\pm 1)^2\mp 6a_4\}$. If we suppose $p=3$, then we have

$$3^{3+n}=(2a_4\pm 1)\{(2a_4\pm 1)^2\mp 6a_4\}\,.$$

Hence we get $(2a_4\pm 1)^2\mp 6a_4=\pm 3$. But this contradicts with $n\geqslant 3$. Hence we may assume $p\neq 3$. Then we have $2a_4\pm 1=\pm 3$, ± 9 or $(2a_4\pm 1)^2\mp 6a_4=\pm 3$, ± 9. But we can easily see that this also contradicts with $n\geqslant 3$.

Next, we shall show that E has no rational point of order 2. Suppose (x_0, y_0) be a rational point on (6) of order 2. Then x_0 is a root of the equation $a_3^2-4(x_0^3+a_2x_0^2+a_3a_4x_0)=0$, Put $2x_0=X_0$, then $X_0^3+2a_2X_0^2+4a_3a_4X_0-2a_3^2=0$. Hence X_0 is an even integer. This implies that a_3 is even. But this is a contradiction. This completes the proof of Theorem 1.

Theorem 2. *There are only two elliptic curves which have three rational points of order* 2, *and they have no other rational point of finite order except zero.*

Proof. Let (1) be a global minimal model of such a curve, then by the Remark we may assume $a_3=a_6=0$, i.e.,

$$y^2+a_1xy+x^3+a_2x^2+a_4x=0\,, \tag{7}$$

then we have

$$(8) \qquad \Delta = a_4^2\{(a_1^2-4a_2)^2-2^6a_4\} = \pm p^m .$$

By the assumption, the equation $(a_1x)^2-4(x^3+a_2x^2+a_4x)=0$ has three rational roots. Hence we get

$$(a_1^2-4a_2)^2-2^6a_4 = r^2 \quad \text{with some} \quad r\in \boldsymbol{Q} .$$

By (8) we get $r=p^n$. Hence we have

$$(9) \qquad 2^6a_4 = (a_1^2-4a_2-p^n)(a_1^2-4a_2+p^n) .$$

If we replace y by $y+ax$, then a_1 is replaced by a_1+2a. By (8) we see that a_1 is odd, so we can take a_1 to be an arbitrary odd integer.

(I) The case $n=0$

We get $\Delta=a_4^2$ and $2^6a_4=(a_1^2-4a_2-1)(a_1^2-4a_2+1)$, hence we have

$$\begin{aligned} a_1^2-4a_2-1 &= \pm 32p^\alpha \\ a_1^2-4a_2+1 &= \pm 32p^\alpha+2 = \pm 2p^\beta \end{aligned}$$

If we suppose $\alpha>0$, then we get $\pm 16p+1=\pm 1$. But this is impossible. Hence, by $\pm 16+1=\pm p^\beta$, we get $p=17$. Then we get the curve 10 by taking $a_1=1$.

(II) The case $n=1$

First, we shall consider the case $p\equiv 1 \bmod 4$, then by (9) we have

$$\begin{aligned} a_1^2-4a_2-p &= \pm 32p^\alpha \\ a_1^2-4a_2+p &= \pm 32p^\alpha+2p = \pm 2p^\beta \end{aligned}$$

If $\alpha=0$, then $\pm 16+p=\pm 1$. Hence we get $p=17$ and $a_4=-1$ by taking $a_1=1$. But we can easily see that this curve is isomorphic to the curve 10 over $\boldsymbol{Q}$. If $\alpha=1$, then $\pm 16+1=p^{\beta'}$. Hence we get $p=17$, the curve 11 by taking $a_1=1$. If $\alpha\geqslant 2$, then $\pm 16p^{\alpha-1}+1=\pm 1$. But this is impossible.

Next, we shall consider the case $p\equiv 3 \bmod 4$, then by (9) we have

$$\begin{aligned} a_1^2-4a_2-p &= \pm 2p^\alpha \\ a_1^2-4a_2+p &= \pm 2p^\alpha+2p = \pm 32p^\beta . \end{aligned}$$

By the same method as above, we obtain $\alpha=2$ and $p=17$. But this contradicts with $p\equiv 3 \bmod 4$.

(III) The case $n\geqslant 2$

Put $a_4=\pm p^\alpha$. If $\alpha\geqslant 3$, then by (9) $a_1^2-4a_2\equiv 0 \bmod p^2$. We may assume $\mathrm{a}_1\equiv 0$

mod p, hence $a_2 \equiv 0 \bmod p^2$. Therefore by (9) $a_4 \equiv 0 \bmod p^4$. But these imply that (7) is not a minimal model. Hence we get $0 \leqslant \alpha \leqslant 2$. If we suppose $\alpha=0$, then by (9) we get

$$\pm 2^6 = (a_1^2-4c_2-p^n)(a_1^2-4a_2+p^n)\,.$$

If $p \equiv 3 \bmod 4$ and n is odd, then we get

$$\begin{aligned} &a_1^2-4a_2-p^n = \pm 2 \\ &a_1^2-4a_2+p^n = \pm 2+2p^n = \pm 32\,. \end{aligned}$$

Hence we get $2p^n = \pm 32 \pm 2$. But this contradicts with $n \geqslant 2$. If $p \equiv 1 \bmod 4$ or n is even, then we get

$$\begin{aligned} &a_1^2-4a_2-p^n = \pm 32 \\ &a_1^2-4a_2+p^n = \pm 32+2p^n = \pm 2 \end{aligned}$$

Hence we get $2p^n = \pm 32 \pm 2$. But this also contradicts with $n \geqslant 2$. If we suppose $\alpha \geqslant 1$, then by (9) we get $\pm 2^6 p^\alpha = (a_1^2-4a_2-p^n)(a_1^2-4a_2+p^n)$. Hence we have $a_1^2-4a_2 \equiv 0 \bmod p$, and we may assume $\alpha=2$. If $p \equiv 1 \bmod 4$ or n is even, then we get

$$\begin{aligned} &a_1^2-4a_2-p^n = \pm 32p \\ &a_1^2-4a_2+p^n = \pm 32p+2p^n = \pm 2p\,. \end{aligned}$$

Hence we get $n=2$, $p=17$, $a_2=64$, and $a_4=-17^2$ by taking $a_1=1$. But we can easily see that this curve is isomorphic to the the curve 11 over $\boldsymbol{Q}$. If $p \equiv 3 \bmod 4$ and n is odd, then we get

$$\begin{aligned} &a_1^2-4a_2-p^n = \pm 2p \\ &a_1^2-4a_2+p^n = \pm 32p\,. \end{aligned}$$

This implies $p=17$. But this is a contradiction.

Since these curves have a good reduction at p for $p=3$ and $p=5$, the latter half of Theorem is obvious by Lemma 2.

Theorem 3. *There are three elliptic curves which have rational points of order* 4. *Each of them has only four rational points of finite order.*

Proof. Let $\boldsymbol{E}$ be such a curve and (1) be a global minimal model of $\boldsymbol{E}$, then by Lemma 1 we may assume that $a_6=0$ and $t=(0, 0)$ is a point of order 4. Hence $a_3 \neq 0$. Moreover, after the transformation $y \to -y$ (if necessary), we assume $a_3>0$. Put $-2t=(x_0, y_0)$. Then we have

$$\begin{aligned} &(-a_4/a_3)^2+a_1(-a_4/a_3)+a_2 = -x_0 \\ &y_0 = (-a_4/a_3)x_0\,. \end{aligned}$$

Since (x_0, y_0) is a point of order 2, we get

$$2y_0+a_1x_0+a_3 = 0\,.$$

Hence

$$-2(-a_4/a_3)\{(-a_4/a_3)^2+a_1(-a_4/a_3)+a_2\}-a_1\{(-a_4/a_3)^2+a_1(-a_4/a_3) \\ +a_2\}+a_3 = 0\,.$$

This shows that $2a_4/a_3$ is an integer. Put

$$(10) \qquad 2a_4 = a_3a_4'\,,$$

then

$$(11) \qquad (a_4'-a_1)(a_4'^2-2a_1a_4'+4a_2)+4a_3 = 0\,.$$

Put

$$(12) \qquad \begin{aligned} a_4'-a_1 &= \alpha \\ a_4'^2-2a_1a_4'+4a_2 &= \beta\,, \end{aligned}$$

then

$$(13) \qquad \alpha\beta+4a_3 = 0$$

$$(14) \qquad a_1^2-4a_2 = \alpha^2-\beta\,.$$

Hence we get

$$\begin{aligned} \Delta &= a_3^2\{(\alpha^2-\beta)^2\beta/4+2\alpha^4\beta-27(-\alpha\beta/4)^2+9(-\alpha\beta/4)\alpha(\alpha^2-\beta)\} \\ &= a_3^2\beta^2(\alpha^2+4\beta)/16\,. \end{aligned}$$

(I) The case a_4' is even

By (12), β is divisible by 4. Put $\beta=4\beta'$, then we have

$$\Delta = a_3^2\beta'^2(\alpha^2+16\beta') = \pm p^m\,.$$

First, we shall consider the cases $\beta'=\pm 1$, then by (13) we get $a_3=\pm\alpha$. Hence

$$\Delta = \mathrm{a}_3^2(\mathrm{a}_3^2\pm 16) = \pm p^m\,.$$

If a_3 is divisible by p, then $a_3^2\pm 16=\pm 1$. But this is impossible. Hence $a_3=\pm 1$. Therefore we may assume $a_3=1$ and $a_1=1$. Hence we get the curve 12. Next, we shall consider the cases $\beta'=\pm p^n$ with $n>0$. If $\alpha=\pm 1$, then by (13) $\beta'=\mp a_3$. Hence we get $\Delta=a_3^4(1\mp 16a_3)$, so $1\mp 16a_3=\pm 1$. But this is impossible. Hence we may assume $\alpha\equiv 0 \bmod p$ and $a_1\equiv 0 \bmod p$, then by (12) we have $a_4'\equiv 0 \bmod p$. If β' is divisible by p^2, then by (12) we see that a_2 is divisible by p^2. Hence we get $a_3\equiv 0 \bmod p^3$ by (13) and $a_4\equiv 0 \bmod p^4$ by (10). But this contradicts with the fact that (1) is a minimal model of $\boldsymbol{E}$. Hence we get

$\beta' = \pm p$ and $\alpha \equiv 0 \bmod p$, so

$$\Delta = a_3^2 p^2(\alpha^2 \pm 16p) = \pm p^m .$$

By (13) we may put $\alpha = \pm p^{m'}$ with $m' > 0$, then we get $p^{2m'-1} \pm 16 = \pm 1$, so $p = 17$, the curve 13 by taking $a_1 = 17$.

(II) The case a_4' is odd

By (10), (12), (13), we see that a_3 is even and α is divisible by 8. Put $a_3 = 2a_3'$ and $\alpha = 8\alpha'$, then we have

$$\Delta = a_3'^2 \beta^2 (16\alpha'^2 + \beta) = \pm p^m .$$

First, we shall consider the cases $\beta = \pm 1$. By looking at (14) modulo 4 we have $\beta = -1$, then by (13) $\alpha' = a_3'$. Hence we have

$$\Delta = a_3'^2 (16 a_3'^2 - 1) = \pm p^m .$$

Therefore a_3' is not divisible by p, so we assume $a_3' = 1$. But this is impossible. Next, we shall consider the case $\beta \equiv 0 \bmod p$. If $\alpha' = \pm 1$, then $\beta = \mp a_3'$. Hence we have

$$\Delta = a'^4_3 (16 \mp a_3') = \pm p^m .$$

Hence we get $a_3' = p = 17$, the curve 14. If α' is divisible by p, then we may assume that β is not divisible by p^2. For if β is divisible by p^2, then we get $a_4' \equiv 0 \bmod p$ by (12), $a_2 \equiv 0 \bmod p^2$ by (12), $a_3 \equiv 0 \bmod p^3$ by (13) and $a_4 \equiv 0 \bmod p^4$ by (10) by taking $a_1 = p$. But this contradicts with the fact that (1) is a minimal model of $\boldsymbol{E}$. Hence we have $\beta = \pm p$ and $\Delta = p^2 a_3'^2 (16 p^{m'} \pm p)$ with $m' \geqslant 2$. Hence we have

$$16 p^{m'-1} \pm 1 = 1 .$$

But this is impossible.

The latter half of Theorem 3 is immediate by the same reasoning as in the proof of Theorem 2.

Theorem 4. *There are only two elliptic curves which have rational points of order* 5, *and then they have no rational point of order* 2.

Proof. Let $\boldsymbol{E}$ be such a curve and (1) be a global minimal model of $\boldsymbol{E}$. By the lemma 1 we may assume $a_6 = 0$ and $t = (0, 0)$ be a point on (1) of order 5. Hence $a_3 \neq 0$ and $-t = (0, -a_3)$. Put $-2t = (x_0, y_0)$, then x_0 and y_0 are integers, and we have

$$(-a_4/a_3)^2 + a_1(-a_4/a_3) + a_2 = -x_0 .$$

Hence a_4/a_3 is an integer. Put $a_4 = a_3 a_4'$, then we have

$$\begin{aligned}\Delta &= a_3^2\{(a_1^2-4a_2)^2(a_4'^2-a_1a_4'+a_2)-8a_3(2a_4'-a_1)^3-27a_3^2+9a_3(a_1^2-4a_2)(2a_4'-a_1)\} \\ &= \pm p^m .\end{aligned}$$

Put $2t=(x_0, y_0')$, then $a_1x_0+a_3=-(y_0+y_0')$. Let $\boldsymbol{E}(2)$ be the reduction of $\boldsymbol{E}$ at 2, then $\boldsymbol{E}(2)$ has just five $GF(2)$-rational points and they are the reductions of $\{nt \mid n=1, 2, 3, 4, 5\}$. Since $t \bmod 2=(0, 0)$ and $-t \bmod 2=(0, 1)$, we have either $2t \bmod 2=(1, 0)$, $-2t \bmod 2=(1, 1)$ or $2t \bmod 2=(1, 1)$, $-2t \bmod 2=(1, 0)$. In either case, we get $y_0+y_0'\equiv 1 \bmod 2$, i.e., $a_1x_0+a_3\equiv 1 \bmod 2$. Since a_3 and x_0 are odd, a_1 must be even. Hence we may assume $a_1=0$. Hence we can assume that

$$(15) \qquad y^2+a_3y+x^3+a_2x^2+a_3a_4x = 0$$

is a global minimal model of $\boldsymbol{E}$; and we have

$$\Delta = a_3^2\{16a_2^2(a_2+a_4^2)-64a_3a_4^3-27a_3^2-72a_2a_3a_4\} ,$$

and $t=(0, 0)$, $-t = (0, -a_3)$, $-2\text{t}=(-(a_2+a_4^2), a_4(a_2+a_4^2))$.
After a suitable translation, if necessary, we may assume that a_3 and $a_2+a_4^2$ are positive. By the assumption, the tangent of $\boldsymbol{E}$ at the point $-2t$ intersects $\boldsymbol{E}$ at the point $-t$. Hence we get

$$(16) \quad \frac{a_4(a_2+a_4^2)+a_3}{-(a_2+a_4^2)} = -\frac{3x_0^2+2a_2x_0+a_3a_4}{2y_0+a_3} = -\frac{3(a_2+a_4^2)^2-2a_2(a_2+a_4^2)+a_3a_4}{2a_4(a_2+a_4^2)+a_3} .$$

By the same reasoning as before this is an integer. Hence $a_2+a_4^2$ divides a_3. Put $a_3=a_3'(a_2+a_4^2)$, then we have by (16)

$$a_4+a_3' = \frac{3(a_2+a_4^2)-2a_2+a_3'a_4}{2\text{a}_4+a_3'} .$$

Hence

$$(17) \qquad a_2+a_4^2 = a_3'(2a_4+a_3') .$$

First we shall consider the case $a_3'=1$. By (17), $a_2+a_4^2=2a_4+1=a_3$, hence we get

$$\begin{aligned}2a_4 &= a_3-1 \\ 4a_2 &= 4a_3-(2a_4)^2 = -a_3^2+6a_3-1 ,\end{aligned}$$

and consequently

$$\begin{aligned}\Delta &= a_3^2\{(-a_3^2+6a_3-1)^2a_3-8a_3(a_3-1)^3-27a_3^2-9a_3(a_3-1)(-a_3^2+6a_3-1)\} \\ &= a_3^5(a_3^2-11a_3-1) = \pm p^m .\end{aligned}$$

Therefore we have $a_3=1$ or $a_3^2-11a_3-1=\pm 1$. Hence we get $a_3=1$, 11, curves 15, 16. Next, we shall consider the case $\text{a}_3'=p^{n'}$ with $n'>0$. Then by (17) we have $a_3=(a_2+a_4^2)a_3'=a_3'^2(2a_4+a_3')$. If we suppose $2a_4+a_3'\equiv 0 \bmod p$, then $a_4\equiv 0 \bmod p$. Hence by (17) we get $a_3\equiv 0 \bmod p^3$ and $a_2\equiv 0 \bmod p^2$. But this contradicts with the fact that (15) is a minimal model of $\boldsymbol{E}$. Hence we get $2a_4+a_3'=1$, i.e., $a_3'^2=a_3$ and $a_2+a_4^2=a_3'$, so

$$\begin{aligned}2a_4 &= -a_3'+1\\ 4a_2 &= -a_3'^2+6a_3'-1\,.\end{aligned}$$

Hence we have

$$\begin{aligned}\Delta &= a_3'^4\{(-a_3'^2+6a_3'-1)^2a_3'-8a_3'^2(-a_3'+1)^3-27a_3'^4-9a_3'^2(-a_3'^2+6a_3'-1)\\ &\qquad (-a_3'+1)\}\\ &= a_3'^5(-a_3'^2-11a_3'+1) = \pm p^m\,.\end{aligned}$$

Therefore we have $-a_3'^2-11a_3'+1=\pm 1$. So $a_3'=-11$. But this contradicts with $a_3'>0$.

The latter half of Theorem 4 is immediate by the same reasoning as in the proof of Theorem 1.

3. Determination of the Galois group

Let $\boldsymbol{E}$ be an elliptic curve defined over $\boldsymbol{Q}$. For a prime number l, put

$$\boldsymbol{E}_l = \{t\in \boldsymbol{E}\,|\,lt=0\}\,.$$

Let $\boldsymbol{Q}(\boldsymbol{E}_l)$ be the field generated by the coordinates of the points of $\boldsymbol{E}_l$. then the field $\boldsymbol{Q}(\boldsymbol{E}_l)$ is a normal extension of $\boldsymbol{Q}$ of finite degree. Put

$$G_l = Gal(\boldsymbol{Q}(\boldsymbol{E}_l)/\boldsymbol{Q})\,.$$

Taking a basis $\{t_1, t_2\}$ of $\boldsymbol{E}_l$, we get a faithful representation R_l of the group G_l in $GL(2, \boldsymbol{Z}/l\boldsymbol{Z})$;

$$\begin{pmatrix} t_1^\sigma \\ t_2^\sigma \end{pmatrix} = R_l(\sigma)\begin{pmatrix} t_1 \\ t_2 \end{pmatrix} \qquad \text{for any} \quad \sigma\in G_l\,.$$

If the invariant of $\boldsymbol{E}$ is not an integer, then it is known that G_l is isomorphic to $GL(2, \boldsymbol{Z}/l\boldsymbol{Z})$ for almost all l (see the theorem of Serre [4] IV-20). Moreover in some cases, following Serre [4] IV-20, we can determine the (finite) set of l's with $R_l(G_l)\neq GL(2, \boldsymbol{Z}/l\boldsymbol{Z})$.

Lemma 3. *If $R_l(G_l)$ satisfies the next three conditions* a), b), c), *then $R_l(G_l)$ is equal to $GL(2, \boldsymbol{Z}/l\boldsymbol{Z})$.*

a) $\det R_l(G_l)=(\boldsymbol{Z}/l\boldsymbol{Z})^\times$.

b) *$R_l(G_l)$ contatins the element $\begin{pmatrix}1&1\\0&1\end{pmatrix}$ with respect to a suitable basis of E_l.*

c) *E_l is irreducible as G_l-module.*

Proof. See the lemma 2 of Serre [4] IV-20.

Theorem 5. *Let E be one of the curves* 1, 2, 6. 7, 10, 11, 12, 13, 14, 15, 16, *in the table at the end of the paper. If E has a Q-rational point of order l_0 ($l_0=2$, 3, or* 5), *then $R_l(G_l)=GL(2, Z/lZ)$ for every prime $l\neq l_0$.*

Proof. We shall consider the case where E is the curve 16. This is the case dealt with in Shimura [6]. In this case we have

$$\begin{aligned} E\colon & y^2+11y+x^3-14x^2+55x=0 \\ & J=-2^{12}\cdot 31^3\cdot 11^{-5}. \end{aligned}$$

Let l be a prime number not equal to 5, then $R_l(G_l)$ satisfies the condition *b*) of Lemma 3 by the lemma 1 of Serre [4] IV-20. The condition *a*) is equivalent to the fact that $Q(E_l)$ contains a primitive l-th root of unity, which is well-known. We shall show that the condition *c*) is satisfied for such l. Assume this is not the case. Then taking a suitable basis $\{t_1, t_2\}$, we have

$$R_l(G_l)\subset\left\{\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}\in GL(2, Z/lZ\right\}$$

Put

$$\begin{aligned} A &= \langle t_2\rangle \\ E' &= E/A\,, \end{aligned}$$

then E' is an elliptic curve defined over Q and has rational points of order 5. Let λ be the canonical isogeny of degree l from E to E', then E' is not isomorphic to E, because E has no complex multiplication. By Serre-Tate [5], E' has a conductor of 11-power. Hence E' must be the curve 15. By Vélu [7], we see that there is an isogeny λ' of degree 5 from the curve 15 to E, i.e., we get

$$E\xrightarrow{\lambda}E'\xrightarrow{\lambda'}E.$$

Then $\lambda'\circ\lambda$ is an endomorphism of E and its degree is $5l$. But this is impossible since E has no complex multiplication.

By Vélu [7], E_5 is completely reducible as G_5-module. This shows that $R_5(G_5)$ is isomorphic to $(Z/5Z)^\times$ and $Q(E_5)=Q(e^{2\pi i/5})$.

For the other curves we can prove the theorem by the same method as above,

TABLE $y^2+a_1xy+a_3y+x^3+a_2x^2+a_4x=0$

	a_1	a_3	a_2	a_4	Δ	N	J	type of $\boldsymbol{F}$
1	0	1	-1	1	-19	19	$2^{15}\cdot 19^{-1}$	a cyclic group of order 3
2	0	1	-4	2	37	37	$2^{15}\cdot 5^3\cdot 37^{-1}$	"
3	0	1	0	0	-3^3	3^3	0	"
4	0	1	-9	-3	-3^5	3^3	$-2^{15}\cdot 3\cdot 5^3$	"
5	0	3	0	0	-3^7	3^5	0	"
6	0	19	-16	76	-19^3	19	$-2^{18}\cdot 7^3\cdot 19^{-3}$	"
7	0	37	-25	185	37^3	37	$2^{15}\cdot 5^3\cdot 7^3\cdot 37^{-3}$	"
8	0	9	-9	27	-3^9	3^3	0	"
9	0	9	0	0	-3^{11}	3^5	0	"
10	1	0	-8	17	17^2	17	$3^3\cdot 7^3\cdot 13^3\cdot 17^{-2}$	(2, 2)-type
11	1	0	-140	17^3	17^8	17^2	$3^3\cdot 7^3\cdot 13^3\cdot 17^{-2}$	"
12	1	1	1	0	17	17	$3^3\cdot 11^3\cdot 17^{-1}$	a cyclic group of order 4
13	17	17^3	-17	17^3	17^7	17^2	$3^3\cdot 11^3\cdot 17^{-1}$	"
14	1	34	-20	153	-17^4	17	$-3^3\cdot 11^3\cdot 17^{-4}$	"
15	0	1	1	0	-11	11	$-2^{12}\cdot 11^{-1}$	a cyclic group of order 5
16	0	11	-14	55	-11^5	11	$-2^{12}\cdot 31^3\cdot 11^{-5}$	"

There are some isogenies connecting these curves, which are easily computed by the method of Vélu [8]. Let $\boldsymbol{E}^q$ be the curve q on the table, then we obtain the isogenies of degree 2

$$\boldsymbol{E}^{12}\sim\boldsymbol{E}^{10}=\boldsymbol{E}^{12}/\langle(-1,0)\rangle,\ \boldsymbol{E}^{14}\sim\boldsymbol{E}^{10}=\boldsymbol{E}^{14}/\left\langle\left(\frac{17}{4},\ \frac{153}{8}\right)\right\rangle$$

$$\boldsymbol{E}^{13}\sim\boldsymbol{E}^{11}=\boldsymbol{E}^{13}/\langle(17,\ -17)\rangle,$$

the isogenies of degree 3

$$\boldsymbol{E}^{1}\sim\boldsymbol{E}^{6}=\boldsymbol{E}^{1}/\langle(0,\ 0)\rangle,\ \boldsymbol{E}^{2}\sim\boldsymbol{E}^{7}=\boldsymbol{E}^{2}/\langle(0,\ 0)\rangle,$$

the isogeny of degree 4

$$\boldsymbol{E}^{12}\sim\boldsymbol{E}^{14}=\boldsymbol{E}^{12}/\langle(0,\ 0)\rangle,$$

and the isogeny of degree 5

$$\boldsymbol{E}^{15}\sim\boldsymbol{E}^{16}=\boldsymbol{E}^{15}/\langle(0,\ 0)\rangle.$$

REMARK. There are some other isogenies of degree 3 among the curves $\boldsymbol{E}^3$, $\boldsymbol{E}^4$, $\boldsymbol{E}^5$, $\boldsymbol{E}^8$, $\boldsymbol{E}^9$. But we exclude them, since we have no need for them to complete the proof of the theorem 5.

OSAKA UNIVERSITY

References

[1] J.W.S. Cassels: *Diophantine equations with specieal references to elliptic curves*, J. London Math. Soc. **41** (1966), 193–291.

[2] A. Néron: *Modèles minimaux des variétés abéliennes sur les corps locaux et globaux*, Inst. Hautes Études Sci. Publ. Math. **21** (1964) 5–125.

[3] A.P. Ogg: *Abelian curves of* 2*-power conductor*, Proc. Cambridge Philos. Soc. **62** (1966), 143–148.

[4] J.-P. Serre: Abelian *l*-adic Representations and Elliptic Curves, Lecture notes, New York. 1968.

[5] J.-P. Serre and J. Tate: *Good reduction of abelian varieties*, Ann. of Math. **88** (1968), 492–517.

[6] G.Shimura: *A reciprocity law in non-solvable extentions*, J. Reine Angew. Math. **221** (1966), 209–220.

[7] J. Vélu: *Courbes elliptiques sur* **Q** *ayant bonne reduction en dehors de* $\{11\}$, C.R. Acad. Sci. Paris **273** (1971), 73–75.

[8] J. Vélu: *Isogénies entre courbes elliptiques*. C.R.Acad. Sci. Paris **273** (1971), 238 –241.

[9] A. Weil: *Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen*, Math. Ann. **168** (1967), 149–156.