96. *On the Mordell-Weil Group of Certain Elliptic Curve*

By Fumio HAZAMA
Department of Mathematics, University of Tokyo

(Communicated by Kunihiko KODAIRA, M. J. A., Dec. 12, 1979)

§1. **Introduction.** Let us consider the elliptic curve

(1.1) $E_j: y^2=x^3-(27j/4(j-1728))(x-1) \qquad (j\neq 0, 1728, \infty)$

which is a well known example of an elliptic curve defined over $\boldsymbol{Q}(j)$ with the absolute invariant j. For any value of j, the point $P_0:(x,y)=(1,1)$ is a $\boldsymbol{Q}$-rational point of E_j. The purpose of this paper is to prove the following

Theorem 1.1. *For every $j\in\boldsymbol{Q}$ ($j\neq 0$, 1728), P_0 is a $\boldsymbol{Q}$-rational point of E_j of infinite order.*

Corollary 1.2. *For any $j\in\boldsymbol{Q}$, there exists an elliptic curve E defined over $\boldsymbol{Q}$ such that* 1) *the absolute invariant is j and* 2) *rank* $(E(\boldsymbol{Q}))\geq 1$.

The proof depends on the following remarkable theorem due to Barry Mazur:

Theorem 1.3 (Mazur [6]). *The order of a $\boldsymbol{Q}$-rational torsion point of an elliptic curve defined over $\boldsymbol{Q}$ is one of the following*:

$$\{1,2,3,4,5,6,7,8,9,10,12\}.$$

For the proof of our theorem, we first show that, in case j is a variable over $\boldsymbol{Q}$, P_0 is a rational point of E_j of infinite order, by considering the associated elliptic surface over the j-line $\boldsymbol{P}^1$. Given a positive integer m, the set $A(m)$ of $j_0\in\boldsymbol{Q}-\{0,1728\}$ such that P_0 is a point of exact order m on E_{j_0} is obviously finite (cf. Proposition 3.2). Then by Mazur's theorem 1.3, $A(m)$ is empty if $m>12$ or $m=11$. Thus we have only to prove that $A(m)$ is also empty for $1\leq m\leq 10$ or $m=12$. This will be done case by case.

Here the author would like to thank Prof. T. Shioda who provided several valuable suggestions.

§2. **Rational points on the generic fibre.** Put $t=27j/4(j-1728)$, then the equation of E_j becomes $y^2=x^3-tx+t$. From now on, we call this E_t. We note that if $j=0, 1728, \infty$, then $t=0, \infty, 27/4$, respectively. We note first the following

Proposition 2.1. rank $(E_t(\boldsymbol{Q}(t)))=1$, *where t denotes a variable over $\boldsymbol{Q}$.*

Proof. Let $B\xrightarrow{\Phi}\boldsymbol{P}^1$ be the elliptic surface associated to E_t, then we have (Shioda [9])

$\rho=r+2+\sum_{v\in S}(m_v-1)$,

ρ; the rank of $NS(B)$,

r; the rank of $E_t(C(t))$,

S; the finite set of points v of P^1 for which $\Phi^{-1}(v)$ is a singular fibre,

m_v; number of irreducible components of $\Phi^{-1}(v)$ for $v\in S$.

As is easily seen, the types of the singular fibres are II $(t=0)$, I_1 $(t=27/4)$, III^* $(t=\infty)$ in Kodaira's notation ([5]). Therefore $m_0=1$, $m_{27/4}=1$, $m_\infty=8$. On the other hand, we have $\rho=b_2=10$, since B is a rational elliptic surface $(t=(x^3-y^2)/(x-1))$. Hence the above formula shows that $r=1$. Now the point $(x,y)=(1,1)$ is a $\boldsymbol{Q}(t)$ rational point of E_t, which cannot be of finite order since there is a singular fibre of additive type such as $\Phi^{-1}(0)$ ([7], [8]). Therefore rank $(E_t(\boldsymbol{Q}(t)))=1$.

Q.E.D.

Actually we can determine the structure of the abelian group $E_t(\boldsymbol{Q}(t))$ completely:

Proposition 2.2. *$E_t(\boldsymbol{Q}(t))$ is an infinite cyclic group generated by $P_0=(1,1)$.*

Proof (due to N. Maruyama). As is shown in the proof of the above proposition, there is no element of finite order in $E_t(\boldsymbol{Q}(t))$. Furthermore we can show that $P_0\neq nQ$ for any $n\geq 2$, $Q\in E_t(\boldsymbol{Q}(t))$ as follows. First we recall that the fibre $C=\Phi^{-1}(27/4)$:

$$y^2z=x^3-(27/4)xz^2+(27/4)z^3$$

(in homogeneous coordinates) is a singular fibre of type I_1, i.e. a rational curve with one ordinary double point. Therefore, if we denote by $C^\#$ the set of non-singular points on C, there is an isomorphism of $C^\#$ to the multiplicative group. By elementary computation, we find that such an isomorphism is given by the following map:

$$f(x,y,z)=(3x+2y-(9/2)z)/(-3x+2y+(9/2)z).$$

Let us consider the induced group homomorphism

$$f\,;\,E_t(\boldsymbol{Q}(t))\xrightarrow{\text{restriction}}C^\#(\boldsymbol{Q})\xrightarrow{f}\boldsymbol{Q}(\sqrt{2}).$$

Note that $f(P_0)=-(1-\sqrt{2})^4$. Suppose that we have $P_0=nQ$, for some $Q\in E_t(\boldsymbol{Q}(t))$. Then

$$f(Q)^n=f(nQ)=f(P_0)=-(1-\sqrt{2})^4.$$

But since the algebraic integer $1-\sqrt{2}$ is a fundamental unit of $\boldsymbol{Q}(\sqrt{2})$ (cf. [1, Chapter 2, § 5]), n must be 1 or 2 or 4. The last two cases do not occur because $f(Q)^n<0$. This proves that P_0 is a generator of $E_t(\boldsymbol{Q}(t))$.

Q.E.D.

§ 3. Preliminaries.

We use the following propositions to prove our theorem.

Proposition 3.1 (Cassels [2]). *Let $P=(X,Y)$ be a point on the elliptic curve*

$$E:y^2=x^3-Ax-B$$

and let m be a positive integer. Then the point mP has the coordinates $(\varphi_m\psi_m^{-2}, \omega_m\psi_m^{-3})$ where $\varphi_m, \psi_m, \omega_m$ are polynomials in X, Y, A, B, with integer coefficients such that if $2^k \| m$ then $2^k \| \psi_m$ ($\|$ denotes exact divisibility) and they are given inductively by the relations

$$\psi_1=1, \quad \psi_2=2Y, \quad \psi_3=3X^4-6AX^2-12BX-A_2,$$
$$\psi_4=4Y(X^6-5AX^4-20BX^3-5A^2X^2-4ABX-8B^2+A^3),$$
$$\varphi_m=X\psi_m^2-\psi_{m-1}\psi_{m+1}, \qquad 4Y\omega_m=\psi_{m+2}\psi_{m-1}^2-\psi_{m-2}\psi_{m+1}^2,$$
$$\psi_{2m}=2\psi_m\omega_m, \qquad \psi_{2m+1}=\psi_{m+2}\psi_m^3-\psi_{m-1}\psi_{m+1}^3.$$

Proposition 3.2 (Cassels [3]). *Let (x_1, y_1) be a point of finite order on the E in Proposition 3.1, where $A, B \in \boldsymbol{Z}$. Then $x_1, y_1 \in \boldsymbol{Z}$; moreover $y_1=0$ or $y_1^2 \mid D(E)=-4A^3+27B^2$.*

§ 4. Rational points on special fibres. Proof of Theorem 1.1.

Now we go back to the elliptic curve (1.1) with $P=P_0$. Then $\varphi_m, \psi_m, \omega_m$ in Proposition 3.1 are polynomials in t with integer coefficients. Let us write these $\varphi_m(t)$, $\psi_m(t)$, $\omega_m(t)$.

Lemma 4.1. *Let $t_0 \in \boldsymbol{Q}-\{0, 27/4\}$. If $P_0=(1,1)$ is a point of finite order on E_{t_0}, then t_0 must be one of the following values*:

(4.1) $\qquad t_0=\pm 1, \pm 3, \pm 5, \pm 7, \pm 9, \pm 1/3, \pm 1/5.$

Proof. If $P_0=(1,1)$ is a point of finite order m on E_{t_0}, then $\psi_m(t_0)=0$ for $2 \leq m \leq 10$ or $m=12$ by Theorem 1.3 and Proposition 3.1. Here we compute the leading coefficients (=l.c.) and constant terms (=const.) of $\psi_m(t)$:

	degree	l.c.	const.		degree	l.c.	const.
ψ_1	0	1	1	ψ_7	12	-1	7
ψ_2	0	2	2	ψ_8	15	8	8
ψ_3	2	-1	3	ψ_9	20	1	9
ψ_4	3	4	4	ψ_{10}	24	10	10
ψ_5	6	1	5	ψ_{11}	30	-1	11
ψ_6	8	6	6	ψ_{12}	35	12	12

We note that $2\mid\psi_2, 4\mid\psi_4, 2\mid\psi_6, 8\mid\psi_8, 2\mid\psi_{10}$ and $4\mid\psi_{12}$ by (3.1). Therefore t_0 must be one of the values in (4.1). Q.E.D.

Lemma 4.2. *For any value of t_0 in (4.1), $P_0=(1, 1)$ is not a point of finite order on E_{t_0}.*

Proof. For $t_0=\pm 1, \pm 3, \pm 5, \pm 7, \pm 9$, we can use Proposition 3.2 directly to show $P_0=(1, 1)$ is not a point of finite order on E_{t_0}. For instance, if $t_0=1$, we get $2P_0=(-1, 1)$, $3P_0=(0, -1)$, $4P_0=(3, -5)$. But $(-5)^2 \nmid D(E_1)=23$, hence P_0 cannot be a point of finite order on E_1 by Proposition 3.2. We sum up the computation for $t_0=-1, \pm 3, \pm 5, \pm 7, \pm 9$ as follows:

E_{-1}: $2P_0=(2, -3)$, $(-3)^2 \nmid D_{-1}=31$.

$E_3: 3P_0=(13/9, -35/27) \notin Z\times Z$.
$E_{-3}: 2P_0=(7, -19)$, $(-19)^2 \nmid D_{-3}=351$.
$E_5: 2P_0=(-1, -3)$, $(-3)^2 \nmid D_5=25\cdot 7$.
$E_{-5}: 2P_0=(14, -53)$, $(-53)^2 \nmid D_{-5}=25\cdot 47$.
$E_7: 4P_0=(9/4, -13/8) \notin Z\times Z$.
$E_{-7}: 2P_0=(23, -111)$, $(-111)^2 \nmid D_{-7}=49\cdot 55$.
$E_9: 2P_0=(7, 17)$, $17^2 \nmid D_9=-3^6$.
$E_{-9}: 2P_0=(34, -199)$, $(-199)^2 \nmid D_{-9}=3^6\cdot 7$.

In case $t_0=\pm 1/3, \pm 1/5$, we can transform the coefficients of E_{t_0} into integers by appropriate birational transformations fixing zero, therefore by isomorphisms of abelian varieties. Then we can proceed as above.

$E_{1/3}: \cong E'_{1/3}: y'^2=x'^3-3^3x'+3^5$ by $x'=3^2x$, $y'=3^3y$. P_0 corresponds to $P'_0=(9, 27)$. $2P'_0=(-2, 17)$, $17^2 \nmid D'_{1/3}=3^9\cdot 77$.

$E_{-1/3}: \cong E'_{1/3}: y'^2=x'^3+3^3x'-3^5$ by $x'=3^2x$, $y'=3^3y$. P_0 corresponds to $P'_0=(9, 27)$. $2P'_0=(7, -17)$, $(-17)^2 \nmid D'_{1/3}=3^9\cdot 85$.

$E_{1/5}: \cong E'_{1/5}: y'^2=x'^3-5^3x'+5^5$ by $x'=5^2x$, $y'=5^3y$. P_0 corresponds to $P'_0=(5^2, 5^3)$. $2P'_0=(-1, 57)$, $57^2 \nmid D'_{1/5}=5^9\cdot 131$.

$E_{-1/5}: \cong E'_{-1/5}: y'^2=x'^3+5^3x'-5^5$ by $x'=5^2x$, $y'=5^3y$. P_0 corresponds to $P'_0=(5^2, 5^3)$. $2P'_0=(14, -37)$, $(-37)^2 \nmid D'_{-1/5}=5^9\cdot 139$.

This completes the proof of Lemma 4.2. Q.E.D.

Theorem 1.1 follows immediately from these two lemmas.

To show the corollary, it suffices to find elliptic curves defind over Q with $j=0$, 1728 and rank ≥ 1. But this is a well known fact. For example, if we take $E': y^2=x^3-2$, and $E'': y^2=x^3-2x$, then $j(E')=0$ and $j(E'')=1728$. Moreover, by Proposition 3.2, we see that $(3, 5) \in E'(Q)$ and $(2, 2) \in E''(Q)$ are not points of finite order.

§ 5. **Remark.** The family E_j (see (1.1)) has connection with the theory of universal families of elliptic curves with level N structure. For $N\geq 3$, there exists such a family E_N parametrized by an affine curve C_N. Moreover, in case the base field is C, Shioda proved $E_N(K_N) \cong (Z/NZ)^2$, where K_N denotes the function field of the base curve C_N (Shioda [9], [10]). On the other hand, there is no such family for $N \leq 2$. However, for $N=2$, it is known that the Legendre form, $E_\lambda: y^2=x(x-1)(x-\lambda)$, gives an "almost" universal family and $E_\lambda(k(\lambda)) \cong (Z/2Z)^2$, where k denotes the base field (see [4], [10]). For $N=1$, the situation is quite different. In fact, the family E_j, defined by (1.1), for variable j, does have a rational point of infinite order (Proposition 2.1). This observation was the starting point of the present work.

References

[1] Z. I. Borevich and I. R. Shafarevich: Number Theory. Academic Press, New York (1966).

[2] J. W. S. Cassels: A note on the division value of $\wp(u)$. Proc. Cambridge Phil. Soc., **45**, 167–172 (1949).

[3] ——: Diophantine equations with special reference to elliptic curves. J. London Math. Soc., **41**, 193–291 (1966).

[4] J. Igusa: Fibre systems of Jacobian varieties (III. Fibre systems of elliptic curves). Amer. J. Math., **81**, 453–476 (1959).

[5] K. Kodaira: On compact complex analytic surfaces. II, III. Ann. of Math., **77**, 563–626 (1963); **78**, 1–40 (1963).

[6] B. Mazur: Modular curves and the Eisenstein ideal. Publ. Math. IHES, **47**, 33–186 (1977).

[7] A. P. Ogg: Cohomology of abelian varieties over function fields. Ann. of Math., **76**, 185–212 (1962).

[8] I. R. Shafarevich: Principal homogeneous spaces defined over a function field. Amer. Math. Soc. Trans., **37**(2), 85–114 (1964).

[9] T. Shioda: On elliptic modular surfaces. J. Math. Soc. Japan, **24**, 20–59 (1972).

[10] ——: On rational points of the generic elliptic curve with level N structure over the field of modular functions of level N. Ibid., **25**, 144–157 (1973).