Points of Finite Order of Elliptic Curves with Complex Multiplication.

Olson, Loren D.

in: Manuscripta mathematica | Manuscripta Mathematica | Article

195 - 206

manuscripta math. 14, 195 - 205 (1974)

POINTS OF FINITE ORDER ON ELLIPTIC CURVES WITH COMPLEX MULTIPLICATION

Loren D. Olson

Let E be an elliptic curve defined over $\mathbb{Q}$. The group of $\mathbb{Q}$ - rational points of finite order on E is a finite group $T(E)$. In this article $T(E)$ is computed for all elliptic curves defined over $\mathbb{Q}$ admitting complex multiplication. The only possible values for the order t of $T(E)$ are $1, 2, 3, 4,$ or 6 in these cases. A standard form for an affine equation describing an elliptic curve with a given j - invariant is obtained. This is used to show that if $j \neq 0, 2^6 3^3$, then the number of $\mathbb{Q}$ - rational points of order 2 on E depends only on j. The results are summarized in the accompanying table.

1. General results

Let E be an elliptic curve defined over $\mathbb{Q}$, i.e. a non-singular projective curve of genus one defined over $\mathbb{Q}$ together with a $\mathbb{Q}$-rational point e on E which acts as the identity element for the group law on E. Any such elliptic curve is isomorphic over $\mathbb{Q}$ to an elliptic curve defined by an affine equation of the form

$$(1.1) \qquad Y^2 = X^3 + a_4X + a_6$$

with $a_i \in \mathbb{Z}$. Let $\Delta = -2^4(2^2a_4^3 + 3^3a_6^2)$ and $j = 2^8 3^3 a_4^3 / (2^2a_4^3 + 3^3a_6^2)$. Assume E admits complex multiplication in $\mathbb{Q}(\sqrt{m})$ with $m < 0$ a square-free integer. Let f be the conductor of $\mathrm{End}(E)$ in the ring of integers in $\mathbb{Q}(\sqrt{m})$. There are precisely 13 values in $\mathbb{Q}$ for the j-invariant of such an elliptic curve (cf. Serre [2, p. 295]). Let p be a prime where E has good reduction, and let N_p denote the number of $\mathbb{Z}/p\mathbb{Z}$ -

m	f	j	t
-1	1	$2^6 3^3$	2 or 4 (cyclic and non-cyclic)
-2	1	$2^6 5^3$	2
-3	1	0	1,2,3, or 6
-7	1	$-3^3 5^3$	2
-11	1	-2^{15}	1
-19	1	$-2^{15} 3^3$	1
-43	1	$-2^{18} 3^3 5^3$	1
-67	1	$-2^{15} 3^3 5^3 11^3$	1
-163	1	$-2^{18} 3^3 5^3 23^3 29^3$	1
-1	2	$2^3 3^3 11^3$	2 or 4 (cyclic)
-3	2	$2^4 3^3 5^3$	2 or 6
-7	2	$3^3 5^3 17^3$	2
-3	3	$-2^{15} 3^1 5^3$	1 or 3

rational points on the reduced curve. Let $f_p = 1 + p - N_p$ be the trace of the Frobenius. Let $\mathcal{P} = \mathcal{P}(E)$ be the set of all primes $p \geq 5$ such that E has good reduction at p. The following proposition is a well-known result (cf. Serre [3]).

PROPOSITION 1.1. *Let E be an elliptic curve defined over $\mathbb{Q}$ admitting complex multiplication. Let $p \in \mathcal{P}$. Then the following conditions are equivalent:* (1) $N_p = p + 1$, (2) $f_p = 0$, (3) *p remains a prime in* $\mathbb{Q}(\sqrt{m})$, and (4) $\left(\frac{m}{p}\right) = -1$.

Let $\mathcal{P}_1 = \{p \in \mathcal{P} \mid \left(\frac{m}{p}\right) = -1\} = \{p \in \mathcal{P} \mid N_p = p+1\}$ and $\mathcal{P}_2 = \{p \in \mathcal{P} \mid \left(\frac{m}{p}\right) = 1\}$. Both $\mathcal{P}_1$ and $\mathcal{P}_2$ have density $1/2$ in $\mathcal{P}$. Let $T(E)$ be the group of $\mathbb{Q}$-rational points on E which have finite order, and let t be the order of $T(E)$. Our purpose here is to determine t and $T(E)$ for all elliptic curves E defined over $\mathbb{Q}$ admitting complex multiplication. We will constantly make use of the following fact (cf. Tate [4, p.195])

PROPOSITION 1.2. Let E be any elliptic curve defined over $\mathbb{Q}$, and let $p \in \mathcal{P}$. Reduction modulo p induces a monomorphism from $T(E)$ into the group of $\mathbb{Z}/p\mathbb{Z}$-rational points on the reduced curve. Thus $t | N_p$ for all $p \in \mathcal{P}$.

PROPOSITION 1.3. Let E be any elliptic curve defined over $\mathbb{Q}$ admitting complex multiplication. The only possible values for t are $1,2,3,4$, or 6.

PROOF: $t | N_p$ for all $p \in \mathcal{P}$. If $p \in \mathcal{P}_1$, then $N_p = p + 1$, so that $t | (p+1)$, i.e. $p \equiv -1 \pmod{t}$. By Dirichlet's theorem the set of all $p \in \mathcal{P}$ such that $p \equiv -1 \pmod{t}$ has density $1/\phi(t)$ where ϕ is Euler's ϕ-function. If $\phi(t) \geq 3$, we have a contradiction. Thus $\phi(t) \leq 2$ and we must have $t \leq 6$ and $t \neq 5$.

PROPOSITION 1.4. If $m \equiv 1 \pmod{4}$, then $t \neq 4$.

PROOF: If $m \equiv 1 \pmod{4}$, then $-m \equiv 3 \pmod{4}$ and $-m$ is a prime greater than or equal to 3. Assume that $p \in \mathcal{P}$ is such that $p \equiv 1 \pmod{4}$. Then $\left(\frac{-1}{p}\right) = 1$, and $\left(\frac{m}{p}\right) = \left(\frac{p}{-m}\right)$ by the quadratic reciprocity law. The arithmetic progression $(-4m)r + (-2m-1)$ contains infinitely many primes and hence there are infinitely many such in $\mathcal{P}$. Let p be one such. $p \equiv 1 \pmod{4}$ and $p \equiv -1 \pmod{-m}$. Thus $\left(\frac{m}{p}\right) = \left(\frac{p}{-m}\right) = \left(\frac{-1}{-m}\right) = -1$ since $-m \equiv 3 \pmod{4}$. Hence $p \in \mathcal{P}_1$ and so $N_p = p + 1$. If $t = 4$, then $4 | (p+1)$ and so $p \equiv 3 \pmod{4}$, a contradiction.

PROPOSITION 1.5. If $m = -2$, then $t \neq 4$.

PROOF: There exist infinitely many primes p such that $p \equiv 5 \pmod{8}$ and hence infinitely many such p in $\mathcal{P}$. Let p be one such in $\mathcal{P}$. Then $\left(\frac{-1}{p}\right) = 1$ and $\left(\frac{2}{p}\right) = -1$. $\left(\frac{m}{p}\right) = \left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = \left(\frac{2}{p}\right) = -1$. Thus $p \in \mathcal{P}_1$ and so $N_p = p + 1$. If $t = 4$, then $4 | (p+1)$ and so $p \equiv 3 \pmod{4}$, a contradiction.

Combining the two preceding propositions we see that the case $t = 4$ can occur only if $m = -1$.

PROPOSITION 1.6. If $m \neq -3$, then 3 does not divide t, i.e. E has no $\mathbb{Q}$-rational points of order 3.

PROOF: The proof follows the pattern of the two preced-

ing proofs. Assume that $3|t$. Then $3|N_p$ for all $p \in \mathcal{P}$. If $p \in \mathcal{P}_1$, then $N_p = p + 1$ and $3|(p+1)$, so that $p \equiv -1 \pmod 3$. We now proceed to demonstrate the existence of a $p \in \mathcal{P}_1$ such that $p \equiv -1 \pmod 3$ in all cases where $m \neq -3$. If $m = -1$, let $p = 12r + 7$ belong to $\mathcal{P}$. If $m = -2$, let $p = 24r + 13$ belong to $\mathcal{P}$. If $m = -11$, let $p = 132r + 109$ belong to $\mathcal{P}$. If $m = -7, -19, -43, -67,$ or -163, let $p = (-12m)r - (2m+1)$ belong to $\mathcal{P}$. In all cases $\left(\frac{m}{p}\right) = -1$, so that $p \in \mathcal{P}_1$. But $p \equiv 1 \pmod 3$, a contradiction.

2. The case $j = 0$, $m = -3$, $f = 1$, and $Y^2 = X^3 + a_6$.

If the elliptic curve E is defined by an affine equation of the form (1.1), then $j = 0$ if and only if $a_4 = 0$. In this case, the determination of $T(E)$ is a classical result due to Fueter [1] and may be summarized as follows.

THEOREM 2.1 (Fueter). *Let E be an elliptic curve defined over $\mathbb{Q}$ with j-invariant $j = 0$ given by the affine equation $Y^2 = X^3 + a_6$ with $a_6 \in \mathbb{Z}$. Then*

(1) *$t = 6$ and $T(E) \cong \mathbb{Z}/6\mathbb{Z}$ $\iff$ a_6 is a sixth power in $\mathbb{Z}$.*

(2) *$t = 3$ and $T(E) \cong \mathbb{Z}/3\mathbb{Z}$ $\iff$ either a_6 is a square in $\mathbb{Z}$ but not a sixth power in $\mathbb{Z}$ or a_6 is -432 times a sixth power.*

(3) *$t = 2$ and $T(E) \cong \mathbb{Z}/2\mathbb{Z}$ $\iff$ a_6 is a cube in $\mathbb{Z}$ but not a sixth power in $\mathbb{Z}$.*

(4) *$t = 1$ and $T(E) = \{e\}$ otherwise.*

3. The case $j = 2^6 3^3$, $m = -1$, $f = 1$, and $Y^2 = X^3 + a_4X$

If the elliptic curve E is given by an affine equation of the form (1.1), then $j = 2^6 3^3$ if and only if $a_6 = 0$. The point $(0,0)$ is clearly a $\mathbb{Q}$-rational point of order 2 on E. By Proposition 1.6, t is either 2 or 4. The case $t = 4$ can occur either with the existence of 3 $\mathbb{Q}$-rational points of order 2 on E or with the existence of a $\mathbb{Q}$-rational point of order 4 on E.

PROPOSITION 3.1. *$t = 4$ and E has 3 $\mathbb{Q}$-rational points*

of order $2 \iff -a_4$ is a square in $\mathbb{Z}$. In this case, $T(E) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

PROOF: A $\mathbb{Q}$-rational point $P = (x,y)$ on E has order $2 \iff y = 0$ and x is a solution of

$$(3.1) \qquad 0 = X^3 + a_4X = X(X^2+a_4)$$

Thus E has 3 $\mathbb{Q}$-rational points of order $2 \iff X^2 + a_4 = 0$ has a solution in $\mathbb{Z} \iff -a_4$ is a square in $\mathbb{Z}$.

PROPOSITION 3.2. $t = 4$ and E has a $\mathbb{Q}$-rational point of order $4 \iff a_4$ is equal to 4 times a fourth power in $\mathbb{Z}$. In this case $T(E) \cong \mathbb{Z}/4\mathbb{Z}$.

PROOF: ($\Longrightarrow$) Let $P = (x,y)$ be a $\mathbb{Q}$-rational point of order 4 on E. Then $x \neq 0$, $y \neq 0$ and $2P = (0,0)$. Let $\lambda = (3x^2+a_4)/2y$. Using the usual formulas for the addition of points, we obtain $0 = \lambda^2 - 2x$ and $0 = y - \lambda x$. Thus $(3x^2+a_4)/2 = \lambda y = \lambda^2 x = 2x^2$ or $3x^2 + a_4 = 4x^2$ or $x^2 = a_4$. Thus $a_4 > 0$ and a_4 is a square in $\mathbb{Z}$. Since (x,y) lies on the curve E, $y^2 = x^3 + a_4x = x^3 + x^3 = 2x^3$. Thus $2|y$. Therefore $4|y^2$ and $4|2x^3$, so $2|x$ and $2|a_4$. a_4 is a square, so we may write $a_4 = (2b)^2$ with $b > 0$. Since $y^2 = x^3 + a_4x$ and $a_4 > 0$, we must have $x > 0$. $x^2 = a_4 = (2b)^2$, so that $x = 2b$. Then $y^2 = x^3 + a_4x = 2x^3 = 2(2b)^3 = 16b^3$. Thus b is a square. Write $b = c^2$ for $c \in \mathbb{Z}$. We have $a_4 = (2b)^2 = 4b^2 = 4c^4$.

($\Longleftarrow$) Suppose $a_4 = 4c^4$ for $c \in \mathbb{Z}$. Let $x = 2c^2$, $y = 4c^3$. $P = (x,y)$ is a $\mathbb{Q}$-rational point on E of order 4.

PROPOSITION 3.3. $t = 2 \iff a_4$ is neither of the form $a_4 = 4c^4$ for some $c \in \mathbb{Z}$ nor of the form $a_4 = -c^2$ for some $c \in \mathbb{Z}$. In this case, $T(E) \cong \mathbb{Z}/2\mathbb{Z}$.

4. A standard form for the affine equation

Let E be an elliptic curve defined over $\mathbb{Q}$ given by an affine equation of the form (1.1). Assume that $j \neq 0$, $2^6 3^3$, i.e. $a_4 \neq 0$ and $a_6 \neq 0$. We shall describe a standard expression for the coefficients a_4 and a_6 in terms of the j-invariant. We may rewrite the formula for j as

$$(4.1) \qquad (2^8 3^3 - 2^2 j)\, a_4^3 = 3^3 j a_6^2$$

If p is a prime, let v_p denote the usual p-adic valuation, i.e. $v_p(p) = 1$. If a is a real number, let $[a]$ denote the largest integer less than or equal to a. Define the following quantities with respect to j:

$$\varepsilon = \begin{cases} 1 & \text{if } 3^3 j/(2^8 3^3 - 2^2 j) > 0 \\ -1 & \text{if } 3^3 j/(2^8 3^3 - 2^2 j) < 0 \end{cases}$$

$$s_p = v_p(3^3 j/(2^8 3^3 - 2^2 j))$$

$$S = \{p \mid s_p \neq 0\}$$

$$t_p = \begin{cases} [s_p/3] & \text{for } s_p \geq 0 \\ [-s_p/2] & \text{for } s_p < 0 \end{cases}$$

$$(4.2) \qquad r_p = (v_p(a_4) - |s_p| + 2t_p)/2$$

$$A = \varepsilon \prod_{p \in S} p^{|s_p| - 2t_p}$$

$$B = \left(\prod_{\substack{p \in S \\ s_p > 0}} p^{s_p - 3t_p} \right) \left(\prod_{\substack{p \in S \\ s_p < 0}} p^{-2s_p - 3t_p} \right)$$

$$D = (a_6/|a_6|) \prod_p p^{r_p}$$

We have $a_4 = AD^2$, $a_6 = BD^3$, and $A, B, D \in \mathbb{Z}$. We may write equation (1.1) as

$$(4.3) \qquad Y^2 = X^3 + AD^2 X + BD^3$$

We will refer to this process of computing ε, A, B, and D as "putting E in standard form." This process enjoys the following useful properties:

(1.) ε, s_p, S, t_p, A, and B depend only on j.

(2.) A, B, and D are non-zero integers.

(3.) If we are given an affine equation (1.1)

defining E with a_4, $a_6 \in \mathbb{Q}$, we may write $a_4 = AD^2$ and $a_6 = BD^3$ with $D \in \mathbb{Q}$. Then $a_4 \in \mathbb{Z}$ and $a_6 \in \mathbb{Z} \iff D \in \mathbb{Z}$.

(4.) Equation (4.3) is a minimal Weierstrass equation for E at a prime $p \geq 5$ if and only if $p^2 \nmid D$. If we are only interested in the properties of E up to isomorphism over $\mathbb{Q}$, we may assume that D is square-free. The isomorphism classes over $\mathbb{Q}$ of elliptic curves with j-invariant j are in 1-1 correspondence with square-free integers D. This square-free D is unique, and we will call it the minimal D-factor of E.

A $\mathbb{Q}$-rational point $P = (x,y)$ on the elliptic curve defined by (1.1) is of order $2 \iff y = 0$, $x \in \mathbb{Z}$, and

$$0 = x^3 + a_4x + a_6 \tag{4.4}$$

Thus we seek integer solutions to the equation

$$0 = X^3 + AD^2X + BD^3 \tag{4.5}$$

Let $X = DW$. Substituting in (4.5), we obtain

$$0 = D^3W^3 + AD^3W + BD^3 \quad \text{or} \tag{4.6}$$

$$0 = W^3 + AW + B \tag{4.7}$$

The solutions to (4.5) correspond to the solutions to (4.7) via $X = DW$. Equation (4.7) depends only on j. We have thus proved the following theorem.

THEOREM 4.1. Let E be an elliptic curve defined over $\mathbb{Q}$ with j-invariant $j \neq 0, 2^6 3^3$. E has a $\mathbb{Q}$-rational point of order $2 \iff$ there exists an integer solution to equation (4.7). E has 3 $\mathbb{Q}$-rational points of order $2 \iff$ there exist 3 integer solutions to equation (4.7). This depends only on j.

COROLLARY 4.2. Let E be an elliptic curve defined over $\mathbb{Q}$ with j-invariant j.

(1.) If $j = 2^6 5^3$, $-3^3 5^3$, $2^3 3^3 11^3$, $2^4 3^3 5^3$, or $3^3 5^3 17^3$, then E has exactly one $\mathbb{Q}$-rational point of order 2.

(2.) If $j = -2^{15}$, $-2^{15} 3^3$, $-2^{18} 3^3 5^3$, $-2^{15} 3^3 5^3 11^3$, $-2^{18} 3^3 5^3 23^3 29^3$, or $-2^{15} 3^1 5^3$, then E has no $\mathbb{Q}$-rational point of order 2.

PROOF: In each case, one computes equation (4.7) and checks this for the number of integer solutions.

5. $\mathbb{Q}$-rational points of order 4 for $j = 2^3 3^3 11^3$.

In this section we give necessary and sufficient conditions for an elliptic curve E defined over $\mathbb{Q}$ with j-invariant $j = 2^3 3^3 11^3$ to have a $\mathbb{Q}$-rational point of order 4 . By the results of 4., E is isomorphic over $\mathbb{Q}$ to an elliptic curve given by an affine equation of the form

$$(5.1) \qquad Y^2 = X^3 + AD^2X + BD^3$$

where $A = -11$, $B = 2^1 7^1$, and $D \in \mathbb{Z}$, $D \neq 0$. By Corollary 4.2, this curve has exactly one $\mathbb{Q}$-rational point of order 2 . Let $a = 2D$. The point $(a,0)$ is the $\mathbb{Q}$-rational point of order 2 on E . By the translation $X \mapsto X + a$, $Y \mapsto Y$, the following equation is obtained:

$$(5.2) \qquad Y^2 = X^3 + a_2X^2 + a_4X$$

where $a_2 = 2^1 3^1 D$ and $a_4 = D^2$.

THEOREM 5.1. Let E be an elliptic curve defined over $\mathbb{Q}$ with j-invariant $j = 2^3 3^3 11^3$ given by (5.1) . E has a $\mathbb{Q}$-rational point of order $4 \iff v_p(D)$ is even for $p \geq 3$ and $D > 0$, i.e. E has 1 or 2 as its minimal D-factor. In this case, $t = 4$ and $T(E) \cong \mathbb{Z}/4\mathbb{Z}$. Otherwise, $t = 2$ and $T(E) \cong \mathbb{Z}/2\mathbb{Z}$.

PROOF: By Proposition 1.6, E has no $\mathbb{Q}$-rational points of order 3 . By Corollary 4.2 it has precisely one $\mathbb{Q}$-rational point of order 2 . Proposition 1.3 then implies that $t = 2$ or 4 (cyclic). We are thus reduced to investigating the existence of a $\mathbb{Q}$-rational point of order 4 on E . The point $(0,0)$ is the only $\mathbb{Q}$-rational point of order 2 on (5.2). Suppose that $P = (x,y)$ is to be a $\mathbb{Q}$-rational point of order 4 . Then $2P = (0,0)$. Let $\lambda = (3x^2+2a_2x+a_4)/2y$ and $\nu = y - \lambda x$. Then

$$(5.3) \qquad 2\lambda y = 3x^2 + 2a_2x + a_4$$

By the formula for the addition of points on E , we must have

$$(5.4) \qquad 0 = \lambda^2 - a_2 - 2x \quad \text{and} \quad 0 = \nu \text{ .} \quad \text{Thus}$$

$$(5.5) \qquad y = \lambda x \quad \text{or} \quad \lambda = y/x \text{ .}$$

Substituting (5.5) in (5.3), we obtain

$$(5.6) \qquad 2y^2 = 3x^3 + 2a_2x^2 + a_4x$$

Since (x,y) is to be a point on (5.2), we should have

$$2y^2 = 2x^3 + 2a_4x^2 + 2a_2x \quad (5.7)$$

Subtracting this from (5.6) gives

$$0 = x^3 - a_4x \quad (5.8)$$

Now $x = 0$ is not possible if (x,y) is to have order 4. Thus

$$x^2 - a_4 = 0 \quad (5.9)$$

Since $a_4 = D^2$, then $x = \sigma D$ where $\sigma = \pm 1$. Substituting in (5.2), we have

$$\begin{aligned} y^2 &= \sigma^3D^3 + 2^1 3^1 D^3 + \sigma D^3 \\ &= (\sigma+6+\sigma)D^3 \\ &= \begin{cases} 2^3D^3 & \text{if } \sigma = 1 \\ 2^2D^3 & \text{if } \sigma = -1 \end{cases} \end{aligned} \quad (5.10)$$

If $v_2(D)$ is even, let $\sigma = -1$; if $v_2(D)$ is odd, let $\sigma = 1$. Applying v_p to (5.10), we see that there exists a $y \in \mathbb{Z}$ satisfying (5.10) $\iff$ $v_p(D)$ is even for $p \geq 3$ and $D > 0$.

6. $\mathbb{Q}$-rational points of order 3 for $j = 2^4 3^3 5^3$ and $-2^{15}3^1 5^3$.

Assume that the elliptic curve E is given by an affine equation of the form (1.1). Suppose that $P = (x,y)$ is a $\mathbb{Q}$-rational point of order 3 on E, then $y \neq 0$. Let $\lambda = (3x^2 + a_4)/2y$ and $\nu = y - \lambda x$.
$2P = (\lambda^2 - 2x, -\lambda^3 + 3\lambda x - y)$. Since $2P = -P$, a necessary condition is

$$\lambda^2 - 2x = x \quad \text{or} \quad (6.1)$$

$$12xy^2 = 9x^4 + 6a_4x^2 + a_4^2 . \quad (6.2)$$

Since $P = (x,y)$ lies on the curve, we have

$$12xy^2 = 12x^4 + 12a_4x^2 + 12a_6x \quad (6.3)$$

Subtract (6.2) from (6.3) and get the necessary condition

$$0 = 3x^4 + 6a_4x^2 + 12a_6x - a_4^2 \quad (6.4)$$

THEOREM 6.1. *Let E be an elliptic curve defined over $\mathbb{Q}$ with $j = -2^{15}3^1 5^3$ given in the standard form (4.3). E has a $\mathbb{Q}$-rational point of order 3 $\iff$ $v_p(D)$ is odd for $p = 2$ and $v_p(D)$ is even for all other primes p and $D > 0$, i.e. E has 2 as its minimal D-factor. In this*

case, $t = 3$ and $T(E) \cong \mathbb{Z}/3\mathbb{Z}$. Otherwise $t = 1$ and $T(E) = \{e\}$.

PROOF: Proposition 1.3 and Corollary 4.2 imply that t is either 1 or 3. Putting E in standard form yields $\varepsilon = -1$, $A = -2^3 3^1 5^1$, $B = 2^1 11^1 23^1$, $a_4 = AD^2$, and $a_6 = BD^3$. Suppose $P = (x,y)$ is a $\mathbb{Q}$-rational point of order 3. Substituting in (6.4) we obtain

$$(6.5)\quad 0 = 3x^4 - 2^4 3^2 5^1 D^2 x^2 + 2^3 3^1 11^1 23^1 D^3 x - 2^6 3^2 5^2 D^4$$

Let $x = 2Dz$. (6.5) then reduces to

$$(6.6)\quad 0 = z^4 - 60z^2 + 253z - 300 .$$

One checks that $z = 3$ is the only integer solution. Thus $x = 6D$. If $P = (x,y)$ is to lie on E, then

$$(6.7)\quad y^2 = x^3 + a_4 x + a_6 \quad \text{or} \quad y^2 = 2D^3$$

Hence $y \in \mathbb{Z} \iff v_p(D)$ is odd for $p = 2$ and $v_p(D)$ is even for all other primes p and $D > 0$. Conversely such a point (x,y) gives a $\mathbb{Q}$-rational point of order 3 on E.

THEOREM 6.2. Let E be an elliptic curve defined over $\mathbb{Q}$ with $j = 2^4 3^3 5^3$ given in the standard form (4.3). E has a $\mathbb{Q}$-rational point of order $3 \iff v_p(D)$ is even for all primes p and $D > 0$, i.e. D has 1 as its minimal D-factor. In this case, $t = 6$ and $T(E) \cong \mathbb{Z}/6\mathbb{Z}$. Otherwise $t = 2$ and $T(E) \cong \mathbb{Z}/2\mathbb{Z}$.

PROOF: Proposition 1.3, Proposition 1.4, and Corollary 4.2 imply that t is either 2 or 6. Putting E in standard form yields $\varepsilon = -1$, $A = -3^1 5^1$, and $B = 2^1 11^1$. (6.4) gives

$$(6.8)\quad 0 = 3x^4 - 2^1 3^2 5^1 D^2 x^2 + 2^3 3^1 11^1 D^3 x - 3^2 5^2 D^4 .$$

Let $x = Dz$. Substitute in (6.8) and reduce to

$$(6.9)\quad 0 = z^4 - 30z^2 + 88z - 75 .$$

One checks that $z = 3$ is the only integer solution. Thus $x = 3D$. If $P = (x,y)$ is to lie on E, then

$$(6.10)\quad y^2 = x^3 + a_4 x + a_6 \quad \text{or} \quad y^2 = 2^2 D^3$$

Hence $y \in \mathbb{Z} \iff v_p(D)$ is even for all primes p and $D > 0$. Conversely such a point (x,y) gives a $\mathbb{Q}$-rational point of order 3 on E.

This completes the determination of $T(E)$ for all elliptic curves E defined over $\mathbb{Q}$ admitting complex

multiplication. The results are summarized in the accompanying table.

Bibliography

[1] Fueter, R.: Uber kubische diophantische Gleichungen. Commentarii Math. Helv. 2, 69-89 (1930).

[2] Serre, J.P.: Complex multiplication in J.W.S. Cassels and A. Fröhlich, Algebraic Number Theory. Washington, D.C., Thompson Book Company 1967.

[3] Serre, J.P.: Groupes de Lie l-adiques attachés aux courbes elliptiques. Coll. Internat. du C.N.R.S., No. 143 a Clermont-Ferrand, Editions du C.N.R.S.: Paris 1966.

[4] Tate, J.: The arithmetic of elliptic curves. Inventiones mathematicae. 23, Fasc. 3/4, 179-206 (1974).

University of Oslo, Norway.

Current mailing address:
Matematisk institutt, avd. A
Universitetet i Bergen,
5014 Bergen
Norway

(Received October 4, 1974)