SOME FORMULAE FOR ELLIPTIC CURVES WITH COMPLEX MULTIPLICATION

by A. R. RAJWADE, *Mathematics Department, Panjab University, Chandigarh*

(*Received* 12 *May* 1976)

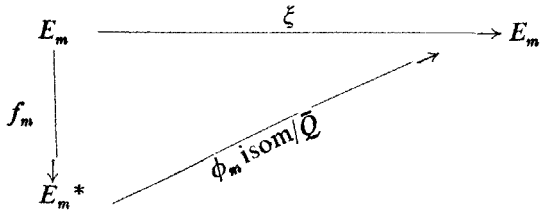
We obtain explicit formulae for elliptic curves defined over the rationals with complex multiplication by the integers of $Q(\sqrt{-7})$ and of $Q(\sqrt{-11})$. We also determine the image of a generic point (x, y) of such a curve under multiplication by $(-1+\sqrt{-7})/2$ for the first one and by $(-1+\sqrt{-11})/2$ for the second one. We use isogeny arguments to derive these formulae.

§ 1. Let E be an elliptic curve defined over Q and let us denote its ring of endomorphisms by End (E). It is well known that whenever End $(E) \supsetneq \mathbf{Z}$, it is a subring of finite index in the ring of integers of an imaginary quadratic field of class number 1. For each of the nine such fields, viz. $Q(\sqrt{-m})$ with $m = 1, 2, 3, 7, 11, 19, 43, 67, 163$, there is a curve, E_m say, with End (E_m) equal to the full ring of integers of $Q(\sqrt{-m})$. In addition to these nine curves there are two further ones. E_3', E_3'' say, with End $(E_3') = \mathbf{Z}[\sqrt{-3}]$ and End $(E_3'') = \mathbf{Z}[3(-1+\sqrt{-3})/2]$ as proper subrings of the full ring of integers of $Q((-1+\sqrt{-3})/2)$, and one further curve, E_7' say, with End $(E_7') = \mathbf{Z}(\sqrt{-7})$, a proper subring of the full ring of integers of $Q(\sqrt{-7})$. All these E's are defined over Q of course.

The object of this paper is to determine the equations of some of the E_m by isogeny arguments. The shapes of these E_m are not easily available in the literature except the ones with End equal to $\mathbf{Z}(i)$ and $\mathbf{Z}[\omega]$, the curves then being $y^2 = x^3 + Dx$ and $y^2 = x^3 + D$ respectively $(D \in \mathbf{Z})$. Methods using p-functions may give, in principle, the equations of the E_m but in practice the whole business becomes unwieldy as m increases and I have not even seen E_7 explicitly anywhere in the literature.

The method used in the derivation of the required equations is the following: Let p be a rational prime and ξ an integer of any of the above fields $Q(\sqrt{-m})$ with norm $\xi = p$. If E_m is the curve with complex multiplication by ξ, then E_m has on it norm $\xi = p\xi$th division points, since multiplication by ξ is an isogeny of degree norm ξ. Now consider the 'Q-isogeny' f_m of E_m having these $p\xi$th division points as its kernel. Since multiplication by ξ is also an isogeny (not a Q-isogeny of course) with the same kernel, it follows that E_m and $E_m{}^*$ (the isogenous curve) are isomorphic over $\bar{Q}$. Hence $j(E_m) = j(E_m{}^*)$. This gives the required relation amongst the coefficients of the equation for E_m (to make it a one parameter curve). Further when one performs the isogeny f_m again, it must give the

same effect on E_m as multiplication by p. This would be a check to the consistency of the method. Actual examples will make the method more clear. We start with the prime $p = 2$.



§ 2. Let $p = 2$. The ξ with norm 2 are $1 + i$, $\sqrt{-2}$, $(1 + \sqrt{-7})/2$ and their conjugates and associates. As soon as E_m has complex multiplication by ξ ($m = 1, 2, 7$ in this case), End (E_m) is the full ring of integers of $Q(\sqrt{-m})$. Of the norm $\xi\,(= 2)$ ξth division points, one is I the point at infinity. Let the other one be P. This P is a 2-division point since

$$2P = (\bar{\xi}\xi)\,P = \bar{\xi}\,(\xi P) = \bar{\xi}\,(I) = I.$$

Hence if $P = (x, y)$ then $y = 0$. If E_m is given, without loss of generality, by $y^2 = x^3 + Ax + B = (x - e_1)\,(x - e_2)\,(x - e_3)$ say, then at least one of e_j, say e_1, is real and we take $P = (e_1, 0)$. Now making the transformation $x \to x - e_1$, we may suppose that E_m has equation

$$E_m\colon\quad y^2 = x\,(x^2 + ax + b)\,(a, b \in \mathbf{Z}) \qquad \ldots(2.1)$$

and the point P, the ξth division point other than I, becomes $(0, 0)$.

To get the Q-isogeny f_m explicitly we use the following theorem of Velu's which we state here for the characteristic zero case, so that E_m has equation

$$y^2 = x^3 + ax^2 + bx + c.$$

Theorem (Velu 1971)—Let $f: E \to E^*$ be an isogeny with a finite kernel F. Let F_2 be the set of points of order 2 of $F - \{I\}$, R the set points of $F - \{I\} - F_2$ such that $F - \{I\} - F_2 = R \cup -R$, so that $R \cap -R = \phi$, and $S = F_2 \cup R$. Then the equation of E^* is given by

$$E^*\colon\quad y^2 = x^3 + ax^2 + (b - 5t)\,x + (c - 4at - 7w),$$

where

$$t = \sum_{Q \in S} t_Q, \qquad w = \sum_{Q \in S} (u_Q + x_Q t_Q),$$

where if $\phi\,(x, y)$ is written for $x^3 + ax^2 + bx + c - y^2$ then

$$g_Q^x = (\partial\phi/\partial x)_Q, \qquad g_Q^y = (\partial\phi/\partial y)_Q, \qquad u_Q = (g_Q^y)^2,$$

$$t_Q = \begin{cases} g_Q^x & \text{if } Q \in F_2 \\ 2g_Q^x & \text{if } Q \notin F_2 \end{cases}, \quad [\text{we write } Q = (x_Q, y_Q)];$$

and the isogeny f is given by $f(x, y) = (X, Y)$ where

$$X = x + \sum_{Q \in S} \left\{ \frac{t_Q}{x - x_Q} + \frac{u_Q}{(x - x_Q)^2} \right\},$$

$$Y = y - \sum_{Q \in S} \left\{ \frac{2yu_Q}{(x - x_Q)^3} + \frac{t_Q(y - y_Q) - g_Q^x \cdot g_Q^y}{(x - x_Q)^2} \right\}.$$

It follows that $E_m{}^*$ has equation $y^2 = x^3 + ax^2 - 4bx - 4ab$. In this we let $x \to x - a$ and we get

$$E_m{}^*: \quad y^2 = x\,(x^2 - 2ax + (a^2 - 4b)) \qquad \ldots(2.2)$$

We put (2.1) and (2.2) in the Weierstrass normal form:

$$y^2 = x^3 - (a^2 - 3b)/3 \,.\, x - a\,(9b - 2a^2)/27$$

$$y^2 = x^3 - (a^2 + 12b)/3 \,.\, x - 2a\,(36b - a^2)/27.$$

These being birationally equivalent over $\bar{Q}$ their absolute invariants are equal. This gives

$$[2a\,(36b - a^2)/27]^2/[(a^2 + 12b)/3]^3 = [a\,(9b - 2a^2)/27]^2/[(a^2 - 3b)/3]^3 \qquad \ldots(2.3)$$

One solution of this is $a = 0$ giving the curve $y^2 = x^3 + bx$ with End $=$ Z $[i]$. Simplifying (2.3) gives:

$$[(72b - 2a^2)/(9b - 2a^2)]^2 = [(a^2 + 12b)/(a^2 - 3b)]^3, \quad \text{i.e. say}$$

$$(N^3)^2 \qquad = \qquad (N^2)^3.$$

Hence

$$27b - 2a^2 = N^3(9b - 2a^2) \qquad\qquad 2a^2(N^3 - 1) = 9b(N^3 - 3)$$

$$a^2 + 12b = N^2(a^2 - 3b) \qquad \text{i.e.} \qquad a^2(N^2 - 1) = 3b(N^2 + 4).$$

Dividing gives, on simplification:

$$(N - 1)(N - 4)(N + 2)(N^2 + 3N + 4) = 0.$$

$N = 1$ gives $b = 0$ and E_m is $y^2 = x^3 + ax^2$ which is of genus 0.

$N = 4$ gives $4b = a^2$ and E_m is $y^2 = x(x + a/2)^2$ which too is of genus 0.

$N = -2$ gives $8b = a^2$ and E_m is $y^2 = x^3 + ax^2 + a^2x/8$ or letting $a \to -4D$ E_m is $y^2 = x^3 - 4Dx^2 + 2D^2x$ which has End $=$ Z $[\sqrt{-2}]$.

Finally the quardratic in N has roots $(-3 \pm \sqrt{-7})/2$ and taking the $+$ sign gives $b = a^2(9 - 5\sqrt{-7})/72$ and so E_m has equation

$$y^2 = x\,(x^2 + ax + a^2(9 - 5\sqrt{-7})/72) \qquad \ldots(2.4)$$

We note here the difference between the $\sqrt{-7}$ case and the $\sqrt{-2}$ and $\sqrt{-1} = i$ cases. For $\xi = 1 + i$ and $\sqrt{-2}$, $\bar{\xi}$ is an associate of ξ and hence the ξth division points are the same as the $\bar{\xi}$th division points. We could therefore take this ξth division point as $(0, 0)$ (real!), and the curve defined over Q; so that $\xi(0, 0) = \bar{\xi}(0, 0) = I$. However, for $\xi = (-1 + \sqrt{-7})/2$, $\bar{\xi}$ is not an associate of ξ and so the proper ξth division point differs from the proper $\bar{\xi}$th division point whence (2.4) is defined over an extension of Q.

Now let

$$x \to \frac{\sqrt{-7} + 7}{84} \cdot x - a\left(\frac{\sqrt{-7} + 11}{12}\right)$$

$$y \to \frac{y}{84}\sqrt{(7 + 5\sqrt{-7})/3} \qquad \ldots(2.5)$$

and (2.4) becomes:

$$y^2 = x(x^2 - 21ax + 112a^2) \qquad \ldots(2.6)$$

which is the simplest form for the curve E_7 with complex multiplication by $\sqrt{-7}$. We put these results down in the following:

Theorem 1—The curves with End = the full ring of integers of $Q(\sqrt{-m})$ with $m = 1, 2, 7$ are given by

$$E_1 : y^2 = x(x^2 + D)$$

$$E_2 : y^2 = x(x^2 - 4Dx + 2D^2)$$

$$E_7 : y^2 = x\left(x^2 + ax + a^2(9 - 5\sqrt{-7})/72\right).$$

The 2-isogenous curves to these are given by

$$E_1^* : y^2 = x(x^2 - 4D)$$

$$E_2^* : y^2 = x(x^2 + 8Dx + 8D^2)$$

(transformed by letting $x \to x + 4D$, $y \to y$ in Velu's theorem)

$$E_7^* : y^2 = x\left(x^2 - 2ax + a^2(9 + 5\sqrt{-7})/18\right)$$

(transformed by letting $x \to x - a$, $y \to y$ in Velu's theorem).

The Kernel of the isogeny is I, $(0, 0)$ in each case.

We next look at the behaviour of a generic point (x, y) of E_m on multiplication by ξ. We look at the three cases $m = 1, 2, 7$ separately.

Case $m = 1$—This may of course be treated directly since $i(x, y) = (-x, iy)$ and $(1 + i)(x, y) = (x, y) + (-x, iy)$. The present method gives the same answer of course. We have first to determine ϕ_m. A direct calculation shows that

$$\phi_1 : \begin{cases} x \to 2ix \\ y \to 2i(1 + i)y \end{cases} \left(\text{in fact } \begin{cases} x \to u^2 x \\ y \to u^3 y \end{cases} \text{ with } u = 1 + i\right)$$

takes E^*: $y^2 = x^3 - 4Dx$ to $E: y^2 = x^3 + Dx$. Hence for a point (x, y) of E we have $(1 + i)(x, y) = (\phi_0 f)(x, y) = \phi(x + D/x, y - Dy/x^2)$ by Velu's theorem $= \phi\left(y^2/x^2, -(y^2 - 2x^2)/x^3\right)$ on eliminating D using $y^2 = x(x^2 + D)$, $= \left(y^2/2ix^2, (1 + i)\, y\,(y^2 - 2x^3)/4x^3\right)$ as required.

Case m = 2—Here

$$\phi_2: \begin{cases} x \to u^2 x \\ y \to u^3 y \end{cases} \quad u = \sqrt{-2}, \text{ takes } y^2 = x\ (x^2 + 8Dx + 8D^2) \text{ to}$$

$y^2 = x(x^2 - 4Dx + 2D^2)$. Hence

$$\sqrt{-2}\,(x, y) = \phi_0 \begin{pmatrix} x \to x + 4D \\ y \to y \end{pmatrix}_0 f(x, y)$$

$$= \phi_0 \begin{pmatrix} x \to x + 4D \\ y \to y \end{pmatrix} (x + 2D^2/x, \quad y - 2D^2 y/x^2) \text{ by Velu's theorem,}$$

$$= \phi\,(x + 2D^2/x - 4D, \quad y - 2D^2 y/x^2)$$

$$= \left((x^2 - 4Dx + 2D^2)/-2x, \quad y\,(x^2 - 2D^2)/-2\sqrt{-2}\,.\,x^2\right).$$

It may be easily checked that (i) this point εE_2, (ii) $\sqrt{-2}\left(\sqrt{-2}\,(x, y)\right) = -2\,(x, y)$.

Case m = 7—Here the mapping $\phi_7: E_7^* \to E_7$ is given by

$$\begin{cases} x \to (-3 + \sqrt{-7})\, x/2 + (1 + \sqrt{-7})\, a/6 \\ y \to (5 + \sqrt{-7})\, y/2. \end{cases}$$

Hence for a generic point (x, y) of E_7 : $y^2 = x\left(x^2 + ax + a^2(9 - 5\sqrt{-7})/72\right)$

$$\frac{-1 + \sqrt{-7}}{2}\ (x, y)$$

$$= \phi_0 \begin{pmatrix} x \to x - a \\ y \to y \end{pmatrix}_0 f(x, y) \text{ and by Velu's theorem this is}$$

$$= \phi_0 \begin{pmatrix} x \to x - a \\ y \to y \end{pmatrix} \left(x + a^2(9 - 5\sqrt{-7})/72x, \quad y\left(1 - a^2(9 - 5\sqrt{-7})/72x^2\right)\right)$$

$$= \phi\left(x + a^2(9 - 5\sqrt{-7})/72x + a, \quad y\left(1 - a^2(9 - 5\sqrt{-7})/72\,x^2\right)\right)$$

$$= \left(\frac{\dfrac{x^2 + a^2(9 - 5\sqrt{-7})/72 + ax}{x} - (1 + \sqrt{-7})\, a/6}{(-3 + \sqrt{-7})/2}, \quad \frac{y\left(x^2 - a^2(9 - 5\sqrt{-7})/72\right)}{x^2(5 + \sqrt{-7})/2}\right)$$

$$= \left(\frac{-(3 + \sqrt{-7})\left(x + a(5 - \sqrt{-7})/12\right)^2}{8x}, \quad \frac{y\left(x^2 - a^2(9 - 5\sqrt{-7})/72\right)(5 - \sqrt{-7})}{16x^2}\right)$$

on simplification. This gives us multiplication by ξ on (2.4). Now we want such a formula on (2.6) which is defined over Q. Since the mapping (2.5) connects (2.6) with (2·4), a simple calculation gives us the following theorem:

Theorem 2—The curve E_7 with End equal to the full ring of integers of $Q(\sqrt{-7})$ is given by

$$y^2 = x(x^2 - 21ax + 112a^2)$$

and for a generic point (x, y) of this we have

$$\frac{-1+\sqrt{-7}}{2}(x, y) = (X, Y)$$

where

$$X = -(3+\sqrt{-7})(x - 2a(7-\sqrt{7}))^2/8(x - (21-\sqrt{-7})a/2)$$
$$Y = (5-\sqrt{-7})y(x - a(7+\sqrt{-7}))(x - 2a(7-\sqrt{-7}))/16$$
$$(x - (21-\sqrt{-7})a/2)^2$$

Using heavy calculation it may be checked that (i) $(X, Y) \in E_7$

(ii) $\xi(\bar{\xi}(x, y)) = 2(x, y)$. We note that

$$2(x, y) = \left(\frac{(x^2-112a^2)^2}{4y^2}, \frac{(x^2-112a^2)(x^2-14ax+56a^2)(x^2-28ax+224a^2)}{8y^3}\right) \quad \ldots(2.7)$$

(We have actually checked (i) and (ii) above !)

§ 3. We next take $p = 3$. The ξ of norm 3 are $1-\omega = (3+\sqrt{-3})/2$, $1+\sqrt{-2}$ and $(1+\sqrt{-11})/2$ and their conjugates and associates. The three ξth division points on E_m are also 3-division points which form a group of order 9, say I, $(x_i, \pm y_i)$, $i = 1, 2, 3, 4$. The x_1, x_2, x_3, x_4 are the roots of the quartic $d^2y/dx^2 = 0$ where $y^2 = x^3 + ax^2 + bx + c$ is the equation of E. This quartic can be worked out as

$$3x^4 + 4ax^3 + 6bx^2 + 12cx + (4ac - b^2) = 0 \quad \ldots(3.1)$$

Lemma—Precisely one pair $\pm(x_i, y_i)$ of these 4 pairs of 3-division points is real.

PROOF: We may take $a = 0$ without loss of generality. Our curve is then $y^2 = x^3 + bx + c = f(x)$ say and the relevant quartic becomes

$$3x^4 + 6bx^2 + 12cx - b^2 = 0. \quad \ldots(3.1a)$$

If $b = 0$ the roots are $x = 0$, $(-4c)^{1/3}$, $\omega(-4c)^{1/3}$, $\omega^2(-4c)^{1/3}$. The corresponding y^2 are c, $-3c$, $-3c$, $-3c$. If $c < 0$ then $((-4c)^{1/3}, \pm\sqrt{-3c})$ are the only real 3-division points while if $c > 0$ then $(0, \pm\sqrt{c})$ are the only real 3-division points. We may therefore suppose that $b \neq 0$.

Now all the 4 roots of (3.1) cannot be complex for if $\alpha \pm i\beta$, $\gamma \pm i\delta$ are the roots, their product $(\alpha^2+\beta^2)(\gamma^2+\delta^2) = -b^2$ which is false.

Case 1—Suppose the roots are α, β, $\gamma \pm i\delta$. Then $\alpha\beta(\gamma^2+\delta^2) = -b^2$. Hence just one of α, β is positive and the other negative, say $\alpha > 0$, $\beta < 0$. We

claim that for this α, $f(\alpha) = \alpha^3 + b\alpha + c$ is > 0 giving real $y = \pm \sqrt{f(\alpha)}$. To see this note first that at $x = \alpha$ we have $f(\alpha) \cdot f''(\alpha) = \frac{1}{2}(f'(\alpha))^2$. But $f''(\alpha) = 6\alpha > 0$ and $\frac{1}{2}(f'(\alpha))^2 > 0$ so $f(\alpha) > 0$ as required. Further for the negative root β, again since $f(\beta) \cdot f''(\beta) = \frac{1}{2}(f'(\beta))^2$ and $f''(\beta) = 6\beta < 0$ we must have $f(\beta) < 0$ so that the pair $(\beta, \pm \sqrt{f(\beta)})$ of 3-division points is complex. Hence just one pair is real.

Case 2—Suppose the roots are α, β, γ, δ all real. Then $\alpha\beta\gamma\delta = -b^2$ hence either just one of α, β, γ, δ is > 0 and the other three < 0, say $\alpha > 0$, β, γ, $\delta < 0$ in which case again we get $f(\alpha) > 0$ and $f(\beta)$, $f(\gamma)$, $f(\delta) < 0$ giving result, or three of α, β, γ, $\delta > 0$ and one < 0, say α, β, $\gamma > 0$, $\delta < 0$. But this gives the real 3-division points as $(\alpha, \pm \sqrt{f(\alpha)})$, $(\beta, \pm \sqrt{f(\beta)})$, $(\gamma, \pm \sqrt{f(\gamma)})$ which together with I form a subgroup of order 7 of the group of all 3-division points which is of order 9 and this is not possible. This completes the proof of the lemma.

Now move the y-axis so that this real pair of three-division points becomes $(0, \pm \sqrt{c}) = \pm P$ say. The condition $d^2y/dx^2 = 0$ gives $b^2 = 4ac$. We take I and $\pm P$ as the ξth division points on E_m.

$$E_m : y^2 = x^3 + ax^2 + bx + c, \quad c > 0, \quad b^2 = 4ac. \qquad \ldots(3.2)$$

Now consider the Q-isogeny with kernel I, $\pm P$. Velu's theorem gives the isogenous curve as

$$E_m^* : y^2 = x^3 + ax^2 - 9bx + (-27c - 8ab). \qquad \ldots(3.3)$$

Putting (3.2) and (3.3) in the Weierstrass' normal form and then equating their absolute invariants gives, as before, the following equation:

$$\left(\frac{2a^3 - 9ab + 27c}{2a^3 - 135ab - 27^2 c}\right)^2 = \left(\frac{a^2 - 3b}{a^2 + 27b}\right)^3$$

i.e. say $(N^2)^3 = (N^3)^2$. $\qquad \ldots(3.4)$

Now we know that $E_3 : y^2 = x^3 + c$ must emerge as a solution, i.e. $a = b = 0$ is a solution. Putting this in (3.4) gives $27c/-27^2 c = N^3$ giving $N = -1/3$. Now substitute for $c = b^2/4a$ and let $\theta = a^2/b$. (3.4) gives

$$\left(\frac{8\theta^2 - 36\theta + 27}{8\theta^2 - 540\theta - 27^2}\right)^2 = (N^3)^2$$

and

$$\left(\frac{\theta - 3}{\theta + 27}\right)^3 = (N^2)^3$$

and eliminating θ gives

$$(N-1)[8(1 + N + N^2)(1 + 9N^2)^2 - 12(1 + N)(1 + 9N^2)(1 - 15N^3) + 3(1 + N)^2(1 - N)(1 + 27N^3)] = 0. \qquad \ldots(3.5)$$

$N = 1$ gives $b = 0$ whence $c = 0$ and E_m becomes $y^2 = x^3 + ax^2$ which is of genus 0. $N = -1/3$ has already been shown to be a root and trial and error gives $1/9$ as a root. Dividing out we are left with $81N^4 + 63N^3 + 28N^2 + 7N + 1 = 0$

which factors as $(9N^2 + 5N + 1)(9N^2 + 2N + 1) = 0$ giving $(-5 \pm \sqrt{-11})/18$ and $(-1 \pm 2\sqrt{-2})/9$ as roots.

$N = 1/9$ gives $b = 8a^2/27$, so that $c = 16a^3/27^2$ and so E_m is given by $y^2 = x^3 + ax^2 + 8a^2x/27 + 16a^3/27^2$ and on multiplying by 27^2 and letting $27y \to y$, $9x \to x$ this becomes $y^2 = (x + a)(x + 4a)^2$ which is of genus 0.

$N = (-1 \pm 2\sqrt{-2})/9$ gives similarly the curve $y^2 = x^3 + ax^2 + 2(2 - 5\sqrt{-2})a^2x/27 - 2(23 + 10\sqrt{-2})a^3/27$, which can be reduced to $y^2 = x^3 - 30a^2x + 56a^3$ which is just E_2 in the normal form.

$N = (-5 \pm \sqrt{-11})/18$ gives the curve

$$y^2 = x^3 + ax^2 + (4 - \sqrt{-11})a^2x/27 + (5 - 8\sqrt{-11})a^3/27^2 \cdot 4 \quad \ldots(3.6)$$

and the mapping

$$x \to (11 + \sqrt{-11}) \cdot x/9 \cdot 11 \cdot 8 - a/3$$
$$y \to (11 + 4\sqrt{-11})^{1/2} \cdot y/27 \cdot 11 \cdot 8 \quad \ldots(3.7)$$

takes this to the required curve E_{11}, viz.

$$E_{11} : y^2 = x^3 - 33 \cdot 32\, a^2x + 7 \cdot 16 \cdot 11^2\, a^3. \quad \ldots(3.8)$$

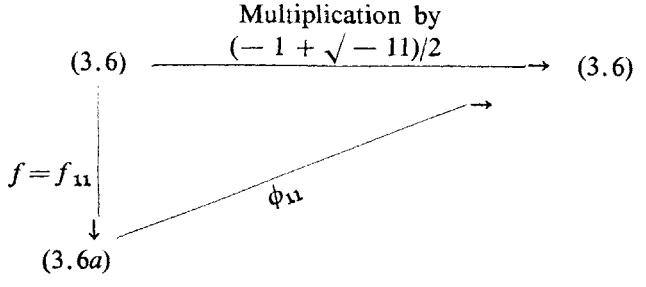
Next Velu's theorem says (3.6) is isogenous by the map f_{11} say to

$$y^2 = x^3 - ax^2 - (4 - \sqrt{-11})a^2x/3 - [(133 - 40\sqrt{-11})a^3/4\,27]. \quad \ldots(3.6a)$$

The point (x, y) of (3.6) is mapped to $f_{11}(x, y) = (x', y')$ of (3.6a) where

$$x' = x + 2(4 - \sqrt{-11}) \cdot a^2/27x + (5 - 8\sqrt{-11}) \cdot a^3/27^2 x^2$$
$$y' = y - 2(5 - 8\sqrt{-11}) \cdot a^3 y/27^2 x^3 - 2(4 - \sqrt{-11}) \cdot a^2 y/27 x^2.$$

The kernel of f_{11} is I, $(0, \pm (4 - \sqrt{-11}) \cdot a\sqrt{a}/54)$. As before we have the following situation:



Here ϕ_{11} is

$$\begin{cases} x \to (-5 + \sqrt{-11}) \cdot x/2 + (-7 + \sqrt{-11}) \cdot a/6 \\ y \to (4 + \sqrt{-11}) \cdot y \end{cases}.$$

Hence

$$\frac{-1+\sqrt{-11}}{2}(x,y) = \phi_0 f(x,y) = \phi(x',\ y')$$

$$= \big([x + 2(4-\sqrt{-11})a^2/27x + (5-8\sqrt{-11})a^3/27^2x^2 - (-7+\sqrt{-11})a/6]/(-5+\sqrt{-11})/2,$$
$$y[1-(5-8\sqrt{-11})\,.\,2a^3/27^2x^3 - 2(4-\sqrt{-11}).$$
$$\times a^2/27x^2]/(4+\sqrt{-11})\big).$$

Now we want such a formula on (3.8) where the map (3.7) connects (3.6) with (3.8). Working out the details we arrive at the following theorem:

Theorem 3—The curve E_{11} with End equal to the full ring of integers of $Q(\sqrt{-11})$ is given by

$$y^2 = x^3 - 33.32\,.\,a^2\,.\,x + 11^2\,.\,7\,.\,16\,.\,a^3,$$

and for a generic point (x, y) of this we have $(-1+\sqrt{-11}/2)(x,y) = (X, Y)$ where

$$X = \left(\frac{-(5+\sqrt{-11})[x^3 - 4(11-\sqrt{-11})ax^2 + 88(11-7\sqrt{-11})a^2x - 704(11-14\sqrt{-11})a^3}{18[x-2(11-\sqrt{-11})a]^2}\right)$$

$$Y = \left(\frac{(4-\sqrt{-11})[x^3 - 6(11-\sqrt{-11})ax^2 + 88.3(3+\sqrt{-11})a^2x + 11.64(11-6\sqrt{-11})a^3)]\,.\,y}{27[x-2(11-\sqrt{-11})a]^3}\right)$$

Reference

Velu, J. (1971). Isogenies entre courbes elliptiques. *C.R. Acad. Paris*, pp. 238–41.