J. Austral. Math. Soc. **24** (Series A) (1977), 286–295.

THE DIOPHANTINE EQUATION $y^2 = x(x^2 + 21Dx + 112D^2)$ AND THE CONJECTURES OF BIRCH AND SWINNERTON-DYER

A. R. RAJWADE

(Received 18 November 1974; revised 11 May 1976)

Communicated by Jane Pitman

Abstract

Some of the conjectures of Birch and Swinnerton-Dyer have been verified for curves with complex multiplication by $\sqrt{-7}$. The L-function $L_D(1)$ of such curves at the point $s = 1$ is written as a finite sum of division values of $\wp$-functions and the integer property of $L_D(1)$ is proved.

0. Introduction

In 1965 Birch and Swinnerton-Dyer made some conjectures about general elliptic curves

$$E: y^2 = x^3 + ax + b \qquad (a, b \in \mathbf{Z}).$$

(See Birch and Swinnerton-Dyer (1963, 1965) and Swinnerton-Dyer (1967).) Roughly speaking, these tell us that the group E_Q of rational points on E is described to a great extent by the L-function of E. The evidence they produced in support of these conjectures was then largely derived from curves E_1 with $\mathrm{End}(E_1) = \mathbf{Z}[\sqrt{-1}]$ (see Birch and Swinnerton-Dyer (1965)). Further evidence was obtained by Rajwade (1968, 1969) for the curves E_2 with $\mathrm{End}(E_2) = \mathbf{Z}[\sqrt{-2}]$ and for E_3 with $\mathrm{End}(E_3) = \mathbf{Z}[\omega]$ ($\omega = (-1 + \sqrt{-3})/2$) and by Stephens (1968) for the curve $X^3 + Y^3 = D$. See also Damerell (1970, 1971). In all thse verifications, $L_E(1)$, the value of the L-function of E at 1, is calculated in finite form in terms of Weierstrass's $\wp$-function. Subsequently it was realized that a different and in many cases (certainly in principle) simpler method may be used when E is parametrizable by L-functions; see Birch and Swinnerton-Dyer (1969), Manin (1971), Slater (1974), and Swinnerton-Dyer (1967). On account of Weil's conjecture that every elliptic curve is isogenous to a curve that can be parametrized by a pair

https://doi.org/10.1017/S1446788700020309 Published online by Cambridge University Press

of functions on $H/\Gamma_0(N)$, for some N, it seems that this simpler method is applicable for all E.

The original method giving $L_E(1)$ in terms of the Weierstrass' $\boldsymbol{p}$-function was applied only to curves with complex multiplication by $\sqrt{-1}$, $\sqrt{-2}$, $\sqrt{-3}$. All these three cases have special features even amongst curves E_m with complex multiplication by $\sqrt{-m}$, i.e., with End(E_m) equal to a subring of finite index in the ring of integers of $\boldsymbol{Q}(\sqrt{-m})$ $(m = 1,2,3,7,11,19,43,67,163)$. The special features being that $\boldsymbol{Q}(\sqrt{-1})$ and $\boldsymbol{Q}(-1+\sqrt{-3})/2$ have 4 and 6 units respectively while $\sqrt{-1}$ and $(-1+\sqrt{-3})/2$, the generators of these fields are themselves units. Also 2 being always a special prime, $\boldsymbol{Q}(\sqrt{-2})$ is bound to have special features. The m that remain, however, are pretty well alike: $m \equiv 1 (\text{mod}\, 4)$, $\boldsymbol{Q}(\sqrt{-m})$ has only 2 units ± 1. It seems, therefore, that $m = \sqrt{-7}$ is the simplest genuinely typical case. In this paper we verify some of the conjectures of Birch and Swinnerton-Dyer for curves E_7 with End$(E_7) =$ the full ring of integers of $\boldsymbol{Q}(\sqrt{-7})$ by the original $\boldsymbol{p}$-function method. As many of the results for the case $m = 7$ are exactly like one (or more) of the cases $m = 1,2,3$, one realizes that after all the $\boldsymbol{p}$-function method is itself fairly quick and will cover all the cases of complex multiplication, in principle fully but in detail in most places, as we shall see. It therefore seems worthwhile to examine this typical case. Wherever proofs of results are exactly like the corresponding ones in any of the cases $m = 1,2,3$, we omit them entirely; if the proof is genuinely different from all these cases then we give it and remark whether or not it can be adapted in the remaining cases $m = 11,19,43,67,163$.

The shape of E_7 and multiplication by $\sqrt{-7}$ of a generic point (x, y) of E_7 may be obtained by the use of $\boldsymbol{p}$-functions and is classical. In any case once we have the formulae, their validity may be checked by easy computations. The formulae are:

$$(0.1) \qquad E_7\colon y^2 = x(x^2 + 21Dx + 112D^2) \qquad (D \in Z)$$

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

$$(0.2) \qquad \begin{cases} X = \dfrac{-(3+\sqrt{-7})(x + 2D(7-\sqrt{-7}))^2}{8(x + \frac{1}{2}(21-\sqrt{-7})D)} \\[2ex] Y = \dfrac{(5-\sqrt{-7})y(x + D(7+\sqrt{-7}))(x + 2D(7-\sqrt{-7}))}{16(x + \frac{1}{2}(21-\sqrt{-7})D)^2} \end{cases}$$

We call a prime p good if $p \nmid 14D$. The curve (0.1) has a good reduction at all the good primes and our first object is to determine the number N_p of points on the complete curve

https://doi.org/10.1017/S1446788700020309 Published online by Cambridge University Press

$$(0.1)' \qquad y^2z = x(x^2 + 21Dxz + 112D^2z^2), \qquad \text{modulo } p.$$

We remark that the method of getting the N_p for E_7 is not immediately adaptable for the remaining m as the $\sqrt{-m}$-division points on E_m need to be explicitly calculated if we are to follow a similar method. For the present case we have managed to calculate the $\sqrt{-7}$-division points on (0.1) explicitly. We now turn to these calculations as an aid to the determination of N_p.

1. Determination of the $\sqrt{-7}$-division points on (0.1) and N_p

From $\frac{1}{2}(-1+\sqrt{-7})\,(x,y) = (X, Y)$ it follows that $\frac{1}{2}(-1-\sqrt{-7})\,(x,y) = (\bar{X}, \bar{Y})$, whence $\frac{1}{2}(1+\sqrt{-7})\,(x,y) = (\bar{X}, -\bar{Y})$. Adding gives

$$\sqrt{-7}\,(x,y) = (X, Y) + (\bar{X}, -\bar{Y}).$$

The $\sqrt{-7}$-division points on (0.1) are those (x, y) for which $\sqrt{-7}\,(x,y) = \underline{I}$, the point at infinity, i.e., for which $X = \bar{X}$, i.e., for which $\mathrm{Im}(X) = 0$. This gives the cubic:

$$(1.1) \qquad x^3 + 28Dx^2 + 2.112D^2x + 4.112D^3 = 0.$$

If x_1, x_2, x_3 are the roots of this then the $\sqrt{-7}$-division points are $\underline{I}$, $(x_i, \pm y_i)$ $i = 1, 2, 3$. Write x for $x/-4D$, then (1.1) can be written as

$$(1.2) \qquad x^3 - 7x^2 + 14x - 7 = 0.$$

To obtain the roots of this we expand $\sin 7\theta$ in terms of powers of $\sin\theta$. We have $\sin 7\theta = 7\sin\theta - 56\sin^3\theta + 112\sin^5\theta - 64\sin^7\theta$, hence $2\sin 7\theta = 7(2\sin\theta) - 14(2\sin\theta)^3 + 7(2\sin\theta)^5 - (2\sin\theta)^7$. It follows that the roots of $7x - 14x^3 + 7x^5 - x^7 = 0$ are

$$0, \quad \pm 2\sin(2\pi/7), \quad \pm 2\sin(4\pi/7), \quad \pm 2\sin(6\pi/7)$$

and hence those of (1.2) are $4\sin^2(2\pi/7)$, $4\sin^2(4\pi/7)$, $4\sin^2(6\pi/7)$. Thus x_1, x_2, x_3 are given by $-16D.\sin^2(2\pi/7)$, $-16D.\sin^2(4\pi/7)$, $-16D.\sin^2(6\pi/7)$. The y-coordinates are found as follows: we have $y^2 = x(x^2 + 21Dx + 112D^2)$ where x satisfies (1.1). Substituting for x^3 from (1.1) gives, on simplification $y^2 = -7D(x+8D)^2$. Hence we have the following theorem:

THEOREM 1. *The $\sqrt{-7}$-division points on* (0.1) *are the following*

$$\underline{I}, \quad (-16D.\sin^2(2\pi/7), \pm 8\sqrt{7}.(-D)^{3/2}.\cos(4\pi/7)),$$

$$(-16D.\sin^2(4\pi/7), \pm 8\sqrt{7}.(-D)^{3/2}.\cos(\pi/7)),$$

$$(-16D.\sin^2(6\pi/7), \pm 8\sqrt{7}.(-D)^{3/2}.\cos(5\pi/7)).$$

https://doi.org/10.1017/S1446788700020309 Published online by Cambridge University Press

Now let $\underline{P}$ be one of these, say $\underline{P} = (-16D.\sin^2(2\pi/7), 8\sqrt{7}.(-D)^{3/2}.\cos(4\pi/7))$. Then the remaining five proper $\sqrt{-7}$-division points are just $-\underline{P}, \pm 2\underline{P}, \pm 3\underline{P}$. We now determine which are which. The formula for the duplication of a point on our curve is

$$2(x, y) = \left(\frac{(x^2 - 112D^2)^2}{4y^2}, \frac{(x^2 - 112D^2)(x^2 + 14Dx + 56D^2)(x^2 + 28Dx + 224D^2)}{8y^3}\right).$$

This is easily computed. Using this we find that

$$(2\underline{P})_x = [16^2D^2\sin^4(2\pi/7) - 112D^2]^2/[-4.64.7D^3\cos^2(4\pi/7)],$$

and letting $\lambda = 4\sin^2(2\pi/7)$ this equals $-D(\lambda^2 - 7)^2/7(1 - \lambda/2)^2$ and we have to find out whether this equals $-16D\sin^2(4\pi/7)$ or $-16D\sin^2(6\pi/7)$. It turns out that the latter works, i.e.,

$$2\underline{P} = (-16D\sin^2(6\pi/7), -8\sqrt{7}(-D)^{3/2}.\cos(5\pi/7)).$$

Similarly $4\underline{P}$ $(= -3\underline{P})$ may be worked out. Hence we have the following stronger result. If

$$\underline{P} = (-16D.\sin^2(2\pi/7), 8\sqrt{7}(-D)^{3/2}.\cos(4\pi/7))$$

then

$$2\underline{P} = (-16D.\sin^2(6\pi/7), -8\sqrt{7}(-D)^{3/2}.\cos(5\pi/7))$$

and

$$3\underline{P} = (-16D.\sin^2(4\pi/7), 8\sqrt{7}(-D)^{3/2}.\cos(\pi/7)),$$

and if we let $\zeta = e^{\pi i/7}$ then we have the following

THEOREM 2. *The six proper $\sqrt{-7}$-division points on the curve* (0.1) *are* $\pm\underline{P}, \pm 2\underline{P}, \pm 3\underline{P}$, *where*

$$\underline{P} = [4D(\zeta^2 - \zeta^{-2})^2, 4\sqrt{7}.(-D)^{3/2}(\zeta^4 + \zeta^{-4})]$$

$$2\underline{P} = [4D(\zeta^6 - \zeta^{-6})^2, -4\sqrt{7}.(-D)^{3/2}(\zeta^5 + \zeta^{-5})]$$

$$3\underline{P} = [4D(\zeta^4 - \zeta^{-4})^2, 4\sqrt{7}.(-D)^{3/2}(\zeta + \zeta^{-1})].$$

We make an application of these $\sqrt{-7}$-division points and prove the following

THEOREM 3. *Let N_p be the number of points on the projective version of* (0.1), *then*

https://doi.org/10.1017/S1446788700020309 Published online by Cambridge University Press

$$N_p = \begin{cases} p+1 \textit{ if } p \textit{ is not a norm i.e. if } p \equiv 3,5,13 \ (\textit{mod } 14), \\ \\ p+1-(D/\pi)_2.\bar{\pi}-(D/\bar{\pi})_2.\pi \textit{ if } p \textit{ is a norm, i.e., if } p \equiv 1,9,11 \ (\textit{mod } 14 \end{cases}$$

where $p = \pi\bar{\pi}$ *is the splitting of* p *in the integers of* $Q(\sqrt{-7})$ *and the factors* π, $\bar{\pi}$ *are normalized so that* π, $\bar{\pi} \equiv 1, 2$ *or* 4 (*mod* $\sqrt{-7}$), *and where the symbol* $(D/\pi)_2$ *is the quadratic residue symbol in* $Z[\sqrt{-7}]$; *we use the symbol* (α/β) $(\alpha, \beta \in Z)$ *to denote the ordinary Legendre symbol.*

We note that for the three cases $p \equiv 1, 9, 11$ (mod 14) the factors π, $\bar{\pi}$ of p respectively satisfy the conditions

$$\pi,\ \bar{\pi} \equiv 1,6;\ 3,4;\ 2,5 \ (\text{mod } \sqrt{-7})$$

and in the theorem one possibility is selected out of each of the two. Note also that the selected possibilities, viz., $1, 2, 4$ (mod $\sqrt{-7}$) form the unique subgroup of index 2 in the group of the non-zero residues mod $\sqrt{-7}$.

Proof. To prove the theorem we use a well known result of Deuring's (see Deuring (1941)), namely:

$$N_p = \begin{cases} p+1 \text{ if } p \text{ is not a norm} \\ \\ p+1-\pi-\bar{\pi} \text{ if } p = \pi\bar{\pi} \text{ is a norm.} \end{cases}$$

The problem is the normalization of π and $\bar{\pi}$ since p also equals $(-\pi)(-\bar{\pi})$. Deuring's theorem also tells us that *that* sign $+\pi$ or $-\pi$ is the correct one for which multiplication of points of (0.1) by the π with the correct sign has the same effect as has the Frobenius automorphism

$$f_p : (x, y) \rightarrow (x^p, y^p) \ (\text{mod } p).$$

We try the action of the Frobenius map on the points of Theorem 2. We split cases as follows:

Case 1. $p \equiv 1$ (mod 14).

Let $\underline{P} = (\lambda, \mu)$, then $f_p(\underline{P}) = (\lambda^p, \mu^p)$. We have $\lambda^p \equiv \lambda$ (mod p) and $\mu^p \equiv (-7D/p).\mu$ (mod p). Hence $f_p(\underline{P}) = (-7D/p).\underline{P}$, but also equals $\pi\underline{P}$ by the very definition of π with the correct sign. Hence $(\pi - (-7D/p)).\underline{P} = \underline{I}$ and $\underline{P}$ being a proper $\sqrt{-7}$-division point we get $\pi \equiv (-7D/p)$ (mod $\sqrt{-7}$), i.e., the normalized π is $(-7D/p).\pi$ where $\pi \equiv 1$ (mod $\sqrt{-7}$).

Case 2. $p \equiv 9$ (mod 14).

Here $\zeta^p = -\zeta^2$ and so as before it follows that $f_p(\underline{P}) = (-7D/p).(-3\underline{P})$ and this equals $\pi\underline{P}$ again whence $\pi \equiv -3(-7D/p)$ (mod $\sqrt{-7}$). Thus the normalized π is $(-7D/p).\pi$ where $\pi \equiv -3$ (mod $\sqrt{-7}$).

https://doi.org/10.1017/S1446788700020309 Published online by Cambridge University Press

Case 3. $p \equiv 11 \pmod{14}$.

As above, since $\zeta^p = -\zeta^4$ we find that the normalized π is $(-7D/p).\pi$ where $\pi \equiv 2 \,(\text{mod}\, \sqrt{-7})$.

Thus in all cases we have

$$N_p = p + 1 - (-7D/p).\pi - (-7D/p).\bar{\pi},$$

where π, $\bar{\pi} = 1, 2, -3 \,(\text{mod}\, \sqrt{-7})$. This gives the theorem since for any rational integer d, $(d/p) = (d/\pi)_2 = (d/\bar{\pi})_2$ and $7 = -(\sqrt{-7})^2$.

2. The L-function of E_7

THEOREM 4.

$$L_D(s) = \sum_{\lambda \equiv 1,2,4 \,(\text{mod}\, \sqrt{-7})} (D/\lambda)(\bar{\lambda}/(N\lambda)^s)$$

PROOF. As for the cases $m = 1, 2, 3$. See Birch and Swinnerton-Dyer (1965) and Rajwade (1968, 1969).

Now write $D = \Delta F$ where F is the product of powers of $\sqrt{-7}$, 2 and units ± 1 of $\boldsymbol{Z}[\frac{1}{2}(1 + \sqrt{-7})]$, and where all the primes in Δ (necessarily to the first power since without loss of generality D is square-free) are normalized $\equiv 1, 2, 4 \,(\text{mod}\, \sqrt{-7})$. Let $\varepsilon = (-1/\Delta)_2$ and let K be such that (i) $\sqrt{-7} \mid K$ (ii) $(\varepsilon F/\lambda)$ depends on the class of $\lambda \bmod K$. Then we have

THEOREM 5. $K = 2\sqrt{-7}$. (Or we may take $K = 14$ if we wish.)

PROOF. Easily worked out by considering reciprocity laws in $\boldsymbol{Z}[\frac{1}{2}(1 + \sqrt{-7})]$.

Now let B be a set of representatives for the residue classes $\bmod \Delta$ and C a set of representatives for those residue classes $\bmod K$ which are $\equiv 1, 2, 4 (\text{mod}\, \sqrt{-7})$. Then λ may be written as

$$\begin{aligned} \lambda &= K\Delta\mu + (K\beta + \Delta\gamma), \quad \beta \in B, \quad \gamma \in C, \quad \mu \in \boldsymbol{Z}[\tfrac{1}{2}(1 + \sqrt{-7})], \\ &= K\Delta\mu + \rho, \quad \text{say.} \end{aligned}$$

We now have the following

THEOREM 6.

$$L_D(s) = \frac{\overline{K\Delta}}{(N(K\Delta))^s} \sum_{\beta,\gamma} (D/\rho)_2 \sum_{\mu} \frac{\bar{\rho}/\bar{K}\bar{\Delta} + \bar{\mu}}{(N(\rho/K\Delta + \mu))^s}.$$

PROOF. As for the case $m = 2, 3$. See Rajwade (1968, 1969).

We have now to continue this analytically as far as $s = 1$. Proceeding as for the case $m = 2$ (see Rajwade (1968)), we obtain the following

https://doi.org/10.1017/S1446788700020309 Published online by Cambridge University Press

THEOREM 7. Let $\Delta \neq 1$ and let Θ and $\sqrt{-7}\,\Theta$ be the periods of the Weierstrass' p-function $p(z)$ which satisfies the equation

$$p'^2(z) = p(z).(p^2(z) + 21sp(z) + 112s^2)$$

for some convenient s (which does not matter at this stage but which will be fixed later). Then

$$L_D(1) = \frac{\Theta}{2K\Delta} \sum_{\beta,\gamma} (D/\rho)_2 . \left(\frac{p'(\Theta\beta/\Delta) - p'(\Theta\gamma/K)}{p(\Theta\beta/\Delta) - p(\Theta\gamma/K)}\right).$$

PROOF. As for the case $m = 2$ (See Rajwade (1968)).

We have used the following results (analogous to the cases $m = 2, 3$):

1. $(s-1)\zeta_{Q(\sqrt{-7})}(s) \to \pi/\sqrt{7}$ as $s \to 1+$.
2. The sum $\Sigma_{\mu \in Z[\frac{1}{2}(1+\sqrt{-7})], \mu \neq 0}\, \bar{\mu}/\mu\,|\mu|^{2s} \to$ a finite limit $= \mathfrak{S}$, as $s \to 1+$.

REMARK. The finitely many cases $\Delta = 1$ require a lot of calculations and are treated in the appendix. These will get more and more messy as m takes values $11, 19, \cdots$.

3. The integer property of $L_D(1)$

THEOREM 8. *Let $D > 1$ be a square-free integer and Θ the real period of the Weierstrass' p-function satisfying*

$$p'^2(z) = p(z)(p^2(z) + 21p(z) + 112).$$

Then $14\sqrt{D}.L_D(1)/\Theta$ and $14\sqrt{7D}.L_{-D}(1)/\Theta$ are rational integers.

REMARK. From the formula for $L_D(1)$ in theorem 7 it follows that $L_{-D} = L_{7D}$ since $7 = -(\sqrt{-7})^2$. Hence it is enough to show that the first of the two expressions of theorem 8 is a rational integer. We shall be taking $K = 14$. As for the cases $m = 2, 3$ (see Rajwade (1968, 1969)), we let $k = Q(\sqrt{-7})$ and $\mathfrak{K} = k(\mathfrak{A})$, where the $\mathfrak{A}$ are the 14Δ-division points on the curve

$$y^2 = x(x^2 + 21sx + 112s^2), \tag{3.1}$$

where we shall be taking $s = 1$, an essential choice as we shall soon see. Then $\mathfrak{K}/k$ is normal and $\mathrm{Gal}(\mathfrak{K}/k)$ is isomorphic to a subgroup of the multiplicative group $G^*_{14\Delta}$ of residues mod 14Δ prime to 14Δ in $Z[\frac{1}{2}(1+\sqrt{-7})]$. If $\tau \in \mathrm{Gal}(\mathfrak{K}/k)$, we let the map $\mathrm{Gal}(\mathfrak{K}/k) \to G^*_{14\Delta}$ take $\tau \to t$. For each such t, there exists a unit $e(t) = \pm 1$ such that $e(t).t \equiv 1, 2, 4 \pmod{\sqrt{-7}}$, for if t is not already $\equiv 1, 2, 4 \pmod{\sqrt{-7}}$ then $-t$ will be. We shall show that if we take $s = 1$ in (3.1) then $e(t) = 1$ always. In other words we have the following

Normalization Lemma. *If $s = 1$ then the automorphisms τ of $\mathfrak{K}/k$ with $\tau \to t$, $e(t) = -1$ are inadmissible (i.e. do not exist).*

Proof. Write $P = (x_P, y_P)$ the proper $\sqrt{-7}$-division point on (0.1) given by Theorem 3. Write the others as $\pm 2P = (x_{2P}, \pm y_{2P})$, $\pm 3P = (x_{3P}, \pm y_{3P})$. Let

$$\begin{aligned}\eta &= y_P + y_{2P} + y_{4P}\\ &= 4s\sqrt{-7s}.(\zeta - \zeta^2 + \zeta^3 - \zeta^4 + \zeta^5 - \zeta^6), \text{ by Theorem 3,}\\ &= 4s\sqrt{-7s}.X \text{ say.}\end{aligned}$$

The simplest way to calculate X is the following: On squaring X we get $X^2 = 6 - 5X$ whence $(X+6)(X-1) = 0$ giving $X = 1$ or -6. Hence $\mathrm{Real}(X) = 1$ or -6. But now

$$\mathrm{Real}(X) = \cos(\pi/7) - \cos(2\pi/7) + \cdots - \cos(6\pi/7)$$

and so $|\mathrm{Real}(X)| < 1 + 1 + \cdots + 1 = 6$. It follows that $X = 1$ (and not -6). So that $\eta = 4s\sqrt{-7s}$. By choosing $s = 1$ we see that $\eta \in \boldsymbol{Q}(\sqrt{-7})$ so that $\tau\eta = \eta$ always. However, since $\eta = y_P + y_{2P} + y_{4P}$ we see that

$$\tau\eta = \begin{cases} \eta & \text{if } \tau \to t \equiv 1, 2, 4 \pmod{\sqrt{-7}} \\ -\eta & \text{if } \tau \to t \equiv -1, -2, -4 \pmod{\sqrt{-7}}. \end{cases}$$

It follows that $\tau \to t \equiv -1, -2, -4 \pmod{\sqrt{-7}}$ are inadmissible. This completes the proof of the normalization lemma.

The remaining points in the proof of Theorem 8 are exactly the same as for the case $m = 2$ (or 3). The exact ennunciation of the corresponding theorems A and B read as follows:

Theorem A. *Suppose the hypothesis as in theorem 8 holds; then $\sqrt{D}.L_D(1)/\Theta$ is a rational number.*

Theorem B (Weaker Form). $\dfrac{14\Delta^{1/2}.L_D(1)}{\Theta}\cdot(7\Delta)^{5/8}$ *is an algebraic integer.*

Remark. All this would go through for the other m except the normalization lemma which would need case wise handling.

We now look at the appendix.

https://doi.org/10.1017/S1446788700020309 Published online by Cambridge University Press

Appendix

$L_D(1)$ *when* $\Delta = 1$.

When $\Delta = 1$ we have only four cases viz. $\varepsilon F = \pm 1, \pm 2$, since $\pm 7 = \mp(\sqrt{-7})^2$ and D is square-free not only in $\boldsymbol{Z}$ but also in $\boldsymbol{Z}[\frac{1}{2}(1+\sqrt{-7})]$.

We proceed as in paragraph 5 of Rajwade (1968). The definitions and results needed here are exactly the same as for the cases $m = 2, 3$. We find that β takes just one value, viz. 1. And γ takes twelve values, viz., the residues $\bmod 2\sqrt{-7}$ that are $\equiv 1, 2, 4 \pmod{\sqrt{-7}}$; they are: 2, 4, 8, $2+\sqrt{-7}$, $4+\sqrt{-7}$, $8+\sqrt{-7}$, $\frac{1}{2}(-3+\sqrt{-7})$, $\frac{1}{2}(1+\sqrt{-7})$, $\frac{1}{2}(9+\sqrt{-7})$, $\frac{1}{2}(-3+3\sqrt{-7})$, $\frac{1}{2}(1+3\sqrt{-7})$, $\frac{1}{2}(9+3\sqrt{-7})$.

$\alpha = 1 + \gamma/2\sqrt{-7}$, $(D/\rho)_2 = (F/\gamma)_2$ and so we get

$$L_D(1) = \frac{1}{K}\sum_{\gamma}(F/\gamma)_2.\left[\xi(1+\gamma/K) - 2(1+\bar{\gamma}/\bar{K})\cdot\frac{\pi}{\sqrt{7}} - \mathfrak{S}(1+\gamma/K)\right],$$

where

$$\xi(\alpha) = \frac{1}{\alpha} + \sum_{\substack{\mu \in \boldsymbol{Z}[\frac{1}{2}(1+\sqrt{-7})] \\ \mu \neq 0}}\left(\frac{1}{\mu+\alpha} - \frac{1}{\mu} + \frac{\alpha}{\mu^2}\right)$$

is the Weierstrass' ξ-function with periods 1, $\sqrt{-7}$.

We also use:

(i) $\xi(1+u) = \xi(u) + 2\pi/\sqrt{7} + \mathfrak{S}$

(ii) $\xi(1/2) = \pi/\sqrt{7} + \mathfrak{S}/2$

(iii) $\sqrt{-7}.\xi(1/2) - \xi(\sqrt{-7}/2) = \pi i$

(iv) $\xi(u+v) = \xi(u) + \xi(v) + \dfrac{\Theta}{2}\left(\dfrac{\boldsymbol{p}'(\Theta u) - \boldsymbol{p}'(\Theta v)}{\boldsymbol{p}(\Theta u) - \boldsymbol{p}(\Theta v)}\right)$.

Using all this information we can get $L_D(1)$ (for $\Delta = 1$) purely in terms of the $\boldsymbol{p}$-functions.

References

B. J. Birch and H. P. F. Swinnerton-Dyer (1963), 'Notes on elliptic curves I', *J. Reine Angew. Math.* **212**, 7–25.

B. J. Birch and H. P. F. Swinnerton-Dyer (1965), 'Notes on elliptic curves II', *J. Reine Angew. Math.* **218**, 79–108.

B. J. Birch (1969), 'Elliptic curves, a progress report', *Proc. Symp. Pure Math.* **20**, 396–401.

R. M. Damerell (1970, 1971), '*L*-functions of elliptic curves with complex multiplication I and II', *Acta Arith.* **17** and **19**, 278–301 and 311–317, respectively.

M. Deuring (1941), 'Die Typen der Multiplikatorenringe Elliptischer Funktionenkorper', *Abh. Math. Sem. Univ. Hamburg*, **14**, 197–272.

Ju I. Manin (1971), 'Cyclotomic fields and modular curves', *Uspehi Mat. Nauk* **26**, 7–71 (in Russian), *Russian Math. Surveys* **26**, 7–78 (in English).

A. R. Rajwade (1968), 'Arithmetic on curves with complex multiplication by $\sqrt{-2}$', *Proc. Camb. Phil. Soc.* **64**, 659–672.

A. R. Rajwade (1969), 'Arithmetic on curves with complex multiplication by the Eisenstein integers', *Proc. Camb. Phil. Soc.* **65**, 59–73.

J. B. Slater (1974), 'Determination of L-functions of elliptic curves parametrized by modular functions', *Proc. Lond. Math. Soc.* **28**, Part 3, 439–456.

N. M. Stephens (1968), 'The Diophantine equation $X^3 + Y^3 = DZ^3$ and the conjectures of Birch and Swinnerton-Dyer', *J. Reine Angew. Math.* **231**, 121–162.

H. P. F. Swinnerton-Dyer (1967), 'The conjectures of Birch and Swinnerton-Dyer and of Tate', *Proc. Conf. Local Fields* (Driebergen) 1966, 132–157 (*Springer*, Berlin).

Mathematics Department,
Panjab University,
Chandigarh,
India.

https://doi.org/10.1017/S1446788700020309 Published online by Cambridge University Press