ACTA ARITHMETICA
XIX (1971)

L-functions of elliptic curves with complex multiplication, II

by

R. M. DAMERELL (London)*

§ 7. Division values of elliptic functions. This paper, like Part I [3], is concerned with certain Hecke zeta functions defined over a complex quadratic ring $\mathbf{S}$. It was proved there that for suitable values of x and s_0, the number

$$\Theta = \zeta(s_0, \lambda)\pi^{n/2-s_0}/x^n$$

is algebraic. In this paper we find an algebraic integer γ such that $\gamma\Theta$ is an algebraic integer. The set of such γ is a principal ideal ($[\alpha]$, say) in the ring of algebraic integers. The value of α is not known, except that α divides γ, so the value of γ given here is not necessarily the best possible. The main result is Theorem 2, stated in § 8. Similar results have been proved in some special cases, see [1], [5], [6], sometimes with better values of γ.

We now adopt the notation of § 2, with some changes. The letter I will denote any algebraic integer, but it will not have any fixed value. Let Γ be a period lattice, $\hat{z}$ a point of finite order (m, say) modulo Γ, and $\mathbf{F}$ an algebraic number field containing $g_2, g_3, \wp(\hat{z}), \wp'(\hat{z})$. We assume that $\frac{1}{12}g_2(\Gamma) = I$ and $\frac{1}{4}g_3(\Gamma) = I$.

Generalizing results of Lutz and Nagell, Cassels has proved the following ([2], Theorem 4):

There is an integral ideal $\mathfrak{t}$ in $\mathbf{F}$ such that $\mathfrak{t}^2\wp(\hat{z})$ and $\frac{1}{2}\mathfrak{t}^3\wp'(\hat{z})$ are integral, and

If $m = p^r$, $p \neq 2$ or 3, then $\mathfrak{t}^{p^r-p^{r-1}}|p$,
If $m = 3^r$, then $\mathfrak{t}^{3^{2r}-3^{2r-2}}|3$,
For all other m, $\mathfrak{t} = 1$.

It is convenient to weaken this result so as to have a single formula valid for all m. The weakened result is:

LEMMA 7.1.

$$m^{1/2}\wp(\hat{z}) = I \quad \text{and} \quad \tfrac{1}{2}m^{3/4}\wp'(\hat{z}) = I.$$

We now apply this result to the functions defined in Part 1.

*Most of this work was done while the author was a research student at the University of Cambridge.

LEMMA 7.2. *Let $h(z)$ be the function discussed in § 4. Then*

$$m^{5/4}h(\hat{z}) = I.$$

Proof. $\wp(z)$ satisfies the addition formula

$$\wp(u+v) = \tfrac{1}{4}\left(\frac{\wp'(u)-\wp'(v)}{\wp(u)-\wp(v)}\right)^2 - \wp(u)-\wp(v)$$

(Fricke [4], page 160). Hence

$$\frac{\wp'(u)-\wp'(v)}{\wp(u)-\wp(v)} = \pm 2\sqrt{\{\wp(u+v)+\wp(u)+\wp(v)\}}.$$

By Lemma 4.3 and equation (4.6),

$$h(\hat{z}) = H_m(\hat{z}) = \frac{1}{2m}\left\{\frac{\wp''(\hat{z})}{\wp'(\hat{z})} - \sum_{r=2}^{m-2}\frac{\wp'(r\hat{z})-\wp'(\hat{z})}{\wp(r\hat{z})-\wp(\hat{z})}\right\}$$

$$= \frac{1}{m}\sum_{r=1}^{m-2}\pm\sqrt{\{\wp(r\hat{z}+\hat{z})+\wp(r\hat{z})+\wp(\hat{z})\}}.$$

Each of the $r\hat{z}$ has order m modulo Γ, so each $\wp(r\hat{z}) = I/m^{1/2}$. Hence $h(\hat{z}) = I/m^{5/4}$, Q.E.D.

LEMMA 7.3. *Let $U(z)$ be a standard function with poles of order r at each lattice point. Then*

$$m^{r/4}U(\hat{z}) = I.$$

Proof. A standard function is a polynomial in $\wp(z)$, $\frac{1}{2}\wp'(z)$, $\frac{1}{12}g_2$, and $\frac{1}{4}g_3$, with rational integral coefficients. By hypothesis, $\frac{1}{12}g_2 = I$ and $\frac{1}{4}g_3 = I$. So U is a polynomial in $\wp(z)$ and $\frac{1}{2}\wp'(z)$ with integral coefficients. A typical term is $I\wp(z)^a\wp'(z)^b$, which has poles of order $2a+3b$ at the lattice points. We may assume $0 \leqslant b \leqslant 1$, and then the poles belonging to different terms cannot cancel because they have different orders. So $2a+3b \leqslant r$, and when $z = \hat{z}$ each term has the form

$$(term) = I(I/m^{1/2})^a(I/m^{3/4})^b = I/m^{(2a+3b)/4} = I/m^{r/4}, \text{ Q.E.D.}$$

LEMMA 7.4. *Let K_j^i be the function defined in § 3, and let α and β be chosen (as in Corollary 4.1) to make $K_j^i(z)+\alpha z+\beta\bar{z}$ periodic. Then*

$$(j-1)!\,m^{r/4}(K_j^i(\hat{z})+\alpha\hat{z}+\beta\bar{\hat{z}}) = I,$$

where

$$r = \begin{cases} i+j & \text{if} \quad j \geqslant i+2, \\ \max(5,\, i+j) & \text{if} \quad j = i+1. \end{cases}$$

Proof. By Corollary 4.1,

$$(j-1)!\,(K_i^j(z)+\alpha z+\beta\bar{z}) = T_j^i(z)+B_j^i h(z).$$

By Lemma 3.3, B_j^i is a standard constant, so $B_j^i = I$ by Lemma 7.3. Also T_j^i is a standard function; by Lemma 3.1, K_j^i (and hence T_j^i) has poles of order $i+j$ at the lattice points. The result now follows from Lemmas 7.3 and 7.2.

LEMMA 7.5. *Suppose now that Γ admits complex multiplication by the ring $\boldsymbol{S}$. Then*

$$(7.1) \qquad \varphi(\Gamma)f\sqrt{|d|} = I.$$

(f and d were defined in § 2, and φ in § 4.)

Proof. By equation (6.1),

$$\varphi(\Gamma) = (\tau\bar{\tau}-\tau^2)^{-1}\sum_{\substack{\varrho\in\Gamma \\ \varrho \bmod \tau\Gamma}}\wp(\varrho/\tau,\Gamma),$$

where τ is any element of $\boldsymbol{S}$, not real. Let $\tau = a+bf\sigma$, and $t = \tau\bar{\tau}$. Then $\wp(\varrho/\tau) = I/t$, by Lemma 7.1, and

$$\tau\bar{\tau}-\tau^2 = \tau bf(\bar{\sigma}-\sigma) = (-i)\tau bf\sqrt{|d|}$$

by the results quoted in § 2. So (6.1) becomes

$$(7.2) \qquad \varphi(\Gamma) = I/(t^2bf\sqrt{|d|}).$$

This holds for all τ, and if we choose two values of τ for which the numbers t^2b are coprime, we may replace the denominator in (7.2) by $f\sqrt{|d|}$. This gives (7.1).

LEMMA 7.6. *Let $0 < s_0 \leqslant \frac{1}{2}n$ and $\frac{1}{2}n - s_0 \in \boldsymbol{Z}$. Put $p = \frac{1}{2}n - s_0$, $q = \frac{1}{2}n + s_0$, $r = 5$ if $p = 0$ and $q = 1$, otherwise $r = 5p+q$. Then*

$$(7.3) \qquad \varphi(\Gamma)^pF_n(\hat{z}, s_0, \Gamma) - B = I/[(q-1)!\,m^{r/4}(f\sqrt{|d|})^p],$$

where F_n is the function defined in § 5, and B is the constant of Lemma 5.2 (so $B = 0$ unless $s_0 = 1$).

Proof. By Lemma 5.2,

$$(7.4) \qquad \varphi^p(\Gamma)F_n(z, s_0, \Gamma) - B$$

$$= \sum_{t+u+v=p}\left[\frac{p!}{t!\,u!\,v!}h(z)^t(-\varphi)^u(-1)^vK_{q-u}^v(z)\right] + Cz + D\bar{z},$$

where $B = 0$ unless $s_0 = 1$ and $C = D = 0$ unless $s_0 = \frac{1}{2}$. First suppose that $s_0 \geqslant 1$. Put $z = \hat{z}$ and apply Lemmas 7.2–7.5:

$$\varphi^p(\Gamma)F_n(\hat{z}, s_0, \Gamma) - B = \sum_{t+u+v=p} I(I/m^{5/4})^t(I/f\sqrt{|d|})^u\left(I/(q-u-1)!\,m^{(q-u+v)/4}\right).$$

The largest power of $f\sqrt{|d|}$ occurs when $u = p$, the largest factorial when $u = 0$, and the largest power of m when $t = p$ and $u = v = 0$. Hence

$$\psi^p(\Gamma)F_n(\hat{z}, s_0, \Gamma) - B = I/[(q-1)!\,m^{(5p+q)/4}(f\sqrt{|d|})^p]$$

as required.

Now suppose $s_0 = \frac{1}{2}$. As in the proof of Lemma 5.2, we may replace each of the non-periodic K's in (7.4) by the corresponding periodic function $K^v_{q-u}(z) + \alpha z + \beta\bar{z}$, and this cancels the terms $Cz + D\bar{z}$. Put $z = \hat{z}$ and apply Lemmas 7.2–7.5:

$$\psi^p(\Gamma)F_n(\hat{z}, s_0, \Gamma) = \sum_{\substack{t+u+v=p\\ t>0}} I(I/m^{5/4})^t(I/f\sqrt{|d|})^u\big(I/(q-u-1)!\,m^{(q-u+v)/4}\big) + $$
$$+ \sum_{\substack{u+v=p\\ t=0}} I(I/f\sqrt{|d|})^u\big(I/(q-u-1)!\,m^{r/4}\big),$$

where $r = \max(5, q-u+v)$. As before the largest power of $f\sqrt{|d|}$ occurs when $u = p$, and the largest factorial when $u = 0$. The largest power of m is either $m^{5/4}$ or $m^{(5p+q)/4}$, and $5p+q > 5$ unless $p = 0$ (so $q = p + 2s_0 = 1$). This proves the Lemma when $s_0 = \frac{1}{2}$.

§ 8. Determination of γ.

LEMMA 8.1. *Let x be such that $\frac{1}{12}g_2(Sx)$ and $\frac{1}{4}g_3(Sx)$ are algebraic integers. Let $\boldsymbol{b}$ be a proper ideal of $\boldsymbol{S}$* (see § 2) *and $\hat{\boldsymbol{b}}$ an ideal number representing $\boldsymbol{b}$.*

Then

$$\tfrac{1}{12}g_2(\boldsymbol{b}x/\hat{\boldsymbol{b}}) = I$$

and

$$\tfrac{1}{4}g_3(\boldsymbol{b}x/\hat{\boldsymbol{b}}) = I.$$

Proof. We prove the lemma for g_2, the proof for g_3 being similar. Let $\hat{\boldsymbol{b}}$ and $\boldsymbol{b}^*$ be two ideal numbers for $\boldsymbol{b}$. Then $\hat{\boldsymbol{b}}/\boldsymbol{b}^*$ is an algebraic unit, so for given $\boldsymbol{b}$ the result is independent of the choice of $\hat{\boldsymbol{b}}$, by the homogeneity of g_2. Now let $\boldsymbol{a}$ and $\boldsymbol{b}$ be in the same ideal class of $\boldsymbol{S}$. Then $\boldsymbol{b} = [\alpha]\,\boldsymbol{a}$ and $\hat{\boldsymbol{b}} = \alpha\hat{\boldsymbol{a}}$ for some α in k, and

$$(8.1)\qquad \tfrac{1}{12}g_2(\boldsymbol{b}x/\hat{\boldsymbol{b}}) = \tfrac{1}{12}g_2(\alpha\boldsymbol{a}x/\alpha\hat{\boldsymbol{a}}) = \tfrac{1}{12}g_2(\boldsymbol{a}x/\hat{\boldsymbol{a}}).$$

Given a proper ideal class A of $\boldsymbol{S}$, let $\boldsymbol{p}$ be a prime ideal in A such that $\boldsymbol{p}\bar{\boldsymbol{p}}$ is a rational prime P, say. Then SPx is a sublattice of $\boldsymbol{p}x$, and

$$g_2(\boldsymbol{p}x) = g_2(SPx) + 10\sum_{\varrho}\wp''(\varrho, SPx)$$

by equation (6.0). Here ϱ runs through all non-zero residues of $\boldsymbol{p}x$ modulo SPx. By equation (3.11) and homogeneity and Lemma 7.1 we deduce:

$$\tfrac{1}{12}g_2(\boldsymbol{p}x) = \tfrac{1}{12}P^{-4}g_2(\boldsymbol{S}x) + 5\sum_{\varrho}\{P^{-4}\wp^2(\varrho/P, \boldsymbol{S}x) - \tfrac{1}{12}P^{-4}\ g_2(\boldsymbol{S}x)\}$$
$$= I/P^4 + I/P^5 + I/P^4 = I/P^5.$$

Hence

$$\tfrac{1}{12}g_2(\boldsymbol{p}x/\hat{\boldsymbol{p}}) = \hat{\boldsymbol{p}}^4 I/P^5 = I/P^5.$$

Similarly, if $\boldsymbol{q}$ is a second prime in the same ideal class, then

$$\tfrac{1}{12}g_2(\boldsymbol{q}x/\hat{\boldsymbol{q}}) = I/Q^5.$$

But the two left-hand sides are equal by (8.1), so their common value is an integer, Q.E.D.

LEMMA 8.2. *For all s for which $F_n(z, s, \Gamma)$ is defined,*

$$(8.2)\qquad \frac{\psi(\Gamma x)^{n/2-s}F_n(zx, s, \Gamma x)}{\psi(\Gamma)^{n/2-s}F_n(z, s, \Gamma)} = x^{-n}.$$

Proof. F_n is defined by equation (5.1) for $\mathrm{re}(s) > 1$:

$$F_n(z, s, \Gamma) = \sum_{\Omega}\frac{(\bar{z}+\bar{\Omega})^{n/2-s}}{(z+\Omega)^{n/2+s}}.$$

Hence

$$\frac{F_n(zx, s, \Gamma x)}{F_n(z, s, \Gamma)} = \frac{\bar{x}^{n/2-s}}{x^{n/2+s}}.$$

From equation (4.5′) we deduce that

$$\frac{\psi(\Gamma x)}{\psi(\Gamma)} = \frac{A(\Gamma)}{A(\Gamma x)} = |x|^{-2} = (x\bar{x})^{-1}.$$

Combining these two results gives (8.2) when $\mathrm{re}(s) > 1$. For other s the result holds by analytic continuation.

THEOREM 2. *Let $\zeta(s, \lambda)$ be a Hecke zeta function defined over the ring $\boldsymbol{S}$, let s_0 be a value of s such that $\frac{1}{2}n - s_0 \in \boldsymbol{Z}$ and $0 \leqslant s_0 \leqslant \frac{1}{2}n$, as in Theorem 1. Let x be chosen such that $\frac{1}{12}g_2(\boldsymbol{S}x)$ and $\frac{1}{4}g_3(\boldsymbol{S}x)$ are algebraic integers. Let γ be defined as follows:*

$$\gamma = \begin{cases} e\,\hat{\boldsymbol{m}}\mathcal{N}(\boldsymbol{m})^{5/4} & \text{if } n = 1 \text{ and } s_0 = \frac{1}{2},\\ 2^{n/2-s_0}e(\frac{1}{2}n+s_0-1)!\,\hat{\boldsymbol{m}}^n\mathcal{N}(\boldsymbol{m})^{n/4} & \text{otherwise,}\end{cases}$$

where e is the number of units of $\boldsymbol{S}$, $\hat{\boldsymbol{m}}$ an ideal number for the conductor $\boldsymbol{m}$ of λ, and $\mathcal{N}(\boldsymbol{m})$ its norm.

Assume also that if $s_0 = 1$, then the character χ is not trivial on the numbers of S (i.e. *there is an a for which $\chi(a) \neq 1$*). *Then*

$$\gamma\Theta = \gamma\zeta(s_0, \lambda)\pi^{n/2-s_0}/x^n$$

is an algebraic integer.

Proof. By equation (6.2)

$$\Theta = e^{-1}\left(-\tfrac{1}{2}\mathcal{N}(\boldsymbol{m})f\sqrt{|d|}\right)^p \sum_{i=1}^{h}\Big[\hat{\boldsymbol{a}}_i^n\chi^{-1}(\hat{\boldsymbol{a}}_i)\sum_{\substack{\beta\in\boldsymbol{a}_i\\ \beta \bmod \boldsymbol{b}}}\chi(\beta)\psi^p(\boldsymbol{b}x)F_n(\beta x, s_0, \boldsymbol{b}x)\Big],$$

where $p = \frac{1}{2}n - s_0$ and $\boldsymbol{b} = \boldsymbol{m}\boldsymbol{a}_i$. Within the square brackets, replace x by $x/\hat{\boldsymbol{b}} = x/\hat{\boldsymbol{m}}\hat{\boldsymbol{a}}_i$. By Lemma 8.2 this gives

$$\Theta = e^{-1}\left(-\tfrac{1}{2}\mathcal{N}(\boldsymbol{m})f\sqrt{|d|}\right)^p\hat{\boldsymbol{m}}^{-n}\times \tag{8.3}$$
$$\times\sum_{i=1}^{h}\Big[\chi^{-1}(\hat{\boldsymbol{a}}_i)\sum_{\substack{\beta\in\boldsymbol{a}_i\\ \beta \bmod \boldsymbol{b}}}\chi(\beta)\psi^p(\boldsymbol{b}x/\hat{\boldsymbol{b}})F_n(\beta x/\hat{\boldsymbol{b}}, s_0, \boldsymbol{b}x/\hat{\boldsymbol{b}})\Big].$$

By Lemma 8.1, $\frac{1}{12}g_2(\boldsymbol{b}x/\hat{\boldsymbol{b}}) = I$ and $\frac{1}{4}g_3(\boldsymbol{b}x/\hat{\boldsymbol{b}}) = I$. Each β is in $\boldsymbol{a}_i$, so β has index $\mathcal{N}(\boldsymbol{m})$ modulo $\boldsymbol{b}$. By Lemma 7.6, with $m = \mathcal{N}(\boldsymbol{m})$, the inner sum of (8.3) is

$$\sum_{\beta}\chi(\beta)\{B + I/[(q-1)!\mathcal{N}(\boldsymbol{m})^{r/4}(f\sqrt{|d|})^p]\}. \tag{8.4}$$

Here B is the constant of Lemma 5.2, so $B = 0$ unless $s_0 = 1$. If $s_0 = 1$, then χ is assumed non-trivial, so $\sum_{\beta}\chi(\beta)B = 0$. So B may be neglected. Since the $\chi(\hat{\boldsymbol{a}}_i)$ and $\chi(\beta)$ are algebraic units, (8.3) reduces to

$$\Theta = e^{-1}\left(\tfrac{1}{2}\mathcal{N}(\boldsymbol{m})f\sqrt{|d|}\right)^p\hat{\boldsymbol{m}}^{-n}I/[(q-1)!\mathcal{N}(\boldsymbol{m})^{r/4}(f\sqrt{|d|})^p].$$

Now put $p = \frac{1}{2}n - s_0$, $q = \frac{1}{2}n + s_0$, $r = 5$ if $n = 1$ and $s_0 = \frac{1}{2}$, and $r = 5p + q = 3n - 4s_0$ otherwise. Then

$$\Theta = \begin{cases} I/e\hat{\boldsymbol{m}}\mathcal{N}(\boldsymbol{m})^{5/4} & \text{if } n = 1 \text{ and } s_0 = \tfrac{1}{2},\\ I/[2^{n/2-s_0}e(\tfrac{1}{2}n + s_0 - 1)!\hat{\boldsymbol{m}}^n\mathcal{N}(\boldsymbol{m})^{n/4}] & \text{otherwise.}\end{cases}$$

This proves Theorem 2.

I would like to thank Professor J. W. S. Cassels for his most valuable help and encouragement, and for his advice in the preparation of this paper.

References

[1] B. J. Birch and H. P. F. Swinnerton-Dyer, *Notes on elliptic curves, II*, J. Reine Ang. Math. 218 (1965), pp. 79–108.

[2] J. W. S. Cassels, *A note on the division values of $\wp(u)$*, Proc. Camb. Phil. Soc. 45 (1948), pp. 167–172.

[3] R. M. Damerell, *L-functions of elliptic curves with complex multiplication, I*, Acta Arith. 17 (1970), pp. 287–301.

[4] R. Fricke, *Die elliptischen Funktionen und ihre Anwendungen, II*, B. G. Teubner, Leipzig and Berlin. Page references apply to the 1916 edition.

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

[6] — *Arithmetic on curves with complex multiplication by the Eisenstein integer*, Camb. Phil. Soc. 65 (1969), pp. 59–73.

ROYAL HOLLOWAY COLLEGE
UNIVERSITY OF LONDON

Received on 10. 7. 1970 104