Proc. Camb. Phil. Soc. (1968), **64**, 659
PCPS 64–82
Printed in Great Britain

Arithmetic on curves with complex multiplication by $\sqrt{-2}$

By A. R. RAJWADE
Panjab University, Chandigarh, India

(*Received* 14 *November* 1966)

1. *Introduction.* This paper is a contribution to the verification of conjectures of Birch and Swinnerton-Dyer about elliptic curves (1). The evidence that they produce is largely derived from curves with complex multiplication by i. It is natural to consider other kinds of complex multiplications and here we shall make a start on the case when the ring of complex multiplications is isomorphic to the ring $\mathbf{Z}[\sigma]$, where $\sigma^2 = -2$.

Without loss of generality, such a curve has the form:

$$\Gamma = \Gamma_D\colon y^2 = x(x^2 - 4Dx + 2D^2) \tag{1·1}$$

where $D \in \mathbf{Z}$ (as can be verified using isogeny arguments), and multiplication by σ of a point (x, y) on (1·1) is given by the formula

$$\sigma(x,y) = \left(\frac{x^2 - 4Dx + 2D^2}{-2x}, \frac{y}{\sigma x}\left(\frac{x^2 - 2D^2}{2x}\right)\right). \tag{1·2}$$

We shall call a prime p 'good' if it does not divide $2D$. The curve (1·1) has a 'good reduction' at all the good primes, and in Section 3, we shall derive a formula for the number N_p of points on (1·1), modulo p.

In the Birch–Swinnerton-Dyer theory, a key role is played by the value, at $s = 1$ of the function

$$L_D(s) = \prod_{p \text{ good}} \{1 + (N_p - p - 1)p^{-s} + p^{1-2s}\}^{-1}. \tag{1·3}$$

It has been conjectured that this function, which is *a priori* defined only for $s > \frac{3}{2}$, can be analytically extended over the whole of the s-plane, and this conjecture has been verified by Deuring when there is complex multiplication, the function then being a Hecke L-function. In Section 4, we obtain this Hecke-function explicitly for our case, using the determination of N_p. This enables us to find a closed expression for $L_D(1)$, analogous to that given by Birch and Swinnerton-Dyer. We then prove the following result analogous to that of Birch and Swinnerton-Dyer:

Theorem. *Let $D > 1$ be a positive square-free rational integer and Θ the real period of the Weierstrass $\wp$-function satisfying the equation*

$$\wp'^2 = \wp^3 - 4\wp^2 + 2\wp.$$

Then $8\sqrt{D}\, L_D(1)/\Theta$ and $8\sqrt{(2D)}\, L_{-D}(1)/\Theta$ are rational integers.

My proof of the above result is more elementary than the corresponding proof of Birch and Swinnerton-Dyer, in that I can dispense with Class field theory.

https://doi.org/10.1017/S0305004100043334 Published online by Cambridge University Press

The Birch–Swinnerton-Dyer conjectures are concerned with the so called 'Tamagawa number', which is the product of $L_D(1)$ by certain factors corresponding to the primes which are not 'good' (including the infinite prime). In the final section of this paper, we show that the irrational factors $\sqrt{D}$ and $\sqrt{(2D)}$ of the theorem enunciated above are in fact just the contributions of the infinite prime to the Tamagawa number. As the contributions of the remaining bad primes are all rational, by definition, it follows that the Tamagawa number is rational. For detailed accounts of the Birch–Swinnerton-Dyer conjectures, see (1), or (3).

In conclusion, I should like to express my most sincere gratitude and thanks to Dr Cassels and to Mr Swinnerton-Dyer for their invaluable help.

2. *Table for the σ^nth division points, and some notation.* With the help of (1·2), we can determine the σ^nth division points for positive integral n using the equation

$$\sigma(x, y) = \mathbf{O}.$$

In this section, we give a table showing what they are for $n = 1, 2, 3, 4, 5$, and introduce some notation.

Write $\theta = \sqrt{(1-\sqrt{2})}$, $\phi = \sqrt{(1+\sqrt{2})}$, so that $\theta\phi = i$.

We also let $\lambda = \sqrt{(1-\sqrt{2}+\sqrt{2}\theta)}, \quad \mu = \sqrt{(1-\sqrt{2}-\sqrt{2}\theta)},$

and $\nu = \sqrt{(1+\sqrt{2}+\sqrt{2}\phi)}, \quad \kappa = \sqrt{(1+\sqrt{2}-\sqrt{2}\phi)}$

so that $\lambda\mu = 1 = \nu\kappa$.

The symbol $(\alpha/\beta)_2$, where α, β are coprime integers of $\mathbf{Z}[\sigma]$ and β a prime, $\neq \sigma$ of $\mathbf{Z}[\sigma]$, shall denote the quadratic residue symbol in $\mathbf{Z}[\sigma]$, i.e. that unit ± 1 of $\mathbf{Z}[\sigma]$, which is $\equiv \alpha^{\frac{1}{2}(\text{norm }\beta-1)} (\text{mod}\,\beta)$. Extend this to any $\beta = \pi_1\pi_2 \dots \pi_n$ (π_i primes $\neq \sigma$ of $\mathbf{Z}[\sigma]$) by multiplication, i.e.

$$\left(\frac{\alpha}{\beta}\right)_2 = \left(\frac{\alpha}{\pi_1}\right)_2 \dots \left(\frac{\alpha}{\pi_n}\right)_2.$$

The symbol $(a/b)_{\mathbf{Z}}$ shall denote the usual quadratic residue symbol in $\mathbf{Z}$.

The only proper σ-division point is $(0, 0)$.

The proper 2-division points are $(-(-2 \pm \sqrt{2})\,D, 0) = \mathbf{S}_1, \mathbf{S}_2$ say, while the proper 2σ-division points are

$$\{D\sqrt{2}, \pm 2Di\sqrt{D}\sqrt{(2-\sqrt{2})}\} \quad \text{and} \quad \{-D\sqrt{2}, \pm 2Di\sqrt{D}\sqrt{(2+\sqrt{2})}\}, \tag{2·1}$$

and these we write as:

$$\left.\begin{aligned} (D\sqrt{2}, \pm 2D\sqrt{D}\,2^{\frac{1}{4}}\theta) &= \pm \mathbf{R}_1 \text{ say,} \\ (-D\sqrt{2}, \pm 2(-D)i\sqrt{D}\,2^{\frac{1}{4}}\phi) &= \pm \mathbf{R}_3 \text{ say.} \end{aligned}\right\} \tag{2·2}$$

The proper 4-division points are the following eight:

$$\left.\begin{aligned} \pm \mathbf{Q}_1 &= \{D(-2\theta-\sqrt{2}+2), \pm 2D\sqrt{D}\,2^{\frac{1}{4}}i(1-\sqrt{2}+\sqrt{2}\theta)\}, \\ \pm \mathbf{Q}_3 &= \{D(2\theta-\sqrt{2}+2), \pm 2D\sqrt{D}\,2^{\frac{1}{4}}i(-1+\sqrt{2}+\sqrt{2}\theta)\}, \\ \pm \mathbf{Q}_5 &= \{D(-2\phi+\sqrt{2}+2), \pm 2D\sqrt{D}\,2^{\frac{1}{4}}(-1-\sqrt{2}+\sqrt{2}\phi)\}, \\ \pm \mathbf{Q}_7 &= \{D(2\phi+\sqrt{2}+2), \pm 2D\sqrt{D}\,2^{\frac{1}{4}}(1+\sqrt{2}+\sqrt{2}\phi)\}. \end{aligned}\right\} \tag{2·3}$$

https://doi.org/10.1017/S0305004100043334 Published online by Cambridge University Press

Finally, the proper 4σ-division points are 16 in number given by

$$\left.\begin{aligned}
\pm\mathbf{P}_1 &= \{D\sqrt{2}(1+\sqrt{2}\,\theta-\sqrt{2}\,\lambda),\ \pm 2D\sqrt{D}\,2^{\frac{1}{4}}\lambda(1+\sqrt{2}\,\theta-\sqrt{2}\lambda)\},\\
\pm\mathbf{P}_3 &= \{D\sqrt{2}(1+\sqrt{2}\,\theta+\sqrt{2}\,\lambda),\ \pm 2D\sqrt{D}\,2^{\frac{1}{4}}\lambda(-1-\sqrt{2}\,\theta-\sqrt{2}\,\lambda)\},\\
\pm\mathbf{P}_5 &= \{D\sqrt{2}(1-\sqrt{2}\,\theta-\sqrt{2}\,\mu),\ \pm 2D\sqrt{D}\,2^{\frac{1}{4}}\mu(-1+\sqrt{2}\,\theta+\sqrt{2}\,\mu)\},\\
\pm\mathbf{P}_7 &= \{D\sqrt{2}(1-\sqrt{2}\,\theta+\sqrt{2}\,\mu),\ \pm 2D\sqrt{D}\,2^{\frac{1}{4}}\mu(1-\sqrt{2}\,\theta+\sqrt{2}\,\mu)\},\\
\pm\mathbf{P}_9 &= \{D\sqrt{2}(-1+\sqrt{2}\,\phi-\sqrt{2}\,\kappa),\ \pm 2D\sqrt{D}\,2^{\frac{1}{4}}\kappa i(-1+\sqrt{2}\,\phi-\sqrt{2}\kappa)\},\\
\pm\mathbf{P}_{11} &= \{D\sqrt{2}(-1+\sqrt{2}\,\phi+\sqrt{2}\,\kappa),\ \pm 2D\sqrt{D}\,2^{\frac{1}{4}}\kappa i(1-\sqrt{2}\,\phi-\sqrt{2}\,\kappa)\},\\
\pm\mathbf{P}_{13} &= \{D\sqrt{2}(-1-\sqrt{2}\,\phi-\sqrt{2}\,\nu),\ \pm 2D\sqrt{D}\,2^{\frac{1}{4}}\nu i(1+\sqrt{2}\,\phi+\sqrt{2}\,\nu)\},\\
\pm\mathbf{P}_{15} &= \{D\sqrt{2}(-1-\sqrt{2}\,\phi+\sqrt{2}\,\nu),\ \pm 2D\sqrt{D}\,2^{\frac{1}{4}}\nu i(-1-\sqrt{2}\,\phi+\sqrt{2}\,\nu)\},
\end{aligned}\right\} \tag{2·4}$$

where in deriving these, we have used the following identities:

$$\left.\begin{aligned}
\sqrt{\{-2(\sqrt{2}+2\theta)\lambda-5+4\sqrt{2}-4\sqrt{2}\,\theta\}} &= \pm i(1+\sqrt{2}\,\theta+\sqrt{2}\,\lambda),\\
\sqrt{\{2(\sqrt{2}+2\theta)\lambda-5+4\sqrt{2}-4\sqrt{2}\,\theta\}} &= \pm i(1+\sqrt{2}\,\theta-\sqrt{2}\,\lambda);\\
\sqrt{\{2(-\sqrt{2}+2\phi)\kappa-5-4\sqrt{2}+4\sqrt{2}\,\phi\}} &= \pm i(1-\sqrt{2}\,\phi+\sqrt{2}\,\kappa),\\
\sqrt{\{-2(-\sqrt{2}+2\phi)\kappa-5-4\sqrt{2}-4\sqrt{2}\,\phi\}} &= \pm i(1-\sqrt{2}\,\phi-\sqrt{2}\,\kappa);
\end{aligned}\right\} \tag{2·5}$$

and the like with μ, ν instead of λ, κ respectively.

Now it can be verified that under multiplication by σ, we have:

$$\left.\begin{aligned}
&\pm\mathbf{R}_1\to\mathbf{S}_1, \qquad \pm\mathbf{R}_3\to\mathbf{S}_2;\\
&\mathbf{Q}_1,\mathbf{Q}_3\to\mathbf{R}_1, \quad -\mathbf{Q}_1,-\mathbf{Q}_3\to-\mathbf{R}_1; \quad \mathbf{Q}_5,\mathbf{Q}_7\to\mathbf{R}_3, \quad -\mathbf{Q}_5,-\mathbf{Q}_7\to-\mathbf{R}_3;\\
\text{and}\quad &\mathbf{P}_1,\mathbf{P}_3\to\mathbf{Q}_1, \qquad \mathbf{P}_5,\mathbf{P}_7\to\mathbf{Q}_3; \quad \mathbf{P}_9,\mathbf{P}_{11}\to\mathbf{Q}_5, \qquad \mathbf{P}_{13},\mathbf{P}_{15}\to\mathbf{Q}_7;
\end{aligned}\right\} \tag{2·6}$$

and similar line with minus sign for each $\mathbf{P}$ and $\mathbf{Q}$.

It may also be verified, using very heavy algebra, that

$$\left.\begin{aligned}
&(1+\sigma)\,\mathbf{Q}_1=-\mathbf{Q}_7, \quad \text{and} \quad 3\mathbf{P}_1=-\mathbf{P}_3, \quad (5+2\sigma)\,\mathbf{P}_1=\mathbf{P}_5,\\
&(7+2\sigma)\,\mathbf{P}_1=-\mathbf{P}_7, \quad (1+\sigma)\,\mathbf{P}_1=-\mathbf{P}_{13}, \quad (3+3\sigma)\,\mathbf{P}_1=\mathbf{P}_{15},\\
&(1+3\sigma)\,\mathbf{P}_1=-\mathbf{P}_9, \quad (3+\sigma)\,\mathbf{P}_1=\mathbf{P}_{11}.
\end{aligned}\right\} \tag{2·7}$$

We shall need one more simple identity later

$$\left.\begin{aligned}
2^{\frac{1}{4}}\lambda &= i(1-\theta), \quad 2^{\frac{1}{4}}\mu=-i(1+\theta),\\
2^{\frac{1}{4}}\nu &= 1+\phi, \qquad 2^{\frac{1}{4}}\kappa=\phi-1.
\end{aligned}\right\} \tag{2·8}$$

3. *The* N_p. The object of this section is to find N_p, the number of points on the projective version of (1·1), in the finite field of p elements. To do this, we use a well known theorem of Deuring's (5), which says:

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

Here we have an ambiguity about the sign of π and $\overline{\pi}$, since p also $=(-\pi)(-\overline{\pi})$. The theorem also tells us that *that* sign $+\pi$ or $-\pi$ is the right one for which multiplication of points of Γ by the π with correct sign has the same effect as has the Frobenius Automorphism

$$f_p\colon (x,y)\to(x^p,y^p) \pmod p.$$

https://doi.org/10.1017/S0305004100043334 Published online by Cambridge University Press

Our object is to prove the following

THEOREM 1.

$$N_p = \begin{cases} p+1 & \text{if} \quad p \equiv -1, -3 \pmod 8, \\ p+1-(D/\pi)_2\,\overline{\pi}-(D/\pi)_2 & \text{if} \quad p \equiv 1, 3 \pmod 8, \end{cases}$$

where $p = \pi\overline{\pi}$ *and the* π *and* $\overline{\pi}$ *are normalized as follows*:

Modulo 4σ, *the group of odd* (i.e. *prime to* σ) *residue classes are* $1, 3, 5, 7, 1+\sigma, 3+\sigma, 5+\sigma, 7+\sigma, 1+2\sigma, 3+2\sigma, 5+2\sigma, 7+2\sigma, 1+3\sigma, 3+3\sigma, 5+3\sigma, 7+3\sigma$.

Of this, the set $\Lambda = 1, 3, 1+\sigma, 3+\sigma, 1+3\sigma, 3+3\sigma, 5+2\sigma, 7+2\sigma$ *is a subgroup of index* 2.

We demand that π *and* $\overline{\pi} \equiv$ *some* $\lambda \in \Lambda \pmod{4\sigma}$ *in Theorem* 1. This fixes the sign of π and $\overline{\pi}$ as desired.

The most convenient points to try the Frobenius on, are the 2σ-division points, since by a good stroke of luck, we find that $\sqrt{(2+\sqrt{2})} = \zeta+\zeta^{-1}$ where $\zeta = e^{\pi i/8}$ and then it may be verified that

$$-\sqrt{(2+\sqrt{2})} = \zeta^7+\zeta^{-7}, \quad \sqrt{(2-\sqrt{2})} = \zeta^3+\zeta^{-3},$$
$$-\sqrt{(2-\sqrt{2})} = \zeta^5+\zeta^{-5}, \quad \text{and note that} \quad \sqrt{2} = \zeta^2+\zeta^{-2}.$$

Now let $p \equiv 1 \pmod 8$ be a rational prime. Then

$$f_p\{\sqrt{(2+\sqrt{2})}\} = (\zeta+\zeta^{-1})^p \equiv \zeta^p+\zeta^{-p} =$$
$$\left\{\begin{matrix} \zeta+\zeta^{-1} & \text{if} \quad p \equiv 1 \pmod{16} \\ -(\zeta+\zeta^{-1}) & \text{if} \quad p \equiv 9 \pmod{16} \end{matrix}\right\} = (-1)^{\frac{1}{8}(p-1)}.\sqrt{(2+\sqrt{2})}.$$

Therefore
$$f_p\{\sqrt{-D}.\sqrt{(2+\sqrt{2})}\} \equiv (-D)^{\frac{1}{2}p}.f_p\{\sqrt{(2+\sqrt{2})}\}$$
$$\equiv \left(\frac{-D}{p}\right)_{\mathbf{Z}}(-1)^{\frac{1}{8}(p-1)}\{\sqrt{-D}.\sqrt{(2+\sqrt{2})}\},$$

and $f_p(-D.\sqrt{2}) \equiv -D.\sqrt{2}$ similarly. Hence

$$f_p\,\mathbf{R}_3 = \left(\frac{-D}{p}\right)_{\mathbf{Z}}(-1)^{\frac{1}{8}(p-1)}.\mathbf{R}_3.$$

But now $f_p\,\mathbf{R}_3 = \pi\mathbf{R}_3$ by the very definition of π, (π with the correct sign), and therefore

$$\left(\pi-\left(\frac{-D}{p}\right)_{\mathbf{Z}}(-1)^{\frac{1}{8}(p-1)}\right)\mathbf{R}_3 = \mathbf{0},$$

and since $\mathbf{R}_3$ is a proper 2σ-division point, we have

$$\pi \equiv \left(\frac{-D}{p}\right)_{\mathbf{Z}}(-1)^{\frac{1}{8}(p-1)} \pmod{2\sigma}.$$

We note now that a factor α (in $\mathbf{Z}[\sigma]$) of a rational prime $p \equiv 1(8)$ is uniquely determined by the condition $\alpha \equiv 1 \pmod{2\sigma}$: for if $\alpha = c+d\sigma$, then $c^2+2d^2 = p \equiv 1 \pmod 8$, so 2 divides d and $\alpha \equiv c \pmod{2\sigma}$, but c is odd: $c \equiv \pm 1 \pmod 4$, i.e. $c \equiv \pm 1 \pmod{2\sigma}$, i.e. $\alpha \equiv 1 \pmod{2\sigma}$. Thus the π with the correct sign attached to it is

$$\left(\frac{-D}{p}\right)_{\mathbf{Z}}(-1)^{\frac{1}{8}(p-1)}\pi, \tag{3·1}$$

where $\pi \equiv 1 \pmod{2\sigma}$.

https://doi.org/10.1017/S0305004100043334 Published online by Cambridge University Press

Similarly for the case $p \equiv 3 \pmod 8$, it may be verified that the π with the correct sign attached to it is

$$-\left(\frac{-D}{p}\right)_{\mathbf{Z}}(-1)^{\frac{1}{8}(p-3)}\pi,$$

where π is normalized by the condition

$$\pi \equiv 1+\sigma \pmod{2\sigma}. \tag{3·2}$$

Now the normalization of π and $\overline{\pi}$ is to be modulo 4σ and so we must make sure that the above normalization agrees with that of Theorem 1. This is easily checked; for example, if $p \equiv 1 \pmod{16}$ then $N_p = p+1-(D/p)_{\mathbf{Z}}(\pi+\overline{\pi})$, where $\pi \equiv 1 \pmod{2\sigma}$, i.e. $\pi \equiv 1, 5, 1+2\sigma, \ 5+2\sigma \pmod{4\sigma}$. But $\pi \equiv 5, \ 1+2\sigma \pmod{4\sigma}$ implies $p \equiv 9 \pmod{16}$; whence $\pi \equiv 1, 5+2\sigma \pmod{4\sigma}$ only. Similarly the other members of Λ may be recovered. This completes the proof of Theorem 1.

4. *The zeta-function of* Γ. Let $\mathfrak{C}$ be a general complete non-singular curve of genus 1 defined over the rationals by the equation

$$y^2z = x^3 - Axz^2 - Bz^3. \tag{4·1}$$

For 'almost all' primes p, this curve, defined over the finite field of p elements retains these properties and then its zeta function (at p) is

$$\zeta_{\mathfrak{C},p}(s) = \frac{1+(N_p-p-1)p^{-s}+p^{1-2s}}{(1-p^{-s})(1-p^{1-s})}. \tag{4·2}$$

The global zeta function of $\mathfrak{C}$ is therefore

$$\prod_{p \text{ good}} \zeta_{\mathfrak{C},p}(s) = \frac{\zeta(s).\zeta(s-1)}{L_{\mathfrak{C}}(s)} = \zeta_{\mathfrak{C}}(s), \tag{4·3}$$

where $\zeta(s)$ is the usual Riemann zeta function, and

$$L_{\mathfrak{C}}(s) = \prod_{p \text{ good}} \{1+(N_p-p-1)p^{-s}+p^{1-2s}\}^{-1} \tag{4·4}$$

and where there should perhaps be factors of some kind for the 'bad' primes. Formally we have $L_{\mathfrak{C}}(1) = \Pi(N_p/p)^{-1}$, but for general $\mathfrak{C}$ the product (4·4) is only known to converge for $R(s) > \frac{3}{2}$ and it is not known whether it can be continued analytically outside this region. If $\mathfrak{C}$ admits complex multiplication, then $L_{\mathfrak{C}}(s)$ *is* analytically continuable over the whole plane as has been shown by Deuring (6).

For the special curve of this paper it is simplest to use the explicit formula for N_p proved in Theorem 1. We find

$$\begin{aligned} L_D(s) &= \prod_{p \equiv 5,7\,(8)} (1+p^{1-2s})^{-1} \prod_{\pi,\, \pi \equiv l \in \Lambda\,(4\sigma)} \left\{1-\overline{\pi}\left(\frac{D}{\overline{\pi}}\right)_2 p^{-s} - \pi\left(\frac{D}{\overline{\pi}}\right)_2 p^{-s} + p^{1-2s}\right\}^{-1} \\ &= \prod_{\pi \equiv l \in \Lambda} \left\{1-\left(\frac{D}{\pi}\right)_2 \frac{\overline{\pi}}{(N\pi)^s}\right\}^{-1}, \end{aligned}$$

where the product is taken over all the relevant primes, real or complex, of $\mathbf{Z}[\sigma]$. This gives

$$L_D(s) = \sum_{\lambda \in \Lambda} \left(\frac{D}{\lambda}\right)_2 \left(\frac{\overline{\lambda}}{(N\lambda)^s}\right). \tag{4·5}$$

It costs us nothing to take D to be an integer of $\mathbf{Z}[\sigma]$, though the important case is when D is a rational integer. We may also assume that D is square-free; for multiplying

https://doi.org/10.1017/S0305004100043334 Published online by Cambridge University Press

D by a square only changes finitely many factors in the formula for $L_D(S)$, and changes those in an obvious way.

Write $D = \Delta F$, where F is the product of powers of σ and units ± 1 of $\mathbf{Z}[\sigma]$, and where $\Delta \in \Lambda$. Let $\epsilon = (-1/\Delta)_{\mathbf{Z}}$. Then we have the following

THEOREM 2.
$$\left(\frac{\Delta}{\lambda}\right)_2 = \left(\frac{\lambda}{\Delta}\right)_2 \left(\frac{\epsilon}{\lambda}\right)_2.$$

Proof. The product formula for the Hilbert norm residue symbol gives:

$$\left(\frac{\Delta}{\lambda}\right)\left(\frac{\lambda}{\Delta}\right)\binom{\lambda, \Delta}{\sigma} = 1.$$

Hence it is enough to prove that

$$\binom{\lambda, \Delta}{\sigma} = \left(\frac{\epsilon}{\lambda}\right)_2. \tag{4·6}$$

The right-hand side of (4·6)

$$= \left\{\begin{matrix} -1 & \text{if} \quad \Delta \equiv \operatorname{norm}\lambda \equiv -1 \pmod 4, \\ 1 & \text{otherwise} \end{matrix}\right\} = (-1)^{\frac{1}{2}(\Delta-1)\frac{\operatorname{norm}\lambda - 1}{2}} = \binom{\Delta, \operatorname{norm}\lambda}{2};$$

hence it remains to show that

$$\binom{\lambda, \Delta}{\sigma}_{\mathbf{Q}(\sigma)} = \binom{N\lambda, \Delta}{2}_{\mathbf{Q}}.$$

This follows from the following well-known class field theoretic

LEMMA. *Let H = local field, K = finite Abelian extension of H, G = any finite extension of H, $\lambda \in G$; then*

$$\left(\frac{KG/G}{\lambda}\right) = \left(\frac{K/H}{\operatorname{norm}_{G/H}(\lambda)}\right),$$

where these are the Artin symbols.

In our case, $H = \mathbf{Q}_2$, $G = \mathbf{Q}_2(\sigma)$, $K = \mathbf{Q}_2(\sqrt{\Delta})$ and so Theorem 3 follows.

Now referring back to (4·5), we have

$$\left(\frac{D}{\lambda}\right)_2 = \left(\frac{\Delta}{\lambda}\right)_2 \left(\frac{F}{\lambda}\right)_2 = \left(\frac{\lambda}{\Delta}\right)_2 \left(\frac{\epsilon F}{\lambda}\right)_2. \tag{4·7}$$

Here the first factor on the right-hand side depends on the class of $\lambda \bmod \Delta$, while the second factor depends on the class of λ modulo 2 if D is a rational integer, and modulo 8 if D is an integer of $\mathbf{Z}[\sigma]$. This may be verified using reciprocity laws in $\mathbf{Z}[\sigma]$. Let K be such that 4σ divides K and such that $(\epsilon F/\lambda)_2$ depends on the class of $\lambda \bmod K$. We could take $K = 4\sigma$ if $D \in \mathbf{Z}$, but must take $K = 8$ if $D \in \mathbf{Z}[\sigma]$.

Let now 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 $\in \Lambda$. Then our λ of (4·5) can be written as

$$\lambda = K\Delta\mu + (K\beta + \Delta\gamma) = K\Delta\mu + \rho \quad \text{say},$$

where $\beta \in B$, $\gamma \in C$ and $\mu \in \mathbf{Z}[\sigma]$. Then (4·7) implies

$$\left(\frac{D}{\lambda}\right)_2 = \left(\frac{K\beta}{\Delta}\right)_2 \left(\frac{\epsilon F}{\Delta\gamma}\right)_2 = \left(\frac{D}{\rho}\right)_2. \tag{4·8}$$

https://doi.org/10.1017/S0305004100043334 Published online by Cambridge University Press

Hence (4·5) now gives

$$L_D(s) = \frac{\overline{K\Delta}}{(N(K\Delta))^s} \sum_{\beta,\gamma} \left(\frac{D}{\rho}\right)_2 \sum_{\mu} \frac{\overline{\rho/K\Delta} + \overline{\mu}}{\{N(\rho/K\Delta + \mu)\}^s}. \tag{4·9}$$

We have now to continue (4·9) analytically as far as $s = 1$ and derive an expression for $L_D(1)$ in finite form. This we do in the next section.

5. *Formulae for* $L_D(1)$ *in terms of the* $\wp$*-functions.* Let $\wp(u)$ be the Weierstrass $\wp$-function, with periods Θ and $\sigma\Theta$, where Θ has been chosen so that $\wp(u)$ satisfies the equation

$$\wp'^2(u) = \wp(u)\,(\wp^2(u) - 4D\wp(u) + 2D^2) \tag{5·1}$$

for some convenient D to be fixed later. The Weierstrass $\wp$-function with periods $1, \sigma$ is then $\Theta^2\,\wp(\Theta u)$. The object of this section is the following theorem:

THEOREM 3. (i) *When* $\Delta \neq 1$

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

(ii) *When* $\Delta = 1$ *and* F *= a square, i.e.* $= 1$ *or* -2*, then*

$$L_D(1) = \frac{-\Theta}{8\sigma}\left[\left(\frac{\frac{\wp'\Theta}{4\sigma} - \frac{\wp'(3\Theta)}{4\sigma}}{\frac{\wp\Theta}{4\sigma} - \frac{\wp(3\Theta)}{4\sigma}}\right) + \left(\frac{\frac{\wp'(\Theta(1+\sigma))}{4\sigma} - \frac{\wp'(\Theta(3+\sigma))}{4\sigma}}{\frac{\wp(\Theta(1+\sigma))}{4\sigma} - \frac{\wp(\Theta(3+\sigma))}{4\sigma}}\right)\right.$$
$$\left. + \left(\frac{\wp'(\Theta(1+3\sigma)/4\sigma) - \wp'(\Theta(3+3\sigma)/4\sigma)}{\wp(\Theta(1+3\sigma)/4\sigma) - \wp(\Theta(3+3\sigma)/4\sigma)}\right) + \left(\frac{\wp'(\Theta(5+2\sigma)/4\sigma) - \wp'(\Theta(7+2\sigma)/4\sigma)}{\wp(\Theta(5+2\sigma)/4\sigma) - \wp(\Theta(7+2\sigma)/4\sigma)}\right)\right]$$

(iii) *When* $\Delta = 1$*, and* $-F$ *= a square, then* $L_D(1)$ *= as in* (ii) *but with the sign of the second and the third terms negative.*

Note. Theorem 3 is valid for any choice of D in (5·1) but later we shall have to choose $D = 1$ for theorem 4 to be true.

We have to consider the sum over μ in (4·9). Let $\alpha = \rho/K\Delta$. Then

$$\overline{\mu}^{s-1}\mu^s \frac{\overline{\alpha} + \overline{\mu}}{(N(\alpha+\mu))^s} = \left(1 + \frac{\overline{\alpha}}{\overline{\mu}}\right)^{1-s}\left(1 + \frac{\overline{\alpha}}{\overline{\mu}}\right)^{-s} = 1 + (1-s)\,\overline{\alpha}/\overline{\mu} - \frac{s\alpha}{\mu} + O(\mu^{-2}). \tag{5·2}$$

Now as the summand stands, the series is of course divergent as $s \to 1$ and so it is natural to consider the summand *minus* the first three terms of the right-hand side of (5·2). With this in mind, we define, for $\alpha \in \mathbf{Z}[\sigma]$,

$$\psi(\alpha, s) = \frac{\overline{\alpha}}{|\alpha|^{2s}} + \sum_{\mu \neq 0}\left\{\frac{\overline{\alpha} + \overline{\mu}}{|\alpha+\mu|^{2s}} - \frac{\overline{\mu}}{|\mu|^{2s}}\left(1 - \frac{s\alpha}{\mu} + \frac{\overline{\alpha}(1-s)}{\overline{\mu}}\right)\right\}. \tag{5·3}$$

Since this sum is uniformly convergent near $s = 1$, we have

$$\psi(\alpha, 1) = \frac{1}{\alpha} + \sum_{\mu \neq 0}\left(\frac{1}{\mu+\alpha} - \frac{1}{\mu} + \frac{\alpha}{\mu^2}\right) = \xi(\alpha),$$

where ξ is the Weierstrass zeta-function with periods $1, \sigma$. Now for s large, rearrange terms in (5·3) and get

$$\sum \frac{\overline{\alpha} + \overline{\mu}}{|\alpha+\mu|^{2s}} = \psi(\alpha, s) + \overline{\alpha}(1-s) \sum_{\mu \neq 0} \frac{1}{|\mu|^{2s}} - \sum_{\mu \neq 0} \frac{\overline{\mu}\alpha s}{\mu|\mu|^{2s}}$$

https://doi.org/10.1017/S0305004100043334 Published online by Cambridge University Press

(since the sum over $\pm\mu$ of the remaining term equals 0),

$$= \psi(\alpha, s) - 2\bar{\alpha}(s-1)\,\zeta_{\mathfrak{Q}(\sigma)}(s) - s\alpha\Sigma^* \quad \text{say;}$$

now substitution for the sum over μ in (4·9) gives

$$L_D(s) = \frac{\bar{K}\,\bar{\Delta}}{(N(K\Delta))^s} \sum_{\beta,\gamma} \left(\frac{D}{\rho}\right)_2 \{\psi(\alpha, s) - 2\bar{\alpha}(s-1)\,\zeta_{\mathfrak{Q}(\sigma)}(s) - \alpha s\Sigma^*\}. \tag{5·4}$$

Now as $s \to 1$, $(s-1)\,\zeta_{\mathfrak{Q}(\sigma)}(s) \to \pi/2\sqrt{2}$, and by letting

$$\chi(M) = \sum\sum_{m^2+2n^2 = N(\mu) \leqslant M} \left(\frac{m-n\sigma}{m+n\sigma}\right),$$

and noting that $\chi(M) = O(\sqrt{M})$, we find that

$$\Sigma^* = \sum_{m>0} [\chi(M+1) - \chi(M)] \frac{1}{(M+1)^s} = -\sum_{m>0} \chi(M) \left[\frac{1}{(M+1)^s} - \frac{1}{M^s}\right]$$

$$= \Sigma\chi(M) \frac{M^s((1+1/M)^s - 1)}{M^s(M+1)^s} \sim \Sigma \frac{\sqrt{M}\,.\,M^{s-1}}{M^{2s}} = \Sigma M^{-s-\frac{1}{2}} \to \text{a limit} = \mathfrak{S} \text{ say as } s \to 1.$$

Thus letting $s \to 1$ in (5·4) we find

$$L_D(1) = \frac{1}{K\Delta} \sum_{\beta,\gamma} \left(\frac{D}{\rho}\right)_2 \left\{\xi(\alpha) - \frac{2\bar{\alpha}\pi}{2\sqrt{2}} - \alpha\mathfrak{S}\right\}. \tag{5·5}$$

Also
$$\xi(u+v) = \xi(u) + \xi(v) + \frac{\Theta}{2}\left(\frac{\wp'(\Theta u) - \wp'(\Theta v)}{\wp(\Theta u) - \wp(\Theta v)}\right). \tag{5·6}$$

Write $u = \beta/\Delta$, $v = \gamma/\kappa$ and write $\alpha = (\beta/\Delta) + (\gamma/\kappa)$ in (5·5). Note also that

$$\left(\frac{D}{\rho}\right)_2 = \left(\frac{K}{\Delta}\right)_2 \left(\frac{\beta}{\Delta}\right)_2 \left(\frac{\epsilon F}{\Delta}\right)_2 \left(\frac{\epsilon F}{\gamma}\right)_2.$$

Case (i) of the theorem splits up into 2 subcases.

Subcase (i). $\epsilon F \neq$ a square; then the sum over β and γ in most of the terms of (5·5) is effectively $\sum(\beta/\Delta)_2$ and $\sum(\epsilon F/\gamma)_2$ respectively, and these are $= 0$ because $\Delta \neq 1$ and $\epsilon F \neq$ a square. Hence (5·5) implies

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

Subcase (ii). $\epsilon F =$ a square; then (5·5) implies

$$L_D(1) = \frac{1}{K\Delta} \Sigma \left(\frac{K\beta}{\Delta}\right)_2 \left\{\frac{\Theta}{2}\left(\frac{\wp'(\Theta\beta/\Delta) - \wp'(\Theta\gamma/K)}{\wp(\Theta\beta/\Delta) - \wp(\Theta\gamma/K)}\right) + \xi\left(\frac{\beta}{\Delta}\right) - \frac{\pi\bar{\beta}}{\sqrt{2}\,\bar{\Delta}} - \frac{\mathfrak{S}\beta}{\Delta}\right\},$$

since the sum over β of the other terms $= 0$. But in the last three terms of the above, by changing the sum over β to that over $-\beta$, we find that they all vanish since $(-1/\Delta)_2 = 1$, Δ being real. This proves (i) of Theorem 3.

Now let $\Delta = 1$; then $D = F, \beta = 1, \alpha = 1 + (\gamma/K)$ and γ takes eight values, the l in the set Λ. Also

$$\left(\frac{D}{\rho}\right)_2 = \left(\frac{F}{K+\gamma}\right)_2 = \left(\frac{F}{\gamma}\right)_2$$

by the very definition of K. Now letting $s \to 1$ in (5·4) we get

$$L_D(1) = \frac{1}{4\sigma} \sum_{\gamma} \left(\frac{F}{\gamma}\right)_2 \left\{\xi\left(1 + \frac{\gamma}{4\sigma}\right) - \frac{\pi}{\sqrt{2}}\left(1 + \frac{\bar{\gamma}}{4\bar{\sigma}}\right) - \mathfrak{S}\left(1 + \frac{\gamma}{4\sigma}\right)\right\}. \tag{5·7}$$

https://doi.org/10.1017/S0305004100043334 Published online by Cambridge University Press

Note now the following results:

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

Proof. Since the right-hand side of (5·5) does not depend on the choice of the representatives ρ of the residue classes mod $K\Delta$, we change just one of the ρ's to $\rho + K\Delta$ and result follows by cancellation.

COROLLARY. $2\xi(\frac{1}{2}) = \pi/\sqrt{2} + \mathfrak{S}$.

Proof. Put $u = -\frac{1}{2}$ in (i).

(ii) Let $1, \sigma = 2\omega_1, 2\omega_2$ be the periods of the $\wp$-function, so that $\xi(u+2\omega_i) = \xi(u) + 2\eta_i$ say, where $\eta_i = \xi(\omega_i)$. Then $\eta_1\omega_2 - \eta_2\omega_1 = \frac{1}{2}\pi i$.

Proof. See (8), p. 446.

COROLLARY. $\sigma\xi(\frac{1}{2}) - \xi(\frac{1}{2}\sigma) = \pi i$.

Going back to (5·7), first let F = a square; then

$$4\sigma L_D(1) = \sum_{\gamma} \xi\left(\frac{\gamma}{4\sigma}\right) - \frac{3\pi}{\sqrt{2}}(1+\sigma) - 3\mathfrak{S}.(1-\sigma), \tag{5·8}$$

since $\sum \gamma = 24 + 12\sigma$. Now in the sum in (5·8), by bracketing the terms in 1, 3; $1+\sigma$, $3+\sigma$; $1+3\sigma$, $3+3\sigma$; $5+2\sigma$, $7+2\sigma$; and using (5·6), we get the result (i.e. case (ii) of Theorem 3).

Similarly, the case $F \neq$ a square, may be dealt with. This completes the proof of Theorem 3.

6. *Rationality and integrity.* Throughout this section, we shall take the K of Section 5 to be 8 rather than 4σ for convenience (see especially the proof of Lemma 2).

Having worked out what $L_D(1)$ is, we now consider how nearly it is a rational integer. It is well known (7) that the division values of $\wp$ and $\wp'$ are in general algebraic functions of g_2, g_3, in the usual notation. Now choose D to be $= 1$ in (5·1). It follows then from our formulae for $L_D(1)$ that $L_D(1)/\Theta$ is an algebraic number. The object of this section is to prove the following

THEOREM 4. *Let $D > 1$ be a positive square-free integer and Θ the real period of the Weierstrass $\wp$-function satisfying*

$$\wp'^2 = \wp^3 - 4\wp^2 + 2\wp. \tag{6·1}$$

Then $8\sqrt{D}.L_D(1)/\Theta$ and $8\sqrt{(2D)}.L_{-D}(1)/\Theta$ are rational integers.

The proof of this result falls into two parts: rationality and integrity. We shall begin with rationality.

THEOREM A. *With the hypothesis of Theorem 4, $\sqrt{D}.L_D(1)/\Theta$ and $\sqrt{(2D)}.L_{-D}(1)/\Theta$ are rational numbers.*

Let $\mathfrak{a}$ be a proper 8Δ-division point of the curve $y^2 = x(x^2 - 4x + 2)$ (see (6·1)). Let $k = \mathbf{Q}(\sigma)$ and let $\mathfrak{R} = k(\mathfrak{a})$.

LEMMA 1. (i) $\mathfrak{R}/k$ *is normal,*

(ii) $\mathrm{Gal}(\mathfrak{R}/k)$ *is Abelian and isomorphic to a subgroup of the multiplicative group of elements* mod 8Δ, *prime to* 8Δ *in* k.

https://doi.org/10.1017/S0305004100043334 Published online by Cambridge University Press

Proof. Let τ: $\mathfrak{R} \to \mathfrak{L}$ be an isomorphism of $\mathfrak{R}$ which leaves k element-wise fixed. This takes $\underline{\mathfrak{a}} \to \underline{\mathfrak{a}}'$ say and $k(\underline{\mathfrak{a}}') = \mathfrak{R} \leqslant \mathfrak{L}$; but τ is an isomorphism and so $\mathfrak{R} = \mathfrak{L}$; therefore τ is an automorphism. Now taking $\mathfrak{L}$ to be any conjugate field to $\mathfrak{R}$, (i) follows.

To see (ii), note that an automorphism of $\mathfrak{R}/k$ is of the form $\underline{\mathfrak{a}} \to \underline{\mathfrak{a}}' = t\underline{\mathfrak{a}}$ where t is an integer of k mod 8Δ prime to 8Δ and so $\tau \leftrightarrow t$ gives what (ii) wants.

LEMMA 2. *Let ζ be a primitive nth root of* 1, *where n divides* 8Δ; *then*

$$\zeta \in \mathfrak{R} \quad \textit{and} \quad \tau\zeta = \zeta^{\operatorname{norm} t}.$$

Proof. Let G be the group of the 8Δth division points. Then there is a pairing (see (3)) $\chi(\underline{\mathfrak{a}}, \underline{\mathfrak{b}}) \in \Omega$, for any pair of points $\underline{\mathfrak{a}}, \underline{\mathfrak{b}} \in G$, where Ω is the group of the 8Δth roots of 1.

Now for any automorph τ of $\mathfrak{R}/k$, we have

$$\tau(\chi(\underline{\mathfrak{a}}_0, \underline{\mathfrak{a}}_0^*)) = \chi(\tau\underline{\mathfrak{a}}_0, \tau\underline{\mathfrak{a}}_0^*). \tag{6·2}$$

Let $\underline{\mathfrak{a}}_0 \in G$ be such that G is the set of all $(r + s\sigma)\,\underline{\mathfrak{a}}_0$, where $r, s = 0, 1, \ldots, 8\Delta - 1$. Then $\tau(\underline{\mathfrak{a}}_0) = r_1\,\underline{\mathfrak{a}}_0 + s_1\,\underline{\mathfrak{b}}_0$, where $\underline{\mathfrak{b}}_0 = \sigma\underline{\mathfrak{a}}_0$; and $\tau(\underline{\mathfrak{b}}_0) = -2s_1\,\underline{\mathfrak{a}}_0 + r_1\,\underline{\mathfrak{b}}_0$. Now by the skew-symmetry of χ, we have

$$\chi(u_1\,\underline{\mathfrak{a}}_0 + v_1\,\underline{\mathfrak{a}}_0^*,\quad u_2\,\underline{\mathfrak{a}}_0 + v_2\,\underline{\mathfrak{a}}_0^*) = (\chi(\underline{\mathfrak{a}}_0, \underline{\mathfrak{a}}_0^*))^{u_1 v_2 - v_1 u_2}.$$

So letting $\underline{\mathfrak{a}}_0^* = \sigma\underline{\mathfrak{a}}_0$, and using (6·2) we get

$$\tau(\chi(\underline{\mathfrak{a}}_0, \underline{\mathfrak{b}}_0)) = (\chi(\underline{\mathfrak{a}}_0, \underline{\mathfrak{b}}_0))^{r_1^2 + 2s_1^2} = (\underline{\mathfrak{a}}_0, \underline{\mathfrak{b}}_0)^{\operatorname{norm}(r_1 + \sigma s_1)}.$$

But for a suitable choice of $\mathfrak{a}_0$, $\chi(\underline{\mathfrak{a}}_0, \underline{\mathfrak{b}}_0) = \zeta_0$ is any primitive nth root of 1, where $n \mid 8\Delta$ so $\tau\zeta_0 = \zeta_0^{\operatorname{norm} t}$.

This proves the lemma.

Let $\tau \leftrightarrow t$ be an automorphism of $\mathfrak{R}/k$. Let $e(t)$ be the unit ± 1 such that $e(t)\,t \equiv$ some $l \in \Lambda$ (see Section 3). Let $\tau' \leftrightarrow t' = e(t)\,t$. Write $L_D(1) = (\Theta/2K\Delta)\,L^*$ say.

LEMMA 3. $\tau L^* = e(t)\,(D/t)_2\,L^*$.

Proof. $\tau'(L^*) = (D/t')_2\,L^*$ since $\beta' = t'\beta$ runs through residues mod Δ and $\gamma' = t'\gamma$ runs through residues modulo 8 since $t' \in \Lambda$. But $\tau'(L^*) = e(t)\,\tau(L^*)$ since

$$\wp'(e(t)\,u) = e(t)\,\wp'(u) \quad \text{and} \quad \wp(e(t)\,u) = \wp(u).$$

This proves Lemma 3.

We shall now show that the $e(t)$ of Lemma 3 is always equal to 1, i.e. that the τ corresponding to those t which lie in $-\Lambda$ are inadmissible. It is here that we have to make a choice of the D as in (6·1). More precisely we have the following

LEMMA 4. *There exists a suitable D such that the automorphisms τ of $\mathfrak{R}/k$ corresponding to the t which lie in $-\Lambda$ are inadmissible.*

Proof. Let $\mathbf{P} = (x_1, y_1)$ be a 4σ – division point. The others are then

$$\pm t_j\,\mathbf{P} \quad (j = 1, 2, \ldots, 8),$$

where $\{t_1 = 1, t_2, \ldots, t_8\}$ is the set Λ. Write $t_j\,\mathbf{P} = (x_{t_j}, y_{t_j})$. Let $\eta = \sum_{j=1}^{8} y_{t_j}$. Then $\eta \overset{\tau}{\to} \eta$ when $\tau \leftrightarrow t \in \Lambda$ and $\eta \overset{\tau}{\to} -\eta$ when $\tau \leftrightarrow t \in -\Lambda$. Thus certainly $\eta^2 \in \mathbf{Q}$. Now η is of the form $D\sqrt{D}$. (a sum of eight terms of the form appearing in (2·4)). Therefore

$$\eta^2 = D^3.(d_1/d_2)$$

https://doi.org/10.1017/S0305004100043334 Published online by Cambridge University Press

say where $d_1, d_2 \in \mathbf{Z}$ since $\eta^2 \in \mathbf{Q}$. Thus again $\eta = D\sqrt{(Dd_1/d_2)}$, and by choosing $D = -2d_2/d_1$ (or $-2d_1 d_2$), for example, we see that we can pick a D such that $\eta \in \mathbf{Q}(\sigma)$.

Now suppose, to begin with that $\eta \neq 0$; then $\tau(\eta) = \eta$ for all τ since $\eta \in \mathbf{Q}(\sigma)$; but $\tau(\eta) = -\eta$ if $\tau \leftrightarrow t \in -\Lambda$, whence such τ are inadmissible. Now if η is equal to 0, then one of the

$$\eta_i = \sum_{j=1}^{8} x_{ij}^i . y_{t_j} \quad (i = 0, 1, \ldots, 7)$$

is non-zero since the Vandermonde determinant of the coefficients is non-zero. Lemma 4 thus follows.

LEMMA 5. *The* $\eta_0^2 = \eta^2$ *of Lemma* 4 *is equal to* $-512 . D^3$.

Proof. Refer back to (2·7). Then $\eta^2 = \left(\sum_{j=1}^{8} y_{t_j}\right)^2$ and the y_{t_j} are all known by (2·7) and (2·4), and working out the whole thing, using (2·8) gives Lemma 5.

From Lemma 5 we see that $\eta = -16D . \sqrt{(-2D)}$ and by choosing $D = 1$, we can make η lie in $\mathbf{Q}(\sigma)$. This gives our normalized key curve as required by Theorem 4.

LEMMA 6. $\tau\sqrt{2} = (2/t)_2 . \sqrt{2}$.

Proof. Use Lemma 2 and the fact that $\sqrt{2} = \zeta + \zeta^{-1}$ where $\zeta = e^{\frac{1}{4}\pi i}$.

Now let

$$\Gamma_p = \sum_{g \pmod p} \left(\frac{g}{p}\right)_{\mathbf{Z}} . \zeta^g,$$

where ζ is a primitive pth root of 1 and p is a rational prime, be the Gaussian sum. Then it is well known that

$$\Gamma_E = \begin{cases} \sqrt{|E|} & \text{if} \quad |E| \equiv 1 \pmod 4, \\ i\sqrt{|E|} & \text{if} \quad |E| \equiv 3 \pmod 4, \end{cases}$$

where $\Gamma_E = \sum (g/E)_{\mathbf{Z}} . \zeta^g$ (ζ = primitive Eth root of 1), and where E is any square-free odd rational integer. We have

$$\tau\Gamma_D = \sum \left(\frac{g}{D}\right)_{\mathbf{Z}} . \zeta^{(Nt)g} = \left(\frac{\text{norm } t}{D}\right)_{\mathbf{Z}} \Gamma_D.$$

LEMMA 7. $\tau\sqrt{D} = (D/t)_2 . \sqrt{D}$, *where we are taking* $D > 0$.

Proof. Use all the above and result follows.

Now using Lemmas 3, 6, 7 we have

$$\tau(\sqrt{D} . L_D^*) = \sqrt{D} . L_D^* \quad \text{and} \quad \tau(\sqrt{(2D)} . L_{-D}^*) = \sqrt{(2D)} . L_{-D}^*,$$

and so the two expressions of Theorem A are invariant under each automorphism τ of $\mathfrak{R}/k$; therefore they $\in k$. This completes the first stage of the argument.

To show that the expressions actually belong to $\mathbf{Q}$, we must show that they are invariant under the automorphism T (say): $\sigma \to \overline{\sigma}$ of $\mathbf{Q}(\sigma)$ ($= k$) over $\mathbf{Q}$. This is easily checked. This completes the proof of Theorem A.

We now come to the integrity part of the argument.

THEOREM B. $\Delta^{9/8} . 8L_D(1)/\Theta$ *is an algebraic integer.*

The idea is to estimate the denominator of $L_D(1)$. Using the addition formula:

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

https://doi.org/10.1017/S0305004100043334 Published online by Cambridge University Press

we see from Theorem 3 that

$$L_D(1) = \frac{\Theta}{8\Delta} \sum_{\beta,\gamma} \left(\frac{D}{\rho}\right)_2 \left\{ \wp\left(\frac{\Theta\beta}{\Delta}\right) + \wp\left(\frac{\Theta\gamma}{8}\right) + \wp\left(\Theta\left(\frac{\beta}{\Delta} + \frac{\gamma}{8}\right)\right)\right\}^{\frac{1}{2}}$$

and it is enough to look at the denominator of

$$\wp\left(\frac{\Theta\beta}{\Delta}\right) + \wp(\tfrac{1}{8}\Theta\gamma) + \wp\left(\Theta\left(\frac{\beta}{\Delta} + \frac{\gamma}{8}\right)\right) = \mathfrak{N} \quad \text{say.}$$

We shall use the following results due to Cassels (4).

(i) If (x, y) is a point of $\mathfrak{C}$ of exact order $p^\alpha (p \neq 2, 3)$ and $\mathfrak{m}$ is the ideal denominator of x, then

$$\mathfrak{m}^{\frac{1}{2}(p-p^{\alpha-1})} \quad \text{divides } p.$$

(ii) If $p = 3$ (in (i)), then $\mathfrak{m}^{\frac{1}{2}(p^{2\alpha}-p^{2(\alpha-1)})}$ divides p.

(iii) For $p = 2$, x is an algebraic integer.

(iv) If (x, y) has exact order $n \neq a$ prime power, then x is an algebraic integer.

A slight modification (given below) of the arguments given by Cassels, proves the following stronger result when there is complex multiplication on $\mathfrak{C}$:

(i') Hypothesis as in (i), then $\mathfrak{m}^{\frac{1}{2}(p^{2\alpha}-p^{2(\alpha-1)})}$ divides p.

Proof. Recalling the proof given by Cassels (Theorem IV, p. 171 of (4)) we see that when we have complex multiplication by σ, we can take the s in $\mathbf{Z}[\sigma]$, rather than in $\mathbf{Z}$, and the denominators of x_1 and x_s, with $(s, p) = 1$, are the same. But now there are $\frac{1}{2}(p^{2\alpha} - p^{2(\alpha-1)})$ x_s's and the result follows.

We look at each term of $\mathfrak{N}$ separately. To begin with $\wp(\Theta\gamma/8)$, $\gamma \in \Lambda$ has exact order 2^3 since no γ is even, therefore by (iii) above, we have:

$$\wp(\tfrac{1}{8}\Theta\gamma) \quad \text{is an algebraic integer.} \tag{6·3}$$

Let $\Delta = p_1 p_2 \ldots$ (where the $p_j \geqslant 3$ are rational primes) $= \pi_1 \pi_2 \ldots$ say, the prime factorization in $\mathbf{Z}[\sigma]$. Now β runs through the residues mod Δ, so when

$$\beta = \prod_{\pi_j \mid \Delta, j \neq i} \pi_j \quad (= \beta_i \text{ say}),$$

we have $\wp(\Theta\beta_i/\Delta) = \wp(\Theta/\pi_i)$, which has exact order

$$= \begin{cases} \text{norm } \pi_i & \text{if } \pi_i \text{ is complex,} \\ \pi_i & \text{if } \pi_i \text{ is rational} \end{cases}$$
$$= p_j \qquad \text{for some } j.$$

Hence by (i), the ideal denominator $\mathfrak{m}$ of $\wp(\Theta\beta/\Delta)$ satisfies: $\mathfrak{m}^{\frac{1}{2}(p-1)}$ divides p, and so

$$(p_i)^{2\lfloor (p_i^2-1)} . \wp(\Theta\beta i/\Delta) \text{ is an algebraic integer.} \tag{6·4}$$

For all other values of β, the exact order of $\wp(\Theta\beta/\Delta)$ is not a prime power and so by (iv),

$$\wp(\Theta\beta/\Delta) \text{ is an algebraic integer.} \tag{6·4}'$$

Finally, all the

$$\wp\left(\Theta\left(\frac{\beta}{\Delta} + \frac{\gamma}{8}\right)\right)$$

https://doi.org/10.1017/S0305004100043334 Published online by Cambridge University Press

contribute no new denominator and so taking the product of the denominators, we find that

$$\left\{\prod_{p\mid\Delta} p^{2/(p^2-1)}\right\}\mathfrak{N}$$

is an algebraic integer, i.e.

$$\left\{\prod_{p\mid\Delta} p\,1/(p^2-1)\right\}\mathfrak{N}^{\frac{1}{2}} \text{ is an algebraic integer.} \tag{6·5}$$

We now estimate $\prod_{p\mid\Delta} p^{1/(p^2-1)}$ as follows: Let $p^* = \min p$; so that $p^* \geqslant 3$. The above product then is

$$\leqslant \prod_{p\mid\Delta} p^{1/(p^{*2}-1)} = \Delta^{1/(p^{*2}-1)} \leqslant \Delta^{\frac{1}{8}}$$

since $p^* \geqslant 3$. Hence $\Delta^{\frac{1}{8}}.\mathfrak{N}^{\frac{1}{2}}$ is an algebraic integer. This completes the proof of Theorem B.

Theorem 4 can now be proved as follows:

By Theorem A, $\sqrt{D}.8L_D(1)/\Theta = A/B$ say, is a rational number in its lowest terms. By Theorem B, $\Delta^{\frac{5}{8}}.\Delta^{\frac{1}{2}}.8L_D(1)/\Theta$ is an algebraic integer $= \Gamma$ say. Hence

$$\frac{A}{B} = \frac{\sqrt{(D/\Delta)}\,\Gamma}{(\Delta)^{\frac{5}{8}}} = \frac{\text{algebraic integer}}{(\Delta)^{\frac{5}{8}}},$$

therefore $\Delta^{\frac{5}{8}}.(A/B) = x$ say, is an algebraic integer; therefore $B^8x^8 - A^8\Delta^5 = 0$ is the irreducible equation over $\mathbf{Q}$ satisfied by x. But B^8 does not divide $A^8(\Delta)^5$ and so, since x is an algebraic integer, we have $B^8 = 1$, therefore $B = \pm 1$, and so $A/B \in \mathbf{Z}$.

Thus $8\sqrt{D}.L_D(1)/\Theta \in \mathbf{Z}$, and similarly $8\sqrt{(2D)}.L_{-D}(1)/\Theta \in \mathbf{Z}$. This completes the proof of Theorem 4.

7. *Contribution of the prime* $p = \infty$ *to the Tamagawa number.* We consider here briefly the contribution of the prime $p = \infty$ to the Tamagawa number of our curve (cf. (1)).

Case 1. $D > 0$; then the three meets of Γ with $y = 0$ are 0, $D(2-\sqrt{2})$, $D(2+\sqrt{2})$, and so the contribution τ is

$$\int_0^{D(2-\sqrt{2})} + \int_{D(2-\sqrt{2})}^{\infty} (dx/y) = \int (dx/y) \quad \text{say for short,}$$

$$= \int \frac{dx}{\sqrt{\{x(x^2-4Dx+2D^2)\}}}$$

and letting $x = tD$, this equals

$$\frac{1}{\sqrt{D}} \int \frac{dt}{\sqrt{t(t^2-4t+2)}} = \Theta/\sqrt{D}$$

in the usual notation.

Case 2. $D < 0$. This is more difficult.

LEMMA 1. *If* $y^2 = x(x^2+8Dx+8D^2)$, *then*

$$Y^2 = X(X^2-4DX+2D^2), \quad \textit{where} \quad X = \frac{y^2}{4x^2}, \quad Y = \frac{y}{8} - \frac{D^2y}{x^2}. \tag{7·1}$$

Proof. Direct substitution. (More elegantly use isogeny arguments.)

LEMMA 2. $dX/Y = 2(dx/y)$.

Proof. $dX = \left(\dfrac{x^2-8D^2}{4x^2}\right)dx$, $Y = \dfrac{x^2-8D^2}{8x^2}\,y$, and result follows.

https://doi.org/10.1017/S0305004100043334 Published online by Cambridge University Press

Let λ be the map $(x, y) \to (X, Y)$. This has kernel $\{(0,0), \mathbf{0}\}$ where $\mathbf{0}$ is this zero element of the group of rational points. Hence the contribution τ is equal to

$$\int_{\text{whole branch}} (dX/Y) = 2\int_{\frac{1}{2}\text{ the branch}} (dx/y) = \int_{\text{whole branch}} (dx/y) = \int \frac{dx}{\sqrt{\{x(x^2+8Dx+8D^2)\}}}$$

and letting $x = -2Dt$, this evaluates to $\Theta/\sqrt{(-2D)}$.

It follows that the irrational factors $\sqrt{(D)}/\Theta$ and $\sqrt{(2D)}/\Theta$ in Theorem 4 are just the contributions of $p = \infty$. Everything now fits in beautifully with the Birch–Swinnerton-Dyer conjectures.

REFERENCES

(1) BIRCH, B. J. and SWINNERTON-DYER, H. P. F. Notes on elliptic curves, I. *J. Reine Angew Math.* **212** (1963), 7–25, and II. *J. Reine Angew Math.* **218** (1965), 79–108.

(2) CASSELS, J. W. S. Arithmetic on an elliptic curve. *Proc. Intern. Congress Math., Stockholm* (1962), 234–246.

(3) CASSELS, J. W. S. Diophantine equations with special reference to elliptic curves. *J. London Math. Soc.* **41** (1966), 193–291.

(4) CASSELS, J. W. S. A note on the division values of $\wp(u)$. *Proc. Cambridge Philos. Soc.* **45** (1948), 167–172.

(5) DEURING, M. Die Typen der Multiplikatorenringe elliptische Funktionenkorper. *Abh. Math. Sem. Univ. Hamburg* **14** (1941), 197–272.

(6) DEURING, M. Die Zetafunktion einer algebraichen Kurve von Geschlechte Eins, I, II, III, IV. *Nachr Akad. Wiss Göttingen Math.-Phys Kl II* (1953), 85–94; (1955), 13–42; (1956), 37–76; (1957), 55–80.

(7) WEBER, H. *Algebra*, vol. 3 (2nd edn, Braunschweig, 1908).

(8) WHITTAKER, E. T. and WATSON, G. N. *Modern Analysis* (Cambridge, 1902).

https://doi.org/10.1017/S0305004100043334 Published online by Cambridge University Press