Notes on elliptic curves. II.

Swinnerton-Dyer, H.P.F.

in: Journal für die reine und angewandte Mathematik - 218 | Periodical
30 page(s) (79 - 108)

Notes on elliptic curves. II

By *B. J. Birch* at Manchester and *H. P. F. Swinnerton-Dyer* at Cambridge

To Gina

§ 1. Introduction

During the past six years, we have made extensive calculations on cubic curves of the form

$$\Gamma: y^2z = x^3 - Axz^2 - Bz^3 \tag{1.1}$$

where A, B are rational integers. In a previous paper [2], we have shown how $\smile\!\!\!\!A$, the group of rational points on (1.1), can conveniently be found on an electronic computer; and we have given extensive tables. In this and subsequent papers, we put forward some conjectures connecting it with other more accessible quantities, together with the numerical evidence on which they are based.

We begin this paper with a history of our investigations. This may make the rest of the paper more understandable; and it enables us to acknowledge the very considerable help we have obtained from other workers in this field.

After the work of Siegel [19] on quadratic forms, it is natural to look at the product

$$\prod N_p/p, \tag{1.2}$$

where N_p is the number of rational points on the curve defined by (1.1) over the finite field of p elements. Write for convenience

$$f(P) = \prod N_p/p \text{ over all } p \leqq P.$$

In the autumn of 1958 we calculated, for a number of curves (1.1), the behaviour of $f(P)$ as P increased. It turned out that the rate of increase of $f(P)$ was fairly closely correlated with the number of generators of infinite order of $\smile\!\!\!\!A$; and there was some tendency for $f(P)$ to be large when the generators of $\smile\!\!\!\!A$ (or more precisely the corresponding values of x, y, z) were small. We were in fact able to predict the number of generators of $\smile\!\!\!\!A$ for specific curves Γ, with fairly consistent success, by examining the values of $f(P)$.

Since the behaviour of $f(P)$ as $P \to \infty$ is at least formally linked to the behaviour of $\zeta_\Gamma(s)$ near $s = 1$ (see § 2 below), we were led to make the two linked conjectures:

(A) *If g is the number of generators of $\smile\!\!\!\!A$ of infinite order, then $f(P) \sim C(\log P)^g$ as $P \to \infty$, and $\zeta_\Gamma(s) \sim C'(s-1)^{g-1}$ as $s \to 1$, for some constants C, C' depending on Γ.*

At this point we ran into difficulties. The value of $f(P)$ oscillates vigorously as P increases, and there seems little hope of being able to find the constant C by this method

with an error of less than say $10^0/_0$. (It takes $O(p)$ operations to calculate N_p, so we cannot let P become very big without spending an unreasonable amount of time.) Moreover, the terms of the product (1. 2) corresponding to primes p dividing $6(4A^3 - 27B^2)$ are almost certainly the wrong ones; and it was not then known what the right ones were. Thus, even if we had been able to find the value of C for a particular curve Γ, there would have been little prospect of identifying it; this difficulty has since been removed by the work of Tamagawa [23]; see § 7 and later on in this introduction. We hope to return to these direct calculations in a subsequent note.

For those curves Γ which admit complex multiplication an alternative approach is possible; for in this case it is known that $\zeta_\Gamma(s)$ can be expressed in terms of the Riemann zeta function $\zeta(s)$ and Hecke L-series. In particular, for the curve

$$\Gamma = \Gamma_D\colon\ y^2z = x^3 - Dxz^2 \tag{1. 3}$$

(to which we confine ourselves for the rest of this paper) we have

$$\zeta_\Gamma(s) = \frac{\zeta(s)\,\zeta(s-1)}{L_D(s)} \tag{1. 4}$$

where $L_D(s)$ is the Hecke L-series defined by (2. 7) below. Formally, $L_D(1) = \prod (N_p/p)^{-1}$. In the summer of 1960 we found an approximation to $L_D(1)$ as a multiple of a reasonably rapidly convergent series. In this way we were able with fair confidence to determine whether $L_D(1)$ vanished or not; and obtained a good deal of evidence for the conjecture

$$L_D(1) = 0 \quad \textit{if and only if } g > 0, \tag{1. 5}$$

which is a weaker form of conjecture (A) above. However, when $g = 0$ we were still not able to calculate $L_D(1)$ accurately enough to be able to interpret it.

At this point Davenport came to our rescue, by suggesting that it should be possible to express $L_D(1)$ in finite form in terms of division values of the Weierstrass $\wp$-function defined by the equation

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

The details of this transformation are given in § 3 below. Exact (algebraic) evaluation of the formulae given there in a few simple cases — together with a remark of Kneser that 'the answer should be an integer' — suggested that

$$L_D(1) = \begin{cases} D^{-\frac{1}{4}} \cdot \omega \cdot \sigma(D) \text{ for } D > 0, \\ (-4D)^{-\frac{1}{4}} \cdot \omega \cdot \sigma(D) \text{ for } D < 0, \end{cases} \tag{1. 6}$$

where ω is the real period of $\wp(u)$ and $\sigma(D)$ is in general a small positive integer. We prove in § 4, by means of class field theory, that $\sigma(D)$ is in general a rational integer; but we can prove nothing about its sign. Using *EDSAC* II, we calculated $\sigma(D)$ from these formulae in a large number of cases, obtaining the results given in Table 1.

To compare these results with our conjecture (1. 5) we needed to be able to find the corresponding values of g. For large D the methods of our previous paper proved too slow and we had to use a method tailored to our special curve (1. 3). This is described in § 5: we do not regard it as novel, but have to describe it at length in the absence of any satisfactory reference. All the results we have obtained are compatible with (1. 5); but there are many curves for which we were not able to find the value of g.

The rest of this paper is concerned with the interpretation of the integer $\sigma(D)$ when it does not vanish. We hoped from the beginning that this would turn out to be

essentially the order of the Tate-Šafarevič group of Γ_D (for a concise popular exposition, see for instance Cassels [6]), and this hope was supported by the fact that $\sigma(D)$ was always a power of 2 times a square. (Cassels [5] has shown that if the Tate-Šafarevič group is finite, its order is a square.) But we found it difficult to get the details right; the trouble is that if $p \mid 2D$ then N_p/p is not usually the natural factor to take in (1. 2), and it was not obvious what one should replace it by. Eventually, much helped by prodding from Cassels, we realized that we should replace the product (1. 2) by $\tau(D)$, the Tamagawa number of the curve Γ_D (see [23]). This too is an infinite product, and differs from (1. 2) only in finitely many terms; the details are described in § 6. We conjecture:

(B) *If* $g = 0$ *then the order of the Tate-Šafarevič group of* Γ_D *is* $\eta^2(D)/\tau(D)$, *where* $\eta(D)$ *is the number of rational points on* Γ_D.

We can almost interpret this in terms analogous to Tamagawa's form of Siegel's theorem. For there is a natural group structure on the set of points lying on everywhere locally soluble coverings, and its Tamagawa number is $\tau(D)$ times the order of the Tate-Šafarevič group — in other words, $\eta^2(D)$ according to our conjecture. That the factor involved should be the square of the number of rational points rather than the number of rational points seems a little odd; subsequently, this has been partly explained by Cassels [7].

The tangible evidence for our conjecture (B) is not great, for unfortunately little is known about the Tate-Šafarevič group — indeed there is not even any case in which it has been proved to be finite. We have never computed more than its 2-component: in every numerical case this at any rate has the order suggested by the conjecture. The labour involved in finding any other component appears to us prohibitive. We note that in our tables $\tau(D)$ is always a perfect square, as it must be in order to be consistent with Cassels' work. But at Stockholm we were informed that Šafarevič possessed results which, in view of the values for $\tau(D)$ given in Table 2, seemed inconsistent with our conjectures. Recently, Cassels [7] has given additional evidence which helps to confirm our conjecture; and the analogy with the work of Ono [18] is very striking.

Certain cases of the function field analogue of (A) are known to be true [20]. In particular, Mumford has shown that two elliptic curves over a finite field are isogenous if and only if they have the same number of rational points (in the classical case, and in older language, this must have been known to Weber; see § 113 of his Algebra [21]; see also Manin [26]); he deduced the analogue of (1. 5) for an elliptic curve with coefficients in a finite field k, considered over a function field of genus 1 over k. Tate [27] has given conjectures concerning the zeta function of a variety over a finite field which generalise this analogue, and which he has confirmed in many cases.

In conclusion, we must apologise for our rather considerable delay in publication; we hope that no harm has been done, since fairly detailed accounts of our results have been publicised — in particular, Cassels was kind enough to describe our work in his Stockholm talk [6], and one of the authors has given an account in a lecture delivered in Pasadena [3]. The informed reader will recognise that this introduction is already somewhat dated.

§ 2. The zeta-function of Γ

Suppose that Γ is defined over the rationals by (1. 1), and is a complete non-singular curve of genus 1. For almost all p, the curve defined by (1. 1) over the finite field of p elements retains these properties; and if it contains N_p points defined over this finite

field, its zeta-function is

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

The global zeta-function of Γ is therefore

$$\zeta_\Gamma(s) = \prod_p \zeta_{\Gamma,p}(s) = \frac{\zeta(s)\,\zeta(s-1)}{L_\Gamma(s)}, \tag{2. 2}$$

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

$$L_\Gamma(s) = \prod_p \{1 + (N_p - p - 1)\, p^{-s} + p^{1-2s}\}^{-1} \tag{2. 3}$$

and finitely many factors in the product may not be the most natural ones. Formally we have

$$L_\Gamma(1) = \prod (N_p/p)^{-1};$$

but for general Γ the product (2. 3) is only known to converge in $R(s) > \frac{3}{2}$, and it is not known whether it can be continued analytically outside this region.

If Γ (possibly defined over an algebraic number field) admits complex multiplication, Deuring [9] has shown that $L_\Gamma(s)$ can be analytically continued over the whole plane and satisfies a functional equation. By this means he also found a natural form for the missing factors in (2. 3), namely that which makes the functional equation as simple as possible.

For the special curve

$$\Gamma_D\colon\ y^2 z = x^3 - Dxz^2 \tag{2. 4}$$

of this paper, it is simplest to use the known explicit formulae for N_p. For convenience we start by recalling some properties of the quartic residue symbol. Suppose that ν is an odd Gaussian prime and μ any Gaussian integer prime to ν. Then we define the quartic residue symbol $\left(\frac{\mu}{\nu}\right)_4$ to be that power of i which is congruent to

$$\mu^{(N\nu-1)/4} \bmod \nu,$$

where N stands for the norm. This is multiplicative in μ, and we extend it to be multiplicative in ν by the condition

$$\left(\frac{\mu}{\nu_1\nu_2}\right)_4 = \left(\frac{\mu}{\nu_1}\right)_4 \left(\frac{\mu}{\nu_2}\right)_4.$$

We also write $(\mu/\nu)_4 = 0$ when μ, ν are not coprime. The principal properties we shall need are that $(\mu/\nu)_4 = 1$ for μ, ν coprime and real, and the law of reciprocity (see for instance [12]). This latter says that if μ, ν are odd and congruent to 1 mod $(2 + 2i)$ — which can always be achieved by multiplication by a unit — then

$$\left(\frac{\mu}{\nu}\right)_4 = \pm\left(\frac{\nu}{\mu}\right)_4$$

where the sign is negative if both μ and ν are congruent to $3 + 2i$ mod 4 and positive otherwise.

Return now to the curve (2. 4), and assume for convenience that $p \nmid 2D$. For $p \equiv 3 \pmod 4$ we have simply $N_p = p + 1$. If $p \equiv 1 \pmod 4$ we can factorize it in Gaussian integers

$$p = \pi\bar{\pi} \text{ with } \pi \equiv 1 \pmod{2 + 2i};$$

then (see [8], [22]) we have

$$N_p = p + 1 - \bar{\pi}\left(\frac{D}{\pi}\right)_4 - \pi\left(\frac{D}{\bar{\pi}}\right)_4. \tag{2.5}$$

Putting these results together we obtain

$$\begin{aligned} L_D(s) &= \prod_{p \equiv 3(4)} (1 + p^{1-2s})^{-1} \prod_{p \equiv 1(4)} \left\{1 - \bar{\pi}\left(\frac{D}{\pi}\right)_4 p^{-s} - \pi\left(\frac{D}{\bar{\pi}}\right)_4 p^{-s} + p^{1-2s}\right\}^{-1} \\ &= \prod_{\pi \equiv 1(2+2i)} \left\{1 - \left(\frac{D}{\pi}\right)_4 \frac{\bar{\pi}}{(N\pi)^s}\right\}^{-1}, \end{aligned} \tag{2.6}$$

where the product is taken over all relevant primes, real or complex, in the Gaussian field $Q(i)$. Note that $L_D(s)$ differs rather trivially from $L_\Gamma(s)$ in that it does not contain factors corresponding to the primes which divide $2D$. Hence finally

$$L_D(s) = \sum_{\sigma \equiv 1(2+2i)} \left(\frac{D}{\sigma}\right)_4 \frac{\bar{\sigma}}{(N\sigma)^s}, \tag{2.7}$$

which is an orthodox Hecke L-series with Größencharakter (see [15]).

Over the rational field, the curve Γ_D is 2-isogenous to

$$\Gamma_{-4D}\colon\ y^2 z = x^3 + 4Dxz^2,$$

the isogeny arising from the rational 2-division point $(0, 0, 1)$ on Γ. It follows that the two curves have the same value of g, the number of generators of infinite order of $\mathcal{A}$; and since $-4 = (1 + i)^4$ they have the same N_p, zeta-functions and L-series. However they need not have the same Tate-Šafarevič group; for examples see [2], § 4.

Even though Γ_D is defined over the rational field Q, from certain points of view its natural field of definition is the Gaussian field $Q(i)$. This is the least field over which the complex multiplication on Γ_D is defined; and it is the field of definition of the quartic residue symbol. Over $Q(i)$, Γ_D is birationally equivalent to Γ_{-4D} instead of merely isogenous. Suppose that $\mathcal{A}_i$ is the group of points on Γ_D defined over $Q(i)$, where we still assume D to be rational. In virtue of the complex multiplication on Γ_D, we can regard $\mathcal{A}_i$ as a $Z(i)$-module; and it then has as many generators of infinite order as does $\mathcal{A}$ regarded as a Z-module. We prove no relations between the various Tate-Šafarevič groups involved, though some are implicit in our conjectures; clearly the Tate-Šafarevič groups of Γ_D and Γ_{-4D} can only differ in their 2-components.

It remains to consider the zeta-function of Γ over $Q(i)$; and here it costs nothing to take D to be a Gaussian integer. If $p \equiv 3 \pmod 4$ is a rational prime then

$$N_p = p^2 + 1 + p\left(\frac{D}{p}\right)_4 + p\left(\frac{\bar{D}}{p}\right)_4;$$

if $\pi \equiv 1 \pmod{2 + 2i}$ is a complex prime then

$$N_\pi = \pi\bar{\pi} + 1 - \bar{\pi}\left(\frac{D}{\pi}\right)_4 - \pi\left(\frac{\bar{D}}{\bar{\pi}}\right)_4.$$

Arguing in much the same way as before, we find

$$\zeta_{\Gamma, Q(i)}(s) = \frac{\zeta_{Q(i)}(s)\,\zeta_{Q(i)}(s-1)}{L_D(s)\,L_{\bar{D}}(s)}$$

where $\zeta_{Q(i)}(s)$ is the zeta-function of the field $Q(i)$ and $L_D(s)$ is still defined by (2.7). Thus in particular, when D is a rational integer $\zeta_{\Gamma, Q(i)}(s)$ can easily be written in terms of $\zeta_\Gamma(s)$ and of well-known functions not involving Γ.

§ 3. Formulae for $L_D(1)$

We have now to derive from (2. 7) an expression for $L_D(s)$ which can be analytically continued as far as $s = 1$ and is such that $L_D(1)$ can be written in finite form. Since the extra generality costs us nothing, we shall assume only that D is a Gaussian integer; however, the important case is when D is rational. We may also assume that D is fourth-power free; for multiplying D by a fourth power only changes finitely many factors in (2. 6), and changes those in an obvious way.

We write $D = EF$, where $E \equiv 1 \bmod (2 + 2i)$ and F is the product of a power of $1 + i$ and a unit; and we define Δ to be the product of the distinct primes dividing E, normalized so that $\Delta \equiv 1 \bmod (2 + 2i)$. If D is real, so are E, F and Δ. For convenience we also write $\varepsilon = (-1/E)_4$, so that $\varepsilon = +1$ if $E \equiv 1 \bmod 4$ and $\varepsilon = -1$ if $E \equiv 3 + 2i \bmod 4$. Remembering that $\sigma \equiv 1 \bmod (2 + 2i)$ where σ is the variable of summation in (2. 7), and using the law of quartic reciprocity, we have

$$\left(\frac{D}{\sigma}\right)_4 = \left(\frac{E}{\sigma}\right)_4 \left(\frac{F}{\sigma}\right)_4 = \left(\frac{\sigma}{E}\right)_4 \left(\frac{\varepsilon F}{\sigma}\right)_4. \tag{3. 1}$$

Here the first factor on the right only depends on the residue class of σ modulo Δ, and the second factor on the class of σ modulo 16. Let K be such that $(2 + 2i) \mid K$, that $K \mid 16$ and that $(\varepsilon F/\sigma)_4$ depends only on the residue class of σ modulo K. (We could take $K = 16$ always, but a smaller value of K reduces the complexity of some of the later formulae and so also the time taken in computation. We may for instance take $K = 8$ if F is real, and $K = 4$ if $F = \pm 1$.)

Now let B be a set of representatives for the residue classes modulo Δ, and let C be a set of representatives for those residue classes mod K which are congruent to 1 mod $(2 + 2i)$. We can write

$$\sigma = K\Delta\mu + K\beta + \Delta\gamma$$

where μ is a Gaussian integer, $\beta \in B$ and $\gamma \in C$; and we can replace any sum over σ by a triple sum over μ, β and γ. For convenience we write $\varrho = K\beta + \Delta\gamma$. It follows that we can rewrite (2. 7) in the form

$$L_D(s) = \sum_{\beta,\gamma} \left(\frac{D}{\varrho}\right)_4 \sum_{\mu} \frac{\bar{K}\bar{\Delta}\bar{\mu} + \bar{\varrho}}{\{N(K\Delta\mu + \varrho)\}^s} \tag{3. 2}$$

in which provided $E \neq 1$ we have

$$\left(\frac{D}{\varrho}\right)_4 = \left(\frac{K}{E}\right)_4 \left(\frac{\varepsilon F}{\Delta}\right)_4 \left(\frac{\beta}{E}\right)_4 \left(\frac{\varepsilon F}{\gamma}\right)_4. \tag{3. 3}$$

We have next to find a more convenient expression for the inner sum in (3. 2). For α not a Gaussian integer, we write

$$\psi(\alpha, s) = \frac{\bar{\alpha}}{|\alpha|^{2s}} + \sum_{\mu \neq 0} \left\{ \frac{\bar{\alpha} + \bar{\mu}}{|\alpha + \mu|^{2s}} - \frac{\bar{\mu}}{|\mu|^{2s}} \left(1 - \frac{s\alpha}{\mu} + \frac{\bar{\alpha}(1 - s)}{\bar{\mu}}\right)\right\}. \tag{3. 4}$$

Since the expression in curly brackets is $O(\mu^{-2s-1})$, this defines an analytic function of s in $R(s) > \frac{1}{2}$; and since the series 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 $1, i$. On the other hand, if $R(s)$ is large we can rearrange the terms in (3. 4) to give

$$\sum_{\mu} \frac{\bar{\alpha}+\bar{\mu}}{|\alpha+\mu|^{2s}} = \psi(\alpha, s) + \bar{\alpha}(1-s) \sum_{\mu \neq 0} \frac{1}{(N\mu)^s}$$
$$= \psi(\alpha, s) + 4\bar{\alpha}(1-s)\, \zeta_{Q(i)}(s);$$

for the other sums vanish on combining the terms arising from $\pm\mu$, $\pm i\mu$. This provides an analytic continuation of the left hand side. Substituting into (3. 2) we obtain

$$L_D(s) = \frac{\bar{K}\bar{\Delta}}{\{N(K\Delta)\}^s}\left\{\sum_{\beta,\gamma}\left(\frac{D}{\varrho}\right)_4 \psi\left(\frac{\varrho}{K\Delta}, s\right) + 4(1-s)\,\zeta_{Q(i)}(s) \sum_{\beta,\gamma} \frac{\bar{\varrho}}{\bar{K}\bar{\Delta}}\left(\frac{D}{\varrho}\right)_4\right\}.$$

In particular, since $(s-1)\,\zeta_{Q(i)}(s) \to \frac{1}{4}\pi$ as $s \to 1$, we have

$$L_D(1) = \frac{1}{K\Delta} \sum \left(\frac{D}{\varrho}\right)_4 \xi\left(\frac{\varrho}{K\Delta}\right) - \frac{\pi}{N(K\Delta)} \sum \bar{\varrho}\left(\frac{D}{\varrho}\right)_4. \tag{3. 5}$$

Since this expression does not depend on the particular choice of representatives ϱ of the residue classes mod $K\Delta$, we see that

$$\xi(u+1) = \xi(u) + \pi, \quad \xi(u+i) = \xi(u) - \pi i.$$

In particular, since ξ is odd it follows that

$$\xi\left(\frac{1}{2}\right) = \frac{1}{2}\pi, \quad \xi\left(\frac{1}{2}i\right) = -\frac{1}{2}\pi i. \tag{3. 6}$$

Provided that $E \neq 1$, we can express the right hand side of (3. 5) in terms of the Weierstrass $\wp$-function. In order to simplify the algebra later, it is convenient to make a change of period. Throughout this paper, we shall therefore denote by $\wp(u)$ the Weierstrass $\wp$-function with periods $\omega, i\omega$, where

$$\omega = 2^{\frac{1}{2}} \pi e^{-\frac{\pi}{6}} \prod (1 - e^{-2\pi n})^2 = 2.6220575\ldots$$

has been chosen so that $\wp(u)$ satisfies the equation

$$\wp'^2 = 4\wp^3 - 4\wp. \tag{3. 7}$$

The Weierstrass $\wp$-function with periods $1, i$ is therefore $\omega^2\wp(\omega u)$; and (see [25]) we can write the addition formula for $\xi(u)$ in the form

$$\xi(u+v) = \xi(u) + \xi(v) + \omega \cdot \frac{\wp'(\omega u) - \wp'(\omega v)}{2\{\wp(\omega u) - \wp(\omega v)\}}. \tag{3. 8}$$

In this we write $u = \gamma/K$, $v = \beta/k$, giving an expression for $\xi(\varrho/K\Delta)$ in terms of functions with simpler arguments. If we substitute the resulting values in (3. 5) and add to this the equation derived by writing $-\beta$ for β throughout, many of the terms cancel. In view of the shape of (3. 3), we split cases on the value of $\varepsilon = (-1/E)_4$.

If $\varepsilon = +1$, then $(D/\varrho)_4$ is not affected by replacing β by $-\beta$ and so we obtain

$$L_D(1) = \frac{1}{K\Delta} \sum_{\beta,\gamma}\left(\frac{D}{\varrho}\right)_4 \left\{\xi\left(\frac{\gamma}{K}\right) - \frac{\pi\bar{\gamma}}{\bar{K}}\right\} + \frac{\omega}{2K\Delta} \sum_{\beta,\gamma}\left(\frac{D}{\varrho}\right)_4 \frac{\wp'(\gamma\omega/K)}{\wp(\gamma\omega/K) - \wp(\beta\omega/\Delta)}.$$

In the first term on the right, the sum over β is effectively $\sum(\beta/E)_4 = 0$, since E is not a fourth power; hence this term vanishes and we have

$$L_D(1) = \frac{\omega}{2K\Delta} \sum_{\beta,\gamma} \left(\frac{D}{\varrho}\right)_4 \frac{\wp'(\gamma\omega/K)}{\wp(\gamma\omega/K) - \wp(\beta\omega/\Delta)}. \tag{3.9}$$

If $\varepsilon = -1$, replacing β by $-\beta$ changes the sign of $(D/\varrho)_4$ and we therefore obtain

$$L_D(1) = \frac{1}{K\Delta} \sum_{\beta,\gamma} \left(\frac{D}{\varrho}\right)_4 \left\{\xi\left(\frac{\beta}{\Delta}\right) - \frac{\pi\bar{\beta}}{\bar{\Delta}}\right\} - \frac{\omega}{2k\Delta} \sum_{\beta,\gamma} \left(\frac{D}{\varrho}\right)_4 \frac{\wp'(\beta\omega/\Delta)}{\wp(\gamma\omega/K) - \wp(\beta\omega/\Delta)}. \tag{3.10}$$

(Here the terms for which $\beta \mid \Delta$ are defined to be zero.) If εF is not an exact fourth power, then the sum over γ in the first term on the right is effectively $\sum(\varepsilon F/\gamma)_4 = 0$; hence this term vanishes. If εF is an exact fourth power, the first term on the right of (3. 10) is

$$\frac{\bar{K}}{8\Delta} \sum_{\beta} \left(\frac{\beta k}{E}\right)_4 \left\{\xi\left(\frac{\beta}{\Delta}\right) - \frac{\pi\bar{\beta}}{\bar{\Delta}}\right\} \tag{3.11}$$

since there are $\frac{1}{8} K\bar{K}$ values of γ to sum over. Writing $i\beta$ for β and adding, we see that (3. 11) vanishes if $(i/E)_4 = -i$. If $(i/E)_4 = i$ we can evaluate (3. 11) by writing $(1 + i)\beta$ for β and using

$$\xi(u(1+i)) = (1-i)\,\xi(u) + \frac{\omega(1+i)}{4} \frac{\wp'(\omega u)}{\wp(\omega u)}, \tag{3.12}$$

which is a special case of (3. 8). We find that (3. 11) is equal to

$$\frac{\bar{K}\omega}{16\Delta} \left\{1 - i + 2i\left(\frac{1+i}{E}\right)_4\right\}^{-1} \sum_{\beta} \left(\frac{\beta K(1+i)}{E}\right)_4 \frac{\wp'(\beta\omega/\Delta)}{\wp(\beta\omega/\Delta)}.$$

In the excluded cases when $E = 1$, we can evaluate $L_D(1)$ directly from (3. 5); for the values of $\xi(u)$ needed can be obtained from (3. 6) and (3. 12).

For explicit numerical calculation on an electronic computer, it is expedient to carry out the summation over γ algebraically. We assume that D is a rational integer, so that we have $\varepsilon = +1$, and that D is not divisible by a fourth power nor, since $L_{4D}(1) = L_{-D}(1)$, by 4. There are therefore four cases to consider. In each of them we write for convenience $\wp$ for $\wp(\beta\omega/\Delta)$. The sums concerned are taken over all $\beta \in B$; but it is enough to consider the β prime to Δ since the terms with β not prime to Δ each vanish.

Case 1: $D \equiv 1 \bmod 4$. Now we have $E = D$, $F = 1$. If we choose $K = 4$ we obtain for $D \neq 1$,

$$L_D(1) = \frac{\omega}{\Delta} \sum \left(\frac{\beta}{D}\right)_4 \frac{\wp}{\wp^2 - 2\wp - 1}. \tag{3.13}$$

Alternatively, we may take $K = 2 + 2i$ and obtain, still for $D \neq 1$,

$$L_D(1) = \frac{i\omega}{2\Delta} \sum \left(\frac{\beta(2+2i)}{D}\right)_4 \frac{1}{\wp - i}. \tag{3.14}$$

For the excluded value $D = 1$ we find $L_1(1) = \frac{1}{4}\omega$.

Case 2: $D \equiv 3 \bmod 4$. Now we have $E = -D$, $F = -1$, $K = 4$ and obtain for $D \neq -1$

$$L_D(1) = \frac{\omega}{\Delta\sqrt{2}} \Sigma\left(\frac{\beta}{-D}\right)_4 \frac{\wp+1}{\wp^2-2\wp-1}. \tag{3.15}$$

For the excluded case $D = -1$ we find $L_{-1}(1) = \frac{1}{4}\omega\sqrt{2}$.

Case 3: $D \equiv 2 \bmod 8$. Now we have $E = \frac{1}{2}D$, $F = 2$, $K = 8$ and obtain for $D \neq 2$

$$L_D(1) = \frac{\omega\sqrt[4]{8}}{\Delta} \Sigma\left(\frac{\beta}{E}\right)_4 \frac{2\wp(\wp^4-1)(\wp^2+2\wp-1)}{(\wp^2-2\wp-1)^4-32\wp^2(\wp^2-1)^2}. \tag{3.16}$$

For the excluded case $D = 2$ we find $L_2(1) = 0$.

Case 4: $D \equiv 6 \bmod 8$. Now we have $E = -\frac{1}{2}D$, $F = 2$, $K = 8$ and obtain for $D \neq -2$

$$L_D(1) = \frac{\omega\sqrt[4]{2}}{\Delta} \Sigma\left(\frac{\beta}{E}\right)_4 \frac{(\wp-1)\{2(\wp^2+1)^3+(\wp^2+2\wp-1)^3\}}{(\wp^2-2\wp-1)^4-32\wp^2(\wp^2-1)^2}. \tag{3.17}$$

For the excluded case $D = -2$ we find $L_{-2}(1) = \frac{1}{2}\omega\sqrt[4]{2}$.

§ 4. Proof of integrity

It is well known [21] that the division values of $\wp$ and $\wp'$ are in general algebraic functions of g_2 and g_3, and so in our particular case algebraic numbers. It follows from the results of § 3 that $\omega^{-1}L_D(1)$ is an algebraic number; in this section we consider how nearly it is a rational integer. We deal only with the case when D is rational: but similar arguments could be used in the Gaussian case. Our object is to prove

Theorem 1. *Let $D > 1$ be a positive integer, fourth power free and not divisible by 4. Then*

$$\frac{D^{\frac{1}{4}}L_D(1)}{\omega} \quad \text{and} \quad \frac{(4D)^{\frac{1}{4}}L_{-D}(1)}{\omega}$$

are rational integers.

The theorem holds for $D = 2$, from the explicit values given at the end of § 3. Setting aside this case, we may therefore make use of (3. 9) and its consequences (3. 13) to (3. 17). The proof of the theorem now falls into two parts. The first part (Lemmas 1—5) is concerned with integrity and is entirely elementary; the second is concerned with rationality and makes use of results from classical class field theory.

For convenience, in dealing with algebraic integers, we shall use 'odd' to mean prime to 2, and 'even' to mean not odd.

Lemma 1. *Let α be an odd Gaussian integer. Then*

$$\wp(\alpha u) = P_\alpha(\wp(u))/Q_\alpha^2(\wp(u)),$$

where P_α, Q_α are polynomials of degrees $\alpha\bar{\alpha}$, $\frac{1}{2}(\alpha\bar{\alpha}-1)$ respectively with Gaussian integer coefficients; P_α has leading coefficient 1 and Q_α has leading coefficient α and constant term ± 1 or $\pm i$.

We know that $\wp(\alpha u)$ is an even doubly-periodic function whose only singularities in the period parallelogram are $\alpha\bar{\alpha}$ double poles at the α-division points. These include the origin but none of the midpoints. It follows, by well-known results on doubly-periodic functions, that we have

$$\wp(\alpha u) = P_\alpha(\wp(u))/Q_\alpha^2(\wp(u)),$$

where P_α, Q_α are polynomials of degrees $\alpha\bar{\alpha}$, $\frac{1}{2}(\alpha\bar{\alpha}-1)$ respectively. Moreover, the zeros of Q_α are just the distinct finite values of $\wp(u)$ at the α-division points, while the zeros of P_α are the values of $\wp(u)$ at those $(1+i)$ α-division points that are not α-division points, taken with their correct multiplicity.

We now normalize so that Q_α has leading coefficient α. Since for small u we have

$$\wp(u) \sim u^{-2}, \quad \wp(\alpha u) \sim \alpha^{-2}u^{-2},$$

it follows that P_α has leading coefficient 1. We shall prove the remaining statements in the lemma by induction on the value of $\alpha\bar{\alpha}$, since they obviously hold when α is a unit. In the identity

$$\wp(v+w)\,\wp(v-w) = \left\{\frac{\wp(v)\,\wp(w)+1}{\wp(v)-\wp(w)}\right\}^2 \tag{4.1}$$

we write $v = \alpha u$, $w = (1+i)u$. Since

$$\wp(u(1+i)) = \frac{\wp^2(u)-1}{2i\wp(u)} \tag{4.2}$$

we deduce

$$\frac{P_{\alpha+1+i}\,P_{\alpha-1-i}}{Q^2_{\alpha+1+i}Q^2_{\alpha-1-i}} = \left\{\frac{(\wp^2-1)\,P_\alpha + 2i\wp Q_\alpha^2}{(\wp^2-1)\,Q_\alpha^2 - 2i\wp\,P_\alpha}\right\}^2.$$

Here the left hand side is in its lowest terms; for from the results above no P can have a zero in common with a Q. But the numerator and denominator on the right have (after squaring) the same degrees and leading coefficients as those on the left. Hence they are equal, giving

$$P_{\alpha+1+i}P_{\alpha-1-i} = \{(\wp^2-1)\,P_\alpha + 2i\wp Q_\alpha^2\}^2,$$
$$Q_{\alpha+1+i}Q_{\alpha-1-i} = (\wp^2-1)\,Q_\alpha^2 - 2i\wp\,P_\alpha.$$

We have also the similar results obtained by writing $-i$ for i. Now therefore, if $\eta = 1$, -1, i or $-i$ and if the assertions of the lemma hold for $\alpha - \eta(1+i)$ and for $\alpha - 2\eta(1+i)$, then they hold for α. But it is geometrically obvious that if α is an odd integer not a unit then we can always choose η so that both $\alpha - \eta(1+i)$ and $\alpha - 2\eta(1+i)$ are strictly smaller than α. The truth of the lemma now follows by induction.

Lemma 2. *Let Δ be an odd square-free Gaussian integer, not a unit; and let β be a Gaussian integer prime to Δ. Let*

$$\varphi(\Delta) = \begin{cases} \Delta^{2/(\Delta\bar{\Delta}-1)} & \text{if } \Delta \text{ is prime,} \\ 1 & \text{otherwise.} \end{cases}$$

Then $\varphi(\Delta)\,\wp(\beta\omega/\Delta)$ is an algebraic unit.

Suppose first that Δ is prime. Then the $\wp(\beta\omega/\Delta)$ are just the roots of $Q_\Delta(x) = 0$. Moreover they all generate the same field K over $Q(i)$; for given any β_1, β_2 prime to Δ we can find an odd α such that $\beta_2 \equiv \alpha\beta_1 \bmod \Delta$, and so

$$\wp(\beta_2\omega/\Delta) = \wp(\alpha\beta_1\omega/\Delta)$$

is a rational function of $\wp(\beta_1\omega/\Delta)$ over $Q(i)$, by Lemma 1. Since they are the roots of $Q_\Delta(x) = 0$, the $\wp(\beta\omega/\Delta)$ each have numerator a unit and denominator a factor of Δ; and not all of them are integers. Let $\mathfrak{q}$ be a prime ideal in K which divides the denominator of $\wp(\beta_1\omega/\Delta)$ to exactly the r^{th} power, where $r > 0$. For any β_2 prime to Δ we define α as before. Then α is prime to $\mathfrak{q}$ and hence, using Lemma 1 again, $\mathfrak{q}$ divides the denominator of

$$\wp(\beta_2\omega/\Delta) = P_\alpha(\wp(\beta_1\omega/\Delta))/Q_\alpha^2(\wp((\beta_1\omega/\Delta))$$

to exactly the r^{th} power. It follows that all the $\wp(\beta\omega/\Delta)$ must have the same denominator, up to a unit; and hence this must be $\varphi(\Delta)$, for there are $\frac{1}{2}(\Delta\bar{\Delta} - 1)$ such denominators and their product is Δ.

Now suppose that $\Delta = \Delta_1\Delta_2$, where Δ_1 and Δ_2 are coprime and not units. Then $\wp(\beta\omega/\Delta)$ is a zero of $Q_\Delta/Q_{\Delta_1}Q_{\Delta_2}$, which has integer coefficients the first and last of which are units. Hence $\wp(\beta\omega/\Delta)$ is itself a unit. This completes the proof of the lemma.

Lemma 3. *Let γ_1, γ_2 be odd Gaussian integers, γ_2 being square-free, and let $r > 1$ be a rational integer. Then $\wp(\gamma_1\omega/\gamma_2(1+i)^r)$ is an algebraic unit.*

Without loss of generality, we may assume γ_1, γ_2 coprime. We first prove that $\wp(\gamma_1\omega/\gamma_2(1+i))$ is an algebraic integer. If γ_2 is a unit, then

$$\wp(\gamma_1\omega/\gamma_2(1+i)) = \wp(\omega/(1+i)) = 0.$$

If not, we have

$$\wp(u)\,\wp(u + \omega/(1+i)) = -1 \tag{4.3}$$

since, after (4. 2), the roots of

$$x^2 - 2ix\wp(u(1+i)) - 1 = 0 \tag{4.4}$$

are $\wp(u)$ and $\wp(u + \omega/(1+i))$. But if we write $u = \gamma_1\omega/\gamma_2(1+i)$ then

$$u + \frac{\omega}{1+i} = \frac{\omega(\gamma_1+\gamma_2)}{\gamma_2(1+i)}$$

is an argument to which we can apply Lemma 2, with γ_2 for Δ. This and (4. 3) show that $\wp(\gamma_1\omega/\gamma_2(1+i))$ is $\varphi(\gamma_2)$ times an algebraic unit, and is therefore an algebraic integer.

The lemma now follows by induction on r; for since $\wp(u)$ is a root of (4. 4) we see that $\wp(u)$ is an algebraic unit whenever $\wp(u(1+i))$ is an algebraic integer.

Lemma 4. *Let $r > 0$ be a rational integer; and let β, γ, Δ be Gaussian integers of which Δ is odd, square-free and not a unit, β is prime to Δ and γ is odd. Write $\lambda = 1 - 2^{1-r}$, and define $\varphi(\Delta)$ as in Lemma 2. Then*

$$2^{-\lambda}\varphi(\Delta)\{\wp(\beta\omega/\Delta) - \wp(\gamma\omega/(1+i)^r)\}$$

is an algebraic unit.

For $r = 1$ we have $\lambda = 0$, $\wp(\gamma\omega/(1+i)) = 0$, and the result is precisely that of Lemma 2. We now proceed by induction on r. From (4. 2) we have

$$\wp(v(1+i)) - \wp(w(1+i)) = \frac{-i\{\wp(v) - \wp(w)\}\{\wp(v)\,\wp(w) + 1\}}{2\wp(v)\,\wp(w)}. \tag{4.5}$$

In this we write $v = \beta\omega/\Delta$, $w = \gamma\omega/(1+i)^r$, and assume the Lemma true for $r-1$. Write for convenience ϑ for an arbitrary algebraic unit, not necessarily the same from one occurrence to the next. By the induction hypothesis we have

$$\wp(v(1+i)) - \wp(w(1+i)) = 2^{2\lambda-1}\vartheta/\varphi(\Delta).$$

By Lemma 3 with $\gamma_2 = 1$ and Lemma 2 we have

$$2\wp(v)\,\wp(w) = 2\vartheta/\varphi(\Delta).$$

By (4. 1) and Lemma 3 with $\gamma_2 = \Delta$ we have

$$\wp(v)\,\wp(w) + 1 = \vartheta\{\wp(v) - \wp(w)\}.$$

Combining these three results with (4. 5) we obtain

$$\{\wp(v) - \wp(w)\}^2 = 2^{2\lambda}\vartheta/\varphi^2(\Delta),$$

and this proves the lemma.

Lemma 5. *Let D be a rational integer, fourth power free and not divisible by 4. If $D \neq \pm 1$ then $2^{\frac{3}{4}}\Delta\omega^{-1}L_D(1)$ is an algebraic integer.*

Here Δ is defined as in § 3. From the actual values of $L_D(1)$ we verify that the Lemma is true for $D = \pm 2$; thus we need only deal with the cases in which one of (3. 13) to (3. 17) hold. As in the proof of Lemma 4 we shall write ϑ for an algebraic unit, which need not be the same from one occurrence to the next. Now, using Lemma 4,

$$\wp^2 - 2\wp - 1 = \left\{\wp - \wp\left(\frac{1}{4}\omega\right)\right\}\left\{\wp - \wp\left(\frac{3}{4}\omega + \frac{1}{2}i\omega\right)\right\} = 2^{\frac{7}{4}}\vartheta/\varphi^2(\Delta)$$

and

$$\wp + 1 = \wp - \wp\left(\frac{1}{2}i\omega\right) = 2^{\frac{1}{2}}\vartheta/\varphi(\Delta).$$

Hence each term on the right of (3. 13) or (3. 15) is of the form $\omega\vartheta\varphi(\Delta)/2^{\frac{7}{4}}\Delta$. But in each of these sums the terms given by β and by $-\beta$ are equal. Hence the right hand sides are $\omega\varphi(\Delta)/2^{\frac{3}{4}}\Delta$ times algebraic integers, and since $\varphi(\Delta)$ is an algebraic integer this proves the lemma in these two cases.

In the cases given by (3. 16) and (3. 17) we argue similarly, using in addition the facts that

$$(\wp^2 - 2\wp - 1)^4 - 32\wp^2(\wp^2 - 1)^2 = 2^{\frac{31}{4}}\vartheta/\varphi^8(\Delta)$$

since the left hand side is the product of eight terms of the form

$$\left\{\wp - \wp\left(\frac{1}{8}\gamma\omega\right)\right\} \text{ with } \gamma \text{ odd};$$

that

$$\wp^2 - 1 = 2\vartheta/\varphi^2(\Delta),$$
$$\wp^2 + 1 = 2^{\frac{3}{2}}\vartheta/\varphi^2(\Delta),$$
$$\wp - 1 = 2^{\frac{1}{2}}\vartheta/\varphi(\Delta)$$

and

$$\wp^2 + 2\wp - 1 = 2^{\frac{7}{4}}\vartheta/\varphi^2(\Delta),$$

all similarly derived from Lemma 4. The rest of the proof goes through exactly as before.

Lemma 5 is the strongest result which we can obtain from elementary divisibility arguments. We now turn to the question of rationality. Here we need to quote classical results of class field theory over $Q(i)$. The relevant part of the Kronecker Jugendtraum (see Fueter [11] or Hasse [13]) is normally stated as follows:

Lemma 6. *Let μ be a Gaussian integer, not a unit. Then the strahlklass field mod μ over $Q(i)$ is generated by $\wp^2(\alpha\omega/\mu)$, where α is any Gaussian integer prime to μ. If this field is K, and if p is any Gaussian prime not dividing μ, then the Artin symbol $\left(\frac{K/Q(i)}{p}\right)$ is the automorphism which takes $\wp^2(\alpha\omega/\mu)$ into $\wp^2(\alpha p\omega/\mu)$.*

The fact that p is only defined up to a power of i is irrelevant; for the value of $\wp^2$ is not changed by multiplying its argument by a power of i. Unfortunately Lemma 6 is not in the most convenient form for us, since it deals with $\wp^2$ rather than with $\wp$. We therefore rephrase the relevant special case of it as follows:

Lemma 7. *Let Δ be an odd square-free Gaussian integer, not a unit. Then the strahlklass field* mod 2Δ *over $Q(i)$ is generated by $\wp(\alpha\omega/\Delta)$ where α is any Gaussian integer prime to Δ. If this field is K, and if p is any Gaussian prime not dividing 2Δ, normalized so that $p \equiv 1 \bmod 2$, then the Artin symbol $\left(\frac{K/Q(i)}{p}\right)$ is the automorphism which takes $\wp(\alpha\omega/\Delta)$ into $\wp(\alpha p\omega/\Delta)$.*

Let K be the strahlklass field mod 2Δ over $Q(i)$. Since

$$\wp\left(\frac{\omega(2\alpha+\Delta)}{2\Delta}\right) = \frac{\wp(\alpha\omega/\Delta)+1}{\wp(\alpha\omega/\Delta)-1},$$

the field generated by $\wp(\alpha\omega/\Delta)$ over $Q(i)$ contains $\wp^2(\beta\omega/2\Delta)$ for some β prime to 2Δ, and so contains K.

To deduce Lemma 7 from Lemma 6, we have still to show that $\wp(\alpha\omega/\Delta)$ is in K and is correctly transformed by the Artin symbol. Since we can alter α by a multiple of Δ, we may assume that $\alpha \equiv \Delta \bmod 2$. We shall now prove — which is clearly sufficient for our needs — that $\wp(\alpha\omega/\Delta)$ can be written as a rational function of $\wp^2(\alpha\omega/2\Delta)$, the function being defined over $Q(i)$ and being independent of α.

For any Gaussian integer ν, $\wp(\nu u)$ is a rational function of $\wp(u)$ defined over $Q(i)$; this follows from (4. 2) and Lemma 1. Moreover, it is an odd function; for writing iu for u changes the signs of both $\wp(u)$ and $\wp(\nu u)$. Hence $\wp^2(\nu u)$ is a rational function of $\wp^2(u)$, defined over $Q(i)$. Let $\gamma = \frac{1}{2}(\alpha - \Delta)$ and choose ν so that $2 \nmid \nu$ and $\Delta \mid (\nu - 1)$. Then $\wp^2(\gamma\omega/\Delta) = \wp^2(\nu\alpha\omega/2\Delta)$ is a rational function of $\wp^2(\alpha\omega/2\Delta)$, defined over $Q(i)$ and independent of α. Moreover

$$\wp(\alpha\omega/\Delta) = \frac{2\{\wp^2(\alpha\omega/2\Delta)+1\}\{\wp^2(\gamma\omega/\Delta)+1\}}{\{\wp^2(\alpha\omega/2\Delta)-1\}\{\wp^2(\gamma\omega/\Delta)-1\}}.$$

Combining these results, we see that $\wp(\alpha\omega/\Delta)$ can be written as a rational function of $\wp^2(\alpha\omega/2\Delta)$ defined over $Q(i)$ and independent of α (since ν is so). This completes the deduction of Lemma 7.

Corollary. *Let $R(x)$ be a rational function of x defined over $Q(i)$, and let D be a rational integer. Then with the notation of* § 3,

$$E^{\frac{1}{4}} \sum \left(\frac{\beta}{E}\right)_4 R(\wp(\beta\omega/\Delta)) \tag{4. 6}$$

is in $Q(i)$.

For let K be defined as in the proof of the Lemma. Then $E^{\frac{1}{4}}$ is in K; for if p prime to $2E$ is a Gaussian prime it splits in $Q(i, E^{\frac{1}{4}})/Q(i)$ if and only if $(E/p)_4 = 1$; and this depends only on the residue class of p modulo 2Δ, by the quartic reciprocity law and the rationality of E. Moreover, the general automorphism of $K/Q(i)$ is that which takes $\wp(\alpha\omega/\Delta)$ into $\wp(\lambda\alpha\omega/\Delta)$ for each α, where λ is prime to Δ and $\lambda \equiv 1 \bmod 2$. By the identification of the Artin symbol in Lemma 7, this also takes $E^{\frac{1}{4}}$ into $(\lambda/E)_4 E^{\frac{1}{4}}$, and hence merely permutes the terms of (4. 6). Thus this expression, being unchanged by each automorphism of $K/Q(i)$, must be in $Q(i)$; and this proves the Corollary.

We can now return to the proof of Theorem 1. Let D be a rational integer, fourth power free and not divisible by 4, but not necessarily positive, and suppose $|D| > 2$. Then one of (3. 13), (3. 15), (3. 16) or (3. 17) is valid. It follows that $L_D(1)$ is real; for the set B over which the sum is taken may be made to consist of real numbers and complex conjugate pairs. Moreover $D^{\frac{1}{4}}\omega^{-1}L_D(1)$ is in $Q(i)$, by the Corollary to Lemma 7. Since $-4 = (1+i)^4$, it follows that the two expressions in the Theorem are rational numbers. But by Lemma 5 they are algebraic numbers whose denominator is at most $(2\Delta)^{\frac{3}{4}}$. Since the only rational integers which divide this are ± 1, it follows that the expressions in Theorem 1 are rational integers. This proves the Theorem.

§ 5. Estimation of g

In order to produce Table 1 below, we need also a method of estimating g, the number of independent generators of infinite order of $\mathcal{A}$, the group of rational points on Γ_D. We cannot do this by the methods of our previous paper, since they would be intolerably slow when D is large. Instead, we use the fact that multiplication by 2 can be written as a product of isogenies. The arguments involved are well known, though we cannot find them explicitly in the literature (compare the theses of Billing [1] and Lind [17]): we have stated them in unusually pompous form to be able to use the analogy with the work of Cassels [5].

We extend the definition of ν-covering to the case where ν: $C_1 \to C$ is an isogeny of elliptic curves instead of an endomorphism. We assume that ν is defined over the rationals and is an n to 1 mapping; and we write $\mathfrak{o}$, $\mathfrak{o}_1$ for the zeros of C, C_1 considered as Abelian groups. There is an isogeny ν_1: $C \to C_1$ such that the composite maps $\nu\nu_1$ and $\nu_1\nu$ are multiplication by n on C, C_1 respectively; and ν_1 is also defined over the rationals. We say that there is a ν-covering of C if there is a curve $\mathcal{D}$ defined over the rationals and a commutative triangle

$$\begin{array}{ccc} C_1 & \longrightarrow & C \\ \updownarrow & \nearrow & \\ \mathcal{D} & & \end{array}$$

with associated generic points

$$\begin{array}{ccc} x_1 & \longrightarrow & x = \nu x_1 \\ \updownarrow & \nearrow & \\ X & & \end{array}$$

where $X \to x$ is over the rationals and $X \leftrightarrow x_1$ over the complex numbers. Another curve $\mathcal{D}'$ and its associated mappings give the same ν-covering if and only if there

is a birational mapping $X \leftrightarrow X'$ over the rationals and a point $\mathfrak{d}_1$ on C_1 with $\nu\mathfrak{d}_1 = \mathfrak{o}$ such that the diagram

$$\begin{array}{ccc} X & \longleftrightarrow & x_1 \\ \updownarrow & & \updownarrow \\ X' & \longleftrightarrow & x_1' = x_1 + \mathfrak{d}_1 \end{array} \tag{5. 1}$$

is commutative. There is a natural law of composition of ν-coverings inherited from the law of composition of homogeneous spaces over C_1; and under it they form an Abelian group. We are interested in two subgroups: G_ν, the group of those coverings for which $\mathcal{D}$ has a point in every p-adic field including the reals, and G'_ν, the group of those coverings for which $\mathcal{D}$ actually has a rational point. If $\mathcal{A}$, $\mathcal{A}_1$ are the groups of rational points on C, C_1 respectively, then G'_ν is isomorphic to $\mathcal{A}/\nu\mathcal{A}_1$.

For convenience of notation, when we use n as an endomorphism it will always refer to the map $C \to C$. Now we have $n = \nu_1\nu$ and so, using square brackets for the order of groups,

$$\begin{aligned} [\mathcal{A}/n\mathcal{A}] &= \frac{[\mathcal{A}/\nu\mathcal{A}_1]\,[\mathcal{A}_1/\nu_1\mathcal{A}]}{\text{Number of cosets of } \nu_1\mathcal{A} \text{ in } \mathcal{A}_1 \text{ which meet } \nu^{-1}\mathfrak{o}} \\ &= \frac{[G'_{\nu_1}]\,[G'_\nu]}{[\mathcal{A} \cap \nu_1^{-1}\mathfrak{o}_1]\,[\mathcal{A}_1 \cap \nu^{-1}\mathfrak{o}]/[\mathcal{A} \cap n^{-1}\mathfrak{o}]}. \end{aligned} \tag{5. 2}$$

Here the denominator only depends on the rational n-division points on C, and so can easily be calculated.

We can obtain this result, and somewhat more, by a different argument. Suppose that $\mathcal{D}$ represents an n-covering of C; then we can find $\mathcal{D}_1$ so that the extended diagram

$$\begin{array}{ccccc} C & \overset{\nu_1}{\dashrightarrow} & C_1 & \overset{\nu}{\dashrightarrow} & C \\ \updownarrow & & \updownarrow & \nearrow & \\ \mathcal{D} & \longrightarrow & \mathcal{D}_1 & & \end{array} \tag{5. 3}$$

is commutative. Here $\mathcal{D} \to \mathcal{D}_1$ and $\mathcal{D}_1 \to C$ are defined over the rationals, and $C_1 \leftrightarrow \mathcal{D}_1$ is over the complex numbers. For let X be a generic point on $\mathcal{D}$ and let $\varphi\colon \mathcal{D} \to C_1$ be the map (over the complex numbers) defined in the obvious way. The support of $\varphi^{-1}\{\varphi(X)\}$ is a divisor defined over $Q(X)$. Let its exact field of definition be $Q(X_1)$; then we may define $\mathcal{D}_1$ as the curve whose generic point is X_1, and now the assertions above are obvious.

The right-hand part of the last diagram provides a ν-covering of C; and it is easy to show that this depends only on the original n-covering and not on its realisation. Moreover, this process is compatible with the law of composition of coverings. Thus we have homomorphisms $G_n \to G_\nu$ and $G'_n \to G'_\nu$; and the second of these is onto since any $\mathcal{D}_1$ which contains a rational point can be lifted back to a $\mathcal{D}$.

We now find the kernels of these mappings. If $\mathcal{D}$ is in the kernel of $G_n \to G_\nu$, then we may take $\mathcal{D}_1$ in (5. 3) to be C_1 and the map $\mathcal{D}_1 \leftrightarrow C_1$ to be the identity. Thus any representation of an n-covering in $\mathrm{Ker}\,(G_n \to G_\nu)$ is a representation of a ν_1-covering in G_{ν_1}, and vice versa. Since the condition for two representations to give the same covering is stricter for ν_1-coverings than for n-coverings, there is a homomorphism $G_{\nu_1} \to G_n$ such that $G_{\nu_1} \to G_n \to G_\nu$ is exact.

It remains to find the kernel of $G_{\nu_1} \to G_n$. If a representation of the trivial n-covering of C is given by

$$\begin{array}{ccccc} C & \to & C_1 & \to & C \\ \uparrow & & & \nearrow & \\ \mathcal{D} & & & & \end{array}$$

then $\mathcal{D}$ contains a rational point and may therefore be taken to be a copy of C. Thus we get just n^2 effectively distinct representations, the birational maps $\mathcal{D} \leftrightarrow C$ being $x \leftrightarrow x + \mathfrak{d}$ for the n^2 distinct n-division points on C. A representation here gives rise to a representation of a ν_1-covering if and only if the map $\mathcal{D} \to C_1$ is defined over the rationals; that is, if $\nu_1 \mathfrak{d}$ is rational. Two of them give rise to the same ν_1-covering if and only if the difference of their $\mathfrak{d}$'s is the sum of a rational point and a ν_1-division point. Hence the order of the kernel is

$$\frac{[\mathcal{A}_1 \cap \nu^{-1}\mathfrak{o}]}{\text{number of cosets of } \nu_1^{-1}\mathfrak{o}_1 \text{ in } n^{-1}\mathfrak{o} \text{ which contain rational points}}.$$

This is clearly just the denominator of (5. 2), and so we have

$$[G_n] \leqq \frac{[G_\nu]\,[G_{\nu_1}]}{[\mathcal{A} \cap \nu_1^{-1}\mathfrak{o}_1]\,[\mathcal{A}_1 \cap \nu^{-1}\mathfrak{o}]/[\mathcal{A} \cap n^{-1}\mathfrak{o}]}. \tag{5. 4}$$

(The inequality sign here arises because the homomorphism $G_n \to G_\nu$ need not be onto.) Similar arguments work for the groups G'; and since $G'_n \to G'_\nu$ is onto, we have (5. 2).

We now apply these arguments to the particular case that interests us, writing

$$C = \Gamma_D\colon\ y^2z = x^3 - Dxz^2,$$
$$C_1 = \Gamma_{-4D}\colon\ y_1^2z_1 = x_1^3 + 4Dx_1z_1^2.$$

We take $n = 2$, and define ν as the map $C_1 \to C$ given by

$$(x_1, y_1, z_1) \to [2x_1(x_1^2 + 4Dz_1^2),\ y_1(x_1^2 - 4Dz_1^2),\ 8x_1^2z_1]$$

and ν_1 as that given by $(x, y, z) \to [y^2z,\ y(x^2 + Dz^2),\ x^2z]$. Then we have

Lemma 8. *There is a natural isomorphism between the ν-coverings of Γ_D and the elements of Q^*/Q^{*2}. If (a) is any element of Q^*/Q^{*2}, the corresponding curve $\mathcal{D}$ may be taken to be*

$$\mathcal{D}\colon\ as^2 = a^2t^4 - D. \tag{5. 5}$$

We follow the proof of Lemma 4 of Cassels [5] II. Let $x_1 = (x_1, y_1, z_1)$ be generic on C_1 and write

$$x = \nu x_1,\ t = y_1/2a^{\frac{1}{2}}x_1.$$

Then we have $y_1^2/x_1^2 = 4x/z = 4at^2$; and if $\mathcal{D}$ is the locus of (x, t) it follows that $\mathcal{D}$ is defined over the rationals and is in birational correspondence with C_1 over the complex numbers, and that the induced map $\mathcal{D} \to C$ maps (x, t) on x. Hence we have a ν-covering. If we write $y/z = ast$ then $\mathcal{D}$ takes the form (5. 5).

Conversely, let $\mathfrak{d}$ be the point $(0, 0, 1)$ on Γ_D, and let $\mathcal{D}$ be the curve of the ν-covering with generic point X corresponding to x_1. The inverse image of $\mathfrak{o}^{-1}\mathfrak{d}$ on $\mathcal{D}$ is rational and linearly equivalent to zero; hence there is a function $f(X)$ defined over the rationals with this divisor; and since x/z has divisor $(\mathfrak{o}^{-1}\mathfrak{d})^2$ it follows that $x/z = af^2(X)$ for some

rational a. The class of a in Q^*/Q^{*2} does not depend on the choice of f; and it is easy to show that the two correspondences we have set up are inverses. This proves the Lemma.

We note that if $\mathcal{D}$ is everywhere locally soluble then we may take a to be a factor of D; for if p is a simple prime factor of a not dividing D then the three terms in (5. 5) are all divisible by different powers of p and so the equation is impossible. If $a \mid D$ then we need only examine the solubility of (5. 5) in the reals and in those p-adic fields with $p \mid 2D$; for the other fields it is trivially soluble. Hence it is easy to find G_ν, and similarly G_{ν_1}.

If, as in our previous paper, we write 2^t for the number of elements of order 2 in the Tate-Šafarevič group of Γ_D, so that 2^t is the order of G_2/G_2', then we can express (5. 2) and (5. 4) as follows:

Lemma 9. *Write 2^λ for the order of G_ν, and define λ', λ_1, λ_1', similarly. Then we have*

$$g = \lambda' + \lambda_1' - 2, \quad g + t \leqq \lambda + \lambda_1 - 2. \tag{5. 6}$$

In proving this we have to split cases. If D is a rational square, the order of G_n is 2^{g+t+2} and the denominator of (5. 2) is 1; otherwise the order of G_n is 2^{g+t+1} and the denominator of (5. 2) is 2. Similarly for (5. 4).

For historical reasons, $\lambda + \lambda_1 - 2$ is called the number of first descents; it is easy to show directly that it is non-negative. In general, there need not be equality in the second equation (5. 6). We shall write G_ν^* for the group of those ν-coverings of Γ_D which can be lifted back to everywhere locally soluble 2-coverings, and define λ^* by analogy with λ; similarly for λ_1^*. Then

$$g + t = \lambda^* + \lambda_1 - 2,$$

and it may be shown by the methods of Cassels that $\lambda - \lambda^*$ is an even integer. Since Γ_D and Γ_{-4D} may have different Tate-Šafarevič groups, $\lambda - \lambda^*$ and $\lambda_1 - \lambda_1^*$ need not be equal; we have many examples of this phenomenon.

Most of the cases with $g = 0$ in Table 1 were obtained at once from Lemma 9; but when $t > 0$ for one of the curves Γ_D or Γ_{-4D} it was necessary to do a further descent. The next step is to find λ^*, and for this we use

Lemma 10. *Let* (5. 5) *be a ν-covering of Γ_D which is everywhere locally soluble, and let σ, τ be rational numbers such that*

$$a\sigma^2 = a^2\tau^2 - D. \tag{5. 7}$$

Then there is a one-one correspondence between the elements of Q^*/Q^{*2} and the ways of extending (5. 5) *to a 2-covering of Γ_D; if (b) is any element of Q^*/Q^{*2}, the corresponding curve $\mathcal{D}$ may be taken to be*

$$as^2 = a^2t^4 - D, \quad as\sigma - a^2t^2\tau + D = bu^2. \tag{5. 8}$$

We know that (5. 7) is soluble; for it is everywhere locally soluble by comparison with (5. 5). Now let x_2 be generic on the left-hand copy of C in the diagram

$$\begin{array}{ccccc} C & \longrightarrow & C_1 & \longrightarrow & C \\ & & \updownarrow & \nearrow & \\ & & \mathcal{D} & & \end{array}$$

and write $x_1 = \nu_1 x_2$; retain otherwise the notation of Lemma 8. If we write

$$u = \left(\frac{a^{\frac{1}{2}}\sigma - a\tau}{b}\right)^{\frac{1}{2}}\left(\frac{x_2^2 - Dz_2^2 - 2x_2z_2(a^{\frac{1}{2}}\sigma + a\tau)}{2y_2z_2}\right)$$

we may after some trouble verify that

$$as\sigma - a^2t^2\tau + D = bu^2.$$

The rest of the proof is analogous to that of Lemma 8, and is therefore omitted. We note that the correspondence is not natural, that is, it depends on the choice of σ and τ.

By eliminating s, we may replace the equations (5. 8) by the single equation

$$b^2u^4 + 2bu^2(a^2t^2\tau - D) + Da^2(t^2 - \tau)^2 = 0. \tag{5. 9}$$

From this we may find necessary conditions on b for $\mathcal{D}$ to be everywhere locally soluble, analogous to those for a which follow the proof of Lemma 8. We may assume b to be a square free integer. Then if p is an odd prime which divides the denominators of σ, τ to an odd power and does not divide D, it must divide b; and the only other primes that may divide b are those that divide $2D$.

If we use Lemma 10 to find the 2-coverings of Γ_D explicitly, some care is needed to avoid duplication. In general, there are several essentially different ways of extending a ν_1-covering to the same n-covering; the number is equal to the order of the kernel of the map $G_\nu \to G_n$ described earlier. In our actual case, if D is not a square there are 2 distinct extensions giving rise to each 2-covering and they correspond to the values b_0 and Db_0 for b. If D is a square, there is only one extension for each 2-covering.

If $t > 0$ for both of the curves Γ_D and Γ_{-4D}, then in order to find g it is necessary to go on at least to the third descent. We have in fact worked out the formulae for this. Unfortunately, mainly owing to machine development, we have not been able to use these formulae, as we had intended, to fill in some of the gaps in Table 1. We therefore omit all the details of the third descent; we will be happy to supply the formulae to any intending computer. An alternative method is given in [10].

§ 6. The Tamagawa number

In this section we define the Tamagawa number that we use, and show how to calculate it. Since we are dealing with an unusually simple particular case, we have tried to make our description at least formally self-contained; for a general account see [23].

Let V be a group-variety of dimension n, defined over the rationals. There exists on V an n^{th} order differential ω which is defined over the rationals and invariant under left translation; and ω is unique up to multiplication by a non-zero rational. (This much freedom does not matter, for the rational factor turns out to be self-cancelling.) If $x_1, \ldots, x_n$ are local coordinates at the origin on V, then we may write

$$\omega = g\,dx_1 \cdots dx_n.$$

For any prime p, including infinity, let V_p be the set of points of V defined over the p-adic numbers; then V_p is a topological group and ω induces on it a Haar measure

$$\omega_p = |\,g\,|_p (dx_1)_p \cdots (dx_n)_p$$

invariant under left translation. Here $|\ g\ |_p$ is the normal p-adic valuation, and for finite p we normalise $(dx)_p$ by the condition

$$\int_{\mathfrak{o}_p} (dx)_p = 1,$$

the integral being taken over the ring of p-adic integers; we note that this is equivalent to

$$\int_{\text{units}} (dx)_p = \frac{p-1}{p}.$$

Suppose now for simplicity that V is complete. We may define the 'adèle variety' V_A to be $\prod_p V_p$, the product being taken over all primes including infinity; then $\omega_A = \prod \omega_p$ is a measure on V_A. Since $\prod |\ a\ |_p = 1$ for non-zero rational a, ω_A remains invariant when ω is multiplied by a non-zero rational. Write V_Q for the subgroup of points of V with rational coordinates; there is a natural imbedding of V_Q into V_A. The Tamagawa number may be defined by

$$t(V) = \int_{V_A/V_Q} \omega_A. \tag{6.1}$$

In the more usual case, V is not complete and one must proceed with more care; see [23]. Tamagawa and others have shown that for the classical groups the Tamagawa number is a small positive integer. For example, the orthogonal group of a quadratic form not representing zero has Tamagawa number 2; and this fact is equivalent to Siegel's theorem, see for instance [24].

In our particular case, V is the elliptic curve Γ_D, with differential

$$\omega = dx/y.$$

In the main case we consider, Γ_D has only finitely many rational points. We have found it more convenient not to factor them out, so we define formally

$$\tau(D) = \prod_p \int_{\Gamma_p} \omega_p, \tag{6.2}$$

where the product is over all primes including infinity and Γ_p is the p-adic completion of the projective curve Γ_D.

Various difficulties may arise in interpreting a product like (6.2). It may be necessary to insert convergence factors, one to each term of the product; we do not do this here, but expect that we shall need to do so when discussing curves Γ_D with $g > 0$. Whether or not this has been done, there are now three useful possibilities for the infinite product. It may converge absolutely, or it may converge conditionally provided the factors are taken in their natural order. Both these cases occur in the work of Tamagawa. Failing these, it is necessary to ascribe a value to the product (6.2) by a suitable summation method; and this we have to do here. Formally, the product (6.2) differs only in finitely many factors from that for $[L_D(1)]^{-1}$, by Lemma 12 below; and we can therefore deduce a value for $\tau(D)$ from that of $L_D(1)$. More rigorously, we regard the infinite product in (6.2) as the formal value of the Euler product form of a Dirichlet series at $s = 1$, and ascribe to it the value at $s = 1$ of the underlying function. This gives rise to a satisfactory summation method, closely allied to that of Abel.

There are no difficulties of principle in calculating the separate integrals in (6.2), though the details are tedious. For convenience we shall as usual assume that D is fourth power free; however we allow D to be divisible by 4 since $\tau(D)$ is not invariant under isogeny.

Lemma 11. *If p is odd and $p \mid D$ then $\int \omega_p = 2$ unless $p^2 \| D$ and D is a p-adic square, in which case $\int \omega_p = 4$.*

Suppose first that $p \| D$; then we have

$$V_p = \bigcup_{n=0}^{\infty} F_n \cup \bigcup_{n=0}^{\infty} G_n,$$

where F_n is the set of points with $p^{2n+1} \| x$, $p^{n+1} \| y$ and G_n is the set of points with $p^{-2n} \| x$, $p^{-3n} \| y$. The point (x, y) can belong to F_n only if $-Dx$ is a p-adic square, and to each such x correspond two values of y; hence the contribution to the integral from F_n is $p^{n+1}(p-1)/p^{2n+2}$. Similarly, (x, y) can belong to G_n only if x is a p-adic square, and to each such x correspond two values of y; hence the contribution to the integral from G_n is $(p-1)/p^{n+1}$. Adding all these together, we find that $\int \omega_p = 2$.

The case $p^3 \| D$ is similar; we have

$$V_p = \bigcup_{n=1}^{\infty} F_n \cup \bigcup_{n=0}^{\infty} G_n$$

where G_n is as before but F_n is the set of points with $p^{2n+1} \| x$, $p^{n+2} \| y$. Now the contribution to the integral from F_n is $(p-1)/p^n$; and adding up as before we find that $\int \omega_p = 2$.

Finally, suppose that $p^2 \| D$. Then we have

$$V_p = \bigcup_{n=1}^{\infty} F_n \cup \bigcup_{n=0}^{\infty} G_n \cup \bigcup_{n=2}^{\infty} H_n,$$

where F_n is the set of points with $p^{2n} \| x$, $p^{n+1} \| y$, G_n is as before and H_n is the set of points with $p \| x$, $p^n \| y$. The contribution to the integral from F_n is $(p-1)/p^n$, and that from G_n is as usual $(p-1)/p^{n+1}$. H_n is null unless D is a p-adic square. If $D = c^2$ then the point (x, y) can belong to H_n only if $p^{2n-2} \| (x \pm c)$ and $2(x \pm c)$ is a p-adic square; and to each such x correspond two values of y. Hence in this case the contribution to the integral from H_n is $2(p-1)/p^{n-1}$. Adding everything up, we obtain the result stated in the lemma.

Lemma 12. *If p is odd and $p \nmid D$ then $\int \omega_p = N_p/p$.*

This is a special case of Theorem 2. 2. 5 of [23]; alternatively it may be proved in the same way as Lemma 11, remembering that in finding N_p we include the point at infinity.

Lemma 13. *If $D \equiv 3 \bmod 4$ then $\int \omega_2 = \frac{1}{2}$; if $D \equiv 4, 12, 36$ or $60 \bmod 64$ then $\int \omega_2 = 2$; in every other case $\int \omega_2 = 1$.*

We omit the proof of the lemma, which is similar to that of Lemma 11. It is necessary to consider a very large number of distinct cases, and though none of them individually presents much difficulty, the succession becomes wearisome.

Lemma 14.

$$\int \omega_\infty = \begin{cases} 4\omega D^{-\frac{1}{4}} & \text{for } D > 0, \\ 4\omega(-4D)^{-\frac{1}{4}} & \text{for } D < 0. \end{cases}$$

In the statement and proof of this lemma, ω denotes the real period of $\wp(u)$ as defined in § 3. If $D > 0$ we have

$$\int \omega_\infty = 2\left[\int_{-\sqrt{D}}^{0} + \int_{\sqrt{D}}^{\infty}\right] \frac{dx}{\sqrt{(x^3 - Dx)}} = 4\omega D^{-\frac{1}{4}};$$

if $D < 0$ we have

$$\int \omega_\infty = 2\int_0^\infty \frac{dx}{\sqrt{(x^3 - Dx)}} = 4\omega(-4D)^{-\frac{1}{4}}.$$

Here the factor 2 arises because there are two values of y for each acceptable x; for the evaluation of the elliptic integrals see [4], formulae 233.00, 237.00 and 239.00.

We can now express the Tamagawa number $\tau(D)$ in terms of $\sigma(D)$ which we have already shown how to compute. By Lemma 12 and the results of § 2, we have formally

$$\Pi \int \omega_p = \Pi (N_p/p) = [L_D(1)]^{-1}, \tag{6. 3}$$

where the products are taken over all finite primes not dividing $2D$. Define $\sigma(D)$ by (1. 6) even when $4 \mid D$, so that we have

$$\sigma(-4D) = 2\sigma(D) \text{ for } D > 0,$$
$$\sigma(-4D) = \sigma(D) \quad \text{for } D < 0.$$

Then by (1. 6), (6. 3) and Lemma 14

$$\tau(D)\,\sigma(D) = 4\Pi \int \omega_p, \tag{6. 4}$$

where the product is taken over the finitely many primes which divide $2D$. The right hand side of (6. 4) can be evaluated in any particular case by Lemmas 11 and 13.

We can similarly ascribe a Tamagawa number to any elliptic curve with finitely many rational points; and it is in each case a computable multiple of the formal product (1. 2). The analogues of Lemmas 11 and 13 are very messy, and we have in general no neat way of evaluating the formal product.

§ 7. The numerical evidence

In this section we describe the calculations that we have actually carried out on EDSAC 2, and the extent to which they confirm our conjectures. Let D be a positive integer not divisible by a fourth power or by 4; define $\sigma(D)$ by (1. 6) and Δ as in § 3. After Theorem 1, we know that $\sigma(D)$ is a rational integer for $|D| > 1$; by means of the formulae (3. 13) to (3. 17) we have computed its value whenever $|\Delta| < 108$ or $|\Delta| = 113, 165, 195, 231$.

The details of the calculation are of little interest, except for one point of organisation. Each of the Δ^2 terms in the formula used involves a quartic residue and a value of $\wp(u)$; and nearly all the time taken by the computation is spent in evaluating these. We therefore gain efficiency by calculating $\sigma(D)$ simultaneously for all D corresponding to a given Δ. If $|\Delta|$ is a prime p then we obtain the 12 cases

$$D = \pm 2^a p^b \ (a = 0, 1;\ b = 1, 2, 3);$$

if $|\Delta|$ is a product of two or three primes, we obtain respectively 36 or 108 cases. For a given value of Δ, the complete run took about $\Delta^2/20$ seconds. There is an automatic check against machine (or program) error, in that the final value of $\sigma(D)$ has to be an integer to within the accuracy of the calculation.

For comparison with our main conjecture (1. 5), we have also found the value of g for as many of the curves as we conveniently could. For each curve we have carried out the first descent by the methods of § 5, and where necessary the second descent also; we had hoped to carry out the third descent, but as explained in § 5 we were unable

to do so. The calculations are straightforward except for the recurrent need to solve equations of the form

$$ax^2 + by^2 + cz^2 = 0 \tag{7.1}$$

over the rationals. One of Lagrange's proofs of his theorem [16] gives a constructive method of solving (7.1) when it is possible. Alternatively we may search for a solution, since Holzer [14] has shown that we need only examine the region

$$x^2 \leqq |bc|,\ y^2 \leqq |ca|,\ z^2 \leqq |ab|.$$

The local solubility of the coverings was checked by methods similar to those described in our previous paper. In searching for rational points on the coverings we considered only relatively small values of the variables; for we have found that time spent on extending such a search is only meagrely rewarded.

For each of the values of D considered, we give in Table 1 the corresponding values of σ, g, λ and λ_1, the last two being the numbers of first descents defined in § 5. These are also the values of σ, g, λ_1 and λ respectively corresponding to $-4D$. Let τ be the Tamagawa number of Γ_D as defined in § 7; and let $\eta(D)$ be the number of rational points on Γ_D of finite order. (Thus within the limits of our table $\eta = 4$ when D is -4 or a square, and $\eta = 2$ otherwise.) Rather than take up space printing the values of $\tau(D)$ and $\tau(-4D)$, we have marked the value of σ with an asterisk whenever $\sigma \neq 0$ and $\tau(D) \neq \eta^2(D)$ or $\tau(-4D) \neq \eta^2(-4D)$. These cases are further described in Table 2; according to our conjectures they are just those in which $g = 0$ and the Tate-Šafarevič group is non-trivial; Table 2 is possibly less reliable than Table 1.

We have given the value of g whenever we know it. A gap instead of the value of g indicates that we do not know it, and indeed have no information beyond that given by the general inequality

$$0 \leqq g \leqq \lambda + \lambda_1 - 2.$$

An entry such as '1—' indicates that (because of the second descent) we know that $g \leqq 1$; in these cases there is a non-trivial Tate-Šafarevič group. An entry such as '1+' indicates that we know that $g \geqq 1$ since we have actually found a generator.

In Table 1 we have packed onto each line the entries corresponding to four linked values of D. In each line the first column gives an odd positive integer D_0. The remaining sixteen columns form four groups of four. The first group gives the values of σ, g, λ and λ_1 for $D = D_0$; and the other three groups correspond to the cases $D = -D_0$, $D = 2D_0$ and $D = -2D_0$ in that order.

Let us write $\gamma = \eta^2/\tau$; then the main conjectures of this paper are that $\gamma \neq 0$ if and only if $g = 0$, and that in this case γ is the order of the Tate-Šafarevič group. The first part of this agrees with our calculations whenever we know g. Moreover, the work of Cassels [5] strongly suggests that g should have the parity of $\lambda + \lambda_1$; and in our tables $\gamma = 0$ whenever $\lambda + \lambda_1$ is odd. For the second part of the conjecture, we note that in our tables γ is always a square; and Cassels has shown that when the order of the Tate-Šafarevič group is finite it is a square. We have made no attempt to calculate p-coverings for any prime $p > 2$; and the practical difficulties appear to us formidable. But we do known the 2-component of the Tate-Šafarevič group in every case for which we know that $g = 0$; and this yields always the correct power of 2 in γ. (The few cases where $\gamma \neq 0$ but we do not know that $g = 0$ are ones in which the second descent is indecisive; it is further corroboration of the conjecture that in these cases γ is divisible by a high power of 2.)

In the course of these calculations, we observed another identity which we conjectured to hold always; this is

$$\tau(-4D)/\tau(D) = 2^{\lambda_1-\lambda}; \tag{7.2}$$

in fact, without some such identity our conjectures for $\tau(-4D)$ and $\tau(D)$ could hardly be consistent. This relation need not be confined to the case $\gamma \neq 0$, for the left hand side may be written as a finite product. In fact we deduce from the results of § 6 that

$$\tau(-4D)/\tau(D) = \prod_{p \mid 2D\infty} \varrho_p,$$

where, for each p, ϱ_p is short for $\int_{\Gamma_D} \omega_p \Big/ \int_{\Gamma_{-4D}} \omega_p$, and may be read off explicitly from Lemmas 11, 13 and 14.

We are glad to say that Cassels [7] has been able to prove a more general theorem including (7. 2), which gives our conjectures considerable support. The identity has also been verified more directly by E. Forrest [10].

Table 1

D	D			$-D$			$2D$			$-2D$		
	σ	g	$\lambda.\lambda_1$	σ	g	$\lambda.\lambda_1$	σ	g	$\lambda.\lambda_1$	σ	g	$\lambda.\lambda_1$
1	¼	0	1.1	½	0	0.2	0	1	2.1	1	0	1.1
3	1	0	1.1	0	1	1.2	0	1	2.1	2	0	1.1
5	0	1	2.1	0	1	1.2	0	1	2.1	2	0	1.1
7	0	1	1.2	2	0	1.1	0	1	2.1	0	2	2.2
9	1	0	2.0	0	1	0.3	2	0	1.1	0	1	2.1
11	1	0	1.1	2	0	1.1	0	1	2.1	2	0	1.1
13	2	0	1.1	0	1	1.2	0	1	2.1	2	0	1.1
15	0	1	1.2	0	1	1.2	0	1	2.1	4	0	1.1
17	0	2	2.2	4*	0	1.3	0	1	3.2	0	2	2.2
19	1	0	1.1	0	1	1.2	0	1	2.1	2	0	1.1
21	0	1	2.1	0	1	1.2	0	1	2.1	4	0	1.1
23	0	1	1.2	2	0	1.1	0	1	2.1	0	2	2.2
25	0	1	2.1	2	0	0.2	0	1	2.1	2	0	1.1
27	1	0	1.1	2	0	1.1	0	1	2.1	2	0	1.1
29	2	0	1.1	0	1	1.2	0	1	2.1	2	0	1.1
31	0	1	1.2	0	1	1.2	0	1	2.1	8*	0	2.2
33	4	0	1.1	0	2	1.3	0	1	2.1	0	2	2.2
35	2	0	1.1	0	1	1.2	0	1	2.1	4	0	1.1
37	0	1	2.1	0	1	1.2	0	1	2.1	2	0	1.1
39	0	1	1.2	0	2	2.2	0	1	2.1	4	0	1.1
41	0	1	2.1	4*	0	1.3	0	3	3.2	8*	0	2.2
43	1	0	1.1	2	0	1.1	0	1	2.1	2	0	1.1
45	0	1	1.2	4	0	1.1	0	2	3.1	0	1	1.2
47	0	1	1.2	0	1	1.2	0	1	2.1	0	2	2.2
49	0	1	2.1	0	1	0.3	4*	0	3.1	0	1	1.2
51	2	0	1.1	0	1	1.2	0	1	2.1	4	0	1.1
53	0	1	2.1	0	1	1.2	0	1	2.1	2	0	1.1
55	0	1	1.2	0	2	2.2	0	1	2.1	4	0	1.1
57	0	1	2.1	8*	0	1.3	0	1	2.1	0	2	2.2
59	1	0	1.1	2	0	1.1	0	1	2.1	2	0	1.1
61	2	0	1.1	0	1	1.2	0	1	2.1	2	0	1.1
63	4	0	1.1	0	2	1.3	4	0	1.1	0	1	2.1
65	0	2	2.2	0	2	1.3	0	1	2.1	4	0	1.1
67	1	0	1.1	0	1	1.2	0	1	2.1	2	0	1.1
69	0	1	2.1	0	1	1.2	0	1	2.1	0	2	2.2
71	0	1	1.2	2	0	1.1	0	1	2.1	8*		2.2
73	0	1	2.1	0	2	1.3	0	1	3.2	8*		2.2
75	2	0	1.1	4	0	1.1	0	1	2.1	0	2	2.2
77	0	2	2.2	0	1	1.2	0	1	2.1	0	2	2.2
79	0	1	1.2	0	1	1.2	0	1	2.1	0	2	2.2

D	D			$-D$			$2D$			$-2D$		
	σ	g	$\lambda.\lambda_1$	σ	g	$\lambda.\lambda_1$	σ	g	$\lambda.\lambda_1$	σ	g	$\lambda.\lambda_1$
83	1	0	1.1	0	1	1.2	0	1	2.1	2	0	1.1
85	0	1	2.1	0	1	1.2	0	1	2.1	4	0	1.1
87	0	1	1.2	4	0	1.1	0	1	2.1	4	0	1.1
89	0	1	2.1	0	2	1.3	0	1	3.2	0	2	2.2
91	2	0	1.1	4	0	1.1	0	1	2.1	4	0	1.1
93	4	0	1.1	0	1	1.2	0	1	2.1	4	0	1.1
95	0	1	1.2	0	1	1.2	0	1	2.1	4	0	1.1
97	0	2	2.2	4*	0	1.3	0	1	3.2	8*		2.2
99	0	1	1.2	0	2	2.2	8*	0	3.1	0	1	1.2
101	0	1	2.1	0	1	1.2	0	1	2.1	2	0	1.1
103	0	1	1.2	2	0	1.1	0	1	2.1	0	2	2.2
105	0	1	2.1	0	2	1.3	0	1	2.1	8	0	1.1
107	1	0	1.1	2	0	1.1	0	1	2.1	2	0	1.1
113	8*		2.2	0	2	1.3	0	3	3.2	0	2	2.2
117	0	2	3.1	8*	0	1.3	4	0	1.1	0	1	2.1
121	1	0	2.0	0	1	0.3	2	0	1.1	0	1	2.1
125	2	0	1.1	0	1	1.2	0	1	2.1	2	0	1.1
135	0	1	1.2	4	0	1.1	0	1	2.1	4	0	1.1
147	0	1	1.2	8	0	1.1	4	0	1.1	0	1	2.1
153	4	0	1.1	0	1	1.2	0	2	3.1	0	1	1.2
165	0	1	2.1	0	1	1.2	0	1	2.1	8	0	1.1
169	0	1	2.1	2	0	0.2	0	1	2.1	2	0	1.1
171	0	1	2.1	0	1	1.2	0	2	2.2	0	1	2.1
175	0	1	1.2	0	1	1.2	0	1	2.1	8	0	1.1
189	4	0	1.1	0	1	1.2	0	1	2.1	4	0	1.1
195	4	0	1.1	0	1	1.2	0	1	2.1	0	2	2.2
207	0	2	1.3	8	0	1.1	8*	0	3.1	0	1	1.2
225	0	1	2.1	0	1	0.3	4	0	1.1	0	1	2.1
231	0	1	1.2	8	0	1.1	0	1	2.1	8	0	1.1
245	4	0	1.1	4	0	1.1	4	0	1.1	0	1	2.1
261	4	0	1.1	4	0	1.1	0	2	3.1	0	1	1.2
275	0	2	2.2	0	1	1.2	0	1	2.1	4	0	1.1
279	4	0	1.1	0	1	1.2	4	0	1.1	0	1	2.1
289	4*	0	2.2	0	2	1.3	0	1	2.1	4	0	1.1
297	0	1	2.1	8*	0	1.3	0	1	2.1	0	2	2.2
315	0	1	1.2	0	1	2.1	0	2	3.1	0	1	1.2
325	0	1	2.1	0	1	1.2	0	1	2.1	0	2	2.2
343	0	1	1.2	2	0	1.1	0	1	2.1	8*		2.2
351	0	1	1.2	0	1	1.2	0	1	2.1	4	0	1.1
361	1	0	2.0	0	1	0.3	2	0	1.1	0	1	2.1
363	0	1	2.1	0	1	1.2	0	2	2.2	0	1	2.1
375	0	1	1.2	4	0	1.1	0	1	2.1	4	0	1.1
425	0	1	2.1	0	2	1.3	0	1	2.1	8	0	1.1
441	0	1	3.0	8*	0	0.4	0	1	2.1	8	0	1.1
459	2	0	1.1	4	0	1.1	0	1	2.1	4	0	1.1
475	4	0	1.1	0	2	2.2	0	1	2.1	4	0	1.1
495	8	0	1.1	0	2	1.3	8	0	1.1	0	1	2.1
507	0	2	2.2	8	0	1.1	0	1	2.1	4	0	1.1
513	4	0	1.1	0	2	1.3	0	1	2.1	16*		2.2
525	0	2	2.2	0	1	1.2	0	1	2.1	8	0	1.1
529	0	1	2.1	0	1	0.3	4*	0	3.1	0	1	1.2
539	0	1	2.1	0	1	1.2	8*	0	3.1	0	1	1.2
585	8	0	1.1	0	1	1.2	0	2	3.1	0	1	1.2
605	0	1	2.1	8*	0	1.3	4	0	1.1	0	1	2.1
621	0	2	2.2	0	1	1.2	0	1	2.1	16*		2.2
637	0	1	1.2	4	0	1.1	4	0	1.1	0	1	2.1
675	2	0	1.1	0	1	1.2	0	1	2.1	8	0	1.1
693	8	0	1.1	8	0	1.1	0	2	3.1	0	1	1.2
735	8	0	1.1	0	2	1.3	0	2	3.1	0	1	1.2
783	0	1	1.2	0	1	1.2	0	1	2.1	4	0	1.1

D	D			$-D$			$2D$			$-2D$		
	σ	g	$\lambda.\lambda_1$	σ	g	$\lambda.\lambda_1$	σ	g	$\lambda.\lambda_1$	σ	g	$\lambda.\lambda_1$
825	0	1	2.1	0	2	1.3	0	1	2.1	16	0	1.1
837	0	1	2.1	0	1	1.2	0	1	2.1	4	0	1.1
841	0	1	2.1	2	0	0.2	0	1	2.1	18*	0	1.1
845	4	0	1.1	0	1	1.2	0	1	3.2	8	0	1.1
847	0	2	1.3	8	0	1.1	8*	0	3.1	0	1	1.2
867	2	0	1.1	0	1	1.2	0	1	2.1	4	0	1.1
875	2	0	1.1	4	0	1.1	0	1	2.1	4	0	1.1
945	8	0	1.1	0	2	1.3	0	1	2.1	8	0	1.1
961	0	1	2.1	0		0.3	0	2	3.1	0		1.2
975	0	1	1.2	0	1	1.2	0	1	2.1	8	0	1.1
1029	0	1	2.1	0	1	1.2	0	1	2.1	4	0	1.1
1083	0	1	1.2	0	1	2.1	8*	0	3.1	0	1	1.2
1089	4	0	2.0	8*	0	0.4	0	1	1.2	0	2	3.1
1125	4	0	1.1	4	0	1.1	8*	0	3.1	0	1	1.2
1183	0	1	1.2	0	1	1.2	0	1	2.1	8	0	1.1
1225	4	0	2.0	0	1	0.3	0	2	3.1	0	1	1.2
1323	0	1	1.2	0	1	2.1	4	0	1.1	0	1	2.1
1331	1	0	1.1	0	1	1.2	0	1	2.1	18*	0	1.1
1369	0	1	2.1	2	0	0.2	0		2.1	2	0	1.1
1375	0	1	1.2	0	1	1.2	0	1	2.1	4	0	1.1
1445	0	1	2.1	0	1	1.2	0	1	2.1	4	0	1.1
1485	8	0	1.1	0	1	1.2	0	1	2.1	8	0	1.1
1521	0	1	2.1	0	1	0.3	4	0	1.1	0	1	2.1
1575	8	0	1.1	0	1	1.2	0	2	2.2	0	1	2.1
1587	0	1	2.1	16*	0	1.3	8*	0	3.1	0	1	1.2
1617	0	1	1.2	0	1	1.2	8	0	1.1	0	1	2.1
1625	0	1	2.1	8*	0	1.3	0	1	2.1	4	0	1.1
1681	0	2	2.2	8*		1.3	0	1	2.1	4	0	1.1
1715	2	0	1.1	0	1	1.2	0	1	2.1	4	0	1.1
1755	4	0	1.1	8	0	1.1	0	1	2.1	0	2	2.2
1805	0	1	2.1	0	2	1.3	4	0	1.1	0	1	2.1
1815	8	0	1.1	0	1	1.2	8	0	1.1	0	1	2.1
1849	9*	0	2.0	0	1	0.3	2	0	1.1	0	1	2.1
2079	0	1	1.2	0	1	1.2	0	1	2.1	8	0	1.1
2125	4	0	1.1	0	1	1.2	0	1	2.1	4	0	1.1
2197	0	1	2.1	0		1.2	0	1	2.1	2	0	1.1
2205	0	2	1.3	0	1	2.1	0	1	2.1	16	0	1.1
2209	0	1	2.1	0		0.3	16*		3.1	0	1	1.2
2375	0	1	1.2	0	2	2.2	0	1	2.1	4	0	1.1
2475	0	1	1.2	0	1	2.1	0	2	3.1	0	1	1.2
2523	18*	0	1.1	4	0	1.1	0	1	2.1	8	0	1.1
2535	0	1	1.2	8	0	1.1	0	1	2.1	0	2	2.2
2541	0	1	1.2	8	0	1.1	0	2	3.1	0	1	1.2
2601	4	0	2.0	0	1	0.3	0	2	2.2	0	1	2.1
2625	8	0	1.1	16*	0	1.3	0	1	2.1	8	0	1.1
2809	0		2.1	2	0	0.2	0		2.1	2	0	1.1
2883	0		1.2	8	0	1.1	4	0	1.1	0	1	2.1
2925	0	1	2.1	0	2	1.3	0	2	2.2	0	1	2.1
3025	0	1	2.1	0	1	0.3	4	0	1.1	0	1	2.1
3087	4	0	1.1	16*	0	1.3	4	0	1.1	0	1	2.1
3249	4	0	2.0	8*	0	0.4	0	1	1.2	0	2	3.1
3267	0	1	2.1	16*	0	1.3	16*		2.2	0	1	2.1
3375	0	1	1.2	0	1	1.2	0	1	2.1	4	0	1.1
3481	1	0	2.0	0		0.3	2	0	1.1	0		2.1
3675	0	1	1.2	0	1	2.1	16	0	1.1	0	1	2.1
3721	0	1	2.1	2	0	0.2	0	1	2.1	18*	0	1.1
3773	16*		2.2	0	1	1.2	0	1	2.1	16*		2.2
3993	0	1	2.1	8*	0	1.3	0	1	2.1	16*		2.2
4125	8	0	1.1	0	1	1.2	0	1	2.1	8	0	1.1
4225	0	2	2.2	8	0	0,2	0	1	2.1	4	0	1.1

D	D			$-D$			$2D$			$-2D$		
	σ	g	$\lambda.\lambda_1$	σ	g	$\lambda.\lambda_1$	σ	g	$\lambda.\lambda_1$	σ	g	$\lambda.\lambda_1$
4459	2	0	1.1	4	0	1.1	0		2.1	4	0	1.1
4489	1	0	2.0	0		0.3	18*	0	1.1	0	1	2.1
4563	16*		2.2	0	1	1.2	0	1	2.1	4	0	1.1
4725	0	1	2.1	0	1	1.2	0	1	2.1	8	0	1.1
4761	0	1	3.0	0	2	0.4	0	1	2.1	32*		2.2
4851	8	0	1.1	0	1	1.2	0	3	4.1	32*	0	1.3
4875	4	0	1.1	8	0	1.1	0	1	2.1	0	2	2.2
4913	8*		2.2	4*	0	1.3	0	1	3.2	8*		2.2
5041	0	1	2.1	0		0.3	4*	0	3.1	0		1.2
5145	0	1	2.1	16*	0	1.3	0	1	2.1	8	0	1.1
5329	4*	0	2.2	8*		1.3	0	1	3.2	0	2	2.2
5445	0	1	2.1	0	1	1.2	0	1	2.1	16	0	1.1
5929	0	1	3.0	0	2	0.4	0	1	2.1	0	2	2.2
6125	0	1	1.2	4	0	1.1	4	0	1.1	0	1	2.1
6241	0		2.1	0		0.3	0	2	3.1	0		1.2
6591	0	1	1.2	0	1	1.2	0	1	2.1	36*	0	1.1
6615	8	0	1.1	0	1	1.2	16*	0	3.1	0	1	1.2
6655	0	1	1.2	0	1	1.2	0	1	2.1	4	0	1.1
6859	9*	0	1.1	2	0	1.1	0		2.1	2	0	1.1
6889	1	0	2.0	0	1	0.3	18*	0	1.1	0	1	2.1
7225	0	1	2.1	8	0	0.2	0	1	3.2	0	2	2.2
7425	8	0	1.1	16*	0	1.3	0	1	2.1	16	0	1.1
7569	0	1	2.1	0	1	0.3	4	0	1.1	0	1	2.1
7605	8	0	1.1	8	0	1.1	0	2	3.1	0	1	1.2
7623	0	1	1.2	16	0	1.1	0	1	2.1	16	0	1.1
7803	18*	0	1.1	4	0	1.1	0	1	2.1	4	0	1.1
7875	0	1	1.2	16	0	1.1	0	2	3.1	0	1	1.2
7921	4*	0	2.2	8*		1.3	0	1	3.2	16*		2.2
8281	4	0	2.0	0	1	0.3	0	2	3.1	0		1.2
8575	0	1	1.2	0	1	1.2	0	1	2.1	8	0	1.1
8649	0	1	3.0	8*	0	0.4	0		2.1	8	0	1.1
8775	0	1	1.2	16	0	1.1	0	1	2.1	8	0	1.1
9025	0	1	2.1	0	1	0.3	4	0	1.1	0	1	2.1
9075	0	1	2.1	0	2	1.3	16	0	1.1	0	1	2.1
9261	4	0	1.1	0	1	1.2	0	1	2.1	36*	0	1.1
9317	0	1	2.1	0	1	1.2	0	1	2.1	16*		2.2
9409	4*	0	2.2	0	2	1.3	0		2.1	4	0	1.1
9747	0	1	1.2	32*		2.2	8*	0	3.1	0	1	1.2
10201	0		2.1	2	0	0.2	0		2.1	18*	0	1.1
10609	0		2.1	0		0.3	4*	0	3.1	0	1	1.2
10985	0	1	2.1	8*	0	1.3	0	1	2.1	4	0	1.1
11025	16	0	2.0	0	2	0.4	0	1	2.1	16	0	1.1
11319	0	1	1.2	8	0	1.1	0		2.1	8	0	1.1
11449	9*	0	2.0	0		0.3	18*	0	1.1	0	1	2.1
11979	0	1	1.2	0	1	2.1	8*	0	3.1	0	1	1.2
12167	0	1	1.2	18*	0	1.1	0		2.1	8*		2.2
12375	8	0	1.1	0	1	1.2	8	0	1.1	0	1	2.1
12675	8	0	1.1	0	1	1.2	0	1	2.1	16	0	1.1
12769	16*		2.2	0	2	1.3	0	1+	3.2	0	2	2.2
14283	0		2.1	0	1	1.2	8*	0	3.1	0		1.2
14553	8	0	1.1	0	1	1.2	8	0	1.1	0	1	2.1
14625	0	1	1.2	0	1	1.2	16*	0	3.1	0	1	1.2
14739	2	0	1.1	0	1	1.2	0		2.1	4	0	1.1
15125	0	2	3.1	8*	0	1.3	4	0	1.1	0	1	2.1
15379	18*	0	1.1	0	1	1.2	0		2.1	4	0	1.1
15435	0	1	1.2	0	1	2.1	16*	0	3.1	0	1	1.2
16335	8	0	1.1	0	2	1.3	8	0	1.1	0	1	2.1
17787	8	0	1.1	16	0	1.1	0	1	1.2	32*	0	3.1
18375	8	0	1.1	0	1	1.2	0	2	3.1	0	1	1.2
19773	0	1	2.1	8*	0	1.3	4	0	1.1	0	1	2.1

D	D			$-D$			$2D$			$-2D$		
	σ	g	$\lambda.\lambda_1$	σ	g	$\lambda.\lambda_1$	σ	g	$\lambda.\lambda_1$	σ	g	$\lambda.\lambda_1$
19965	8	0	1.1	0	1	1.2	0	1	2.1	8	0	1.1
20577	4	0	1.1	32*		1.3	0		2.1	0	2	2.2
21125	0	1	2.1	0		1.2	0	1	2.1	0	2	2.2
22707	2	0	1.1	0	1	1.2	0		2.1	0	2	2.2
22815	0	1	1.2	0	1	1.2	0	1	2.1	0	2	2.2
22869	8	0	1.1	8	0	1.1	16*	0	3.1	0	1	1.2
23625	0	1	2.1	16*	0	1.3	0	1	2.1	8	0	1.1
24389	0		2.1	0		1.2	0		2.1	2	0	1.1
24565	0	1	2.1	0	1	1.2	0		2.1	4	0	1.1
25725	16	0	1.1	0	1	1.2	0	1	2.1	8	0	1.1
25947	0	1	1.2	0		2.1	36*	0	1.1	0	1	2.1
27225	0	1	3.0	0	2	0.4	0	1	1.2	32*	0	3.1
27951	0	1	1.2	0	1	1.2	0	1	2.1	72*	0	1.1
29791	0		1.2	0		1.2	0		2.1	8*		2.2
32955	4	0	1.1	8	0	1.1	0	1	2.1	32*		2.2
33075	0	1	1.2	16	0	1.1	0	2	2.2	0	1	2.1
33275	16*		2.2	8	0	1.1	0		2.1	4	0	1.1
33957	8	0	1.1	8	0	1.1	0	2	3.1	0	1	1.2
34295	0		1.2	16*		2.2	0	1	2.1	4	0	1.1
35937	4	0	1.1	32*		1.3	0		2.1	16*		2.2
36125	4	0	1.1	0		1.2	0		2.1	4	0	1.1
36501	0	1	2.1	0		1.2	0		2.1	16*		2.2
37125	0	1	2.1	0	1	1.2	0		2.1	8	0	1.1
38025	16	0	2.0	0	1	0.3	8	0	1.1	0	1	2.1
41503	32*		1.3	8	0	1.1	8*	0	3.1	0	1	1.2
42875	18*	0	1.1	4	0	1.1	0	1	2.1	4	0	1.1
43875	4	0	1.1	0	1	1.2	0	1	2.1	32*		2.2
44217	4	0	1.1	0		1.2	32*		3.1	0	1	1.2
45125	8*	0	3.1	32*		1.3	4	0	1.1	0		2.1
45375	8	0	1.1	32*	0	1.3	8	0	1.1	0	1	2.1
46305	8	0	1.1	16*	0	1.3	0		2.1	8	0	1.1
50653	18*	0	1.1	0		1.2	0	1	2.1	2	0	1.1
53361	0	1	3.0	0	1	0.5	16	0	1.1	0	1	2.1
54925	4	0	1.1	0		1.2	0	1	3.2	8	0	1.1
55125	0	1	1.2	0	1	2.1	0	1	2.1	16	0	1.1
57967	0	1	1.2	0	1	1.2	0	1	2.1	8	0	1.1
59319	0		1.2	16*		2.2	0		2.1	4	0	1.1
59895	8	0	1.1	0	1	1.2	8	0	1.1	0	1	2.1
61731	0		2.1	16*	0	1.3	16*		2.2	0		2.1
63375	0	1	1.2	0	1	1.2	0	1	2.1	16	0	1.1
65219	0		2.1	16*	0	1.3	8*	0	3.1	0	1	1.2
68921	0		2.1	4*	0	1.3	0	1+	3.2	32*		2.2
73167	0		1.2	0		1.2	0		2.1	4	0	1.1
77175	8	0	1.1	0	1	1.2	16	0	1.1	0	1	2.1
79507	1	0	1.1	0		1.2	0		2.1	2	0	1.1
81675	0		2.1	0	1	1.2	16	0	1.1	0	1	2.1
83853	0	1	1.2	8	0	1.1	16*	0	3.1	0		1.2
89373	36*	0	1.1	0	1	1.2	0		2.1	4	0	1.1
98865	0	1	1.2	0	1	1.2	0	2	3.1	0	1	1.2
99825	8	0	1.1	16*	0	1.3	0	1	2.1	16	0	1.1
101871	0	1	1.2	0	1	1.2	0	1	2.1	8	0	1.1
103823	0		1.2	0		1.2	0		2.1	0	1+	2.2
107653	36*	0	1.1	4	0	1.1	4	0	1.1	0		2.1
109503	32*		1.3	8	0	1.1	8*	0	3.1	0	1	1.2
114075	8	0	1.1	0	2	2.2	0	1	2.1	64*		2.2
122825	0		2.1	0	2	1.3	0	1	2.1	8	0	1.1
124509	0	1	1.2	8	0	1.1	64*		3.1	0	1	1.2
128625	8	0	1.1	0	2	1.3	0	1	2.1	72*	0	1.1
132651	2	0	1.1	36*	0	1.1	0		2.1	36*	0	1.1
136125	16	0	1.1	0	1	1.2	0	1	2.1	16	0	1.1

D	D			$-D$			$2D$			$-2D$		
	σ	g	$\lambda.\lambda_1$	σ	g	$\lambda.\lambda_1$	σ	g	$\lambda.\lambda_1$	σ	g	$\lambda.\lambda_1$
148877	2	0	1.1	0		1.2	0		2.1	18*	0	1.1
160083	72*	0	1.1	0	1	1.2	0	1	1.2	0	2	3.1
164775	0	1	1.2	16	0	1.1	0	1	2.1	8	0	1.1
165375	8	0	1.1	32*	0	1.3	16*	0	3.1	0		1.2
166375	0		1.2	16*		2.2	0		2.1	4	0	1.1
171475	4	0	1.1	0	1	1.2	0	1	2.1	36*	0	1.1
179685	0	1	2.1	0		1.2	0		2.1	8	0	1.1
185193	0		2.1	8*	0	1.3	0		2.1	16*		2.2
190125	0	1	1.2	8	0	1.1	32*	0	3.1	0	1	1.2
195657	8	0	1.1	0		1.2	72*	0	1.1	0	1	2.1
205379	9*	0	1.1	0		1.2	0		2.1	2	0	1.1
219501	0	1	1.2	4	0	1.1	8*	0	3.1	0		1.2
226981	0		2.1	0		1.2	0		2.1	98*	0	1.1
231525	0	1	2.1	0	1	1.2	0		2.1	8	0	1.1
251559	0		1.2	8	0	1.1	0		2.1	8	0	1.1
268119	4	0	1.1	0	1	1.2	100*	0	1.1	0	1	2.1
274625	16*		2.2	32*		1.3	0		2.1	36*	0	1.1
296595	4	0	1.1	0	1	1.2	0	1	2.1	32*		2.2
299475	0	1	1.2	32	0	1.1	64*		3.1	0	1	1.2
300763	49*	0	1.1	2	0	1.1	0		2.1	18*	0	1.1
328509	16*		2.2	0		1.2	0		2.1	0	2	2.2
357911	0	1	1.2	18*	0	1.1	0		2.1	0	1+	2.2
373527	0	1	1.2	16	0	1.1	0		2.1	16	0	1.1
385875	0		1.2	16	0	1.1	16*	0	3.1	0		1.2
389017	0		2.1	64*		1.3	0	1—	3.2	8*		2.2
408375	8	0	1.1	0	1	1.2	8	0	1.1	0		2.1
456533	0		2.1	0		1.2	0		2.1	64*		2.2
493039	0		1.2	0	1	1.2	0		2.1	32*		2.2
494325	16*	0	3.1	64*		1.3	16	0	1.1	0	1	2.1
499125	0		2.1	0	1	1.2	0		2.1	72*	0	1.1
570375	0		1.2	8	0	1.1	0		2.1	16	0	1.1
571787	9*	0	1.1	50*	0	1.1	0		2.1	2	0	1.1
586971	8	0	1.1	16	0	1.1	0	1	4.1	128*		1.3
614125	4	0	1.1	0		1.2	0		2.1	36*	0	1.1
658503	0		1.2	4	0	1.1	0		2.1	100*	0	1.1
704969	0		2.1	0	2	1.3	0	1	3.2	32*		2.2
753571	2	0	1.1	0		1.2	0		2.1	100*	0	1.1
804357	0		2.1	0		1.2	0		2.1	4	0	1.1
823875	4	0	1.1	0	1	1.2	0		2.1	0	2	2.2
857375	0	1	1.2	0		1.2	0		2.1	36*	0	1.1
898425	0		2.1	0	2	1.3	0		2.1	16	0	1.1
912673	72*		2.2	4*	0	1.3	0	1—	3.2	0	1+	2.2
1030301	18*	0	1.1	0		1.2	0		2.1	50*	0	1.1
1092727	0	1	1.2	98*	0	1.1	0		2.1	8*		2.2
1120581	8	0	1.1	72*	0	1.1	16*	0	3.1	0		1.2
1157625	0		2.1	64*		1.3	0		2.1	8	0	1.1
1225043	81*	0	1.1	0		1.2	0		2.1	18*	0	1.1
1369599	0		1.2	0		1.2	0		2.1	8	0	1.1
1442897	8*		2.2	64*		1.3	0		3.2	0	1+	2.2
1482975	0	1	1.2	0	1	1.2	0		2.1	72*	0	1.1
1497375	8	0	1.1	32*	0	1.3	8	0	1.1	0		2.1
1760913	0		1.2	0	1	1.2	8	0	1.1	0		2.1
2471625	8	0	1.1	0	1	1.2	16*	0	3.1	0		1.2
4108797	0	1	1.2	200*	0	1.1	16*	0	3.1	0	1	1.2
4492125	72*	0	1.1	0		1.2	0		2.1	8	0	1.1
7414875	36*	0	1.1	72*	0	1.1	0		2.1	32*		2.2
12326391	0		1.2	72*	0	1.1	0		2.1	72*	0	1.1

Table 2

We write $\gamma(D) = \eta^2(D)/\tau(D)$ as in § 7. Then in the range of Table 1

$$\gamma(D) = \gamma(-4D) = 0 \text{ or } 1,$$

except in the cases marked by asterisks. In the exceptional cases, γ takes the following values: —

(i) $\gamma(D) = 1$, $\gamma(-4D) = 4$

for $D =$ 98, 198, 414, 1058, 1078, 1694, 2166, 2250, 3174, 10082, 13230, 19494, 21218, 23958, 28566, 29250, 30870, 45125, 45738, 83006, 130438, 167706, 219006, 330750, 380250, 439002, 494325, 771750, 2241162, 4943250, 8217594;

and for $-D = 35574$, 54450.

(ii) $\gamma(D) = 4$, $\gamma(-4D) = 1$ for $D = 289$, 5329, 7921, 9409;

and for $-D =$ 17, 41, 57, 97, 117, 297, 441, 605, 1089, 1587, 1625, 2625, 3087, 3249, 3267, 3993, 4913, 5145, 7425, 8649, 9702, 10985, 15125, 19773, 23625, 45375, 46305, 61731, 65219, 68921, 99825, 165375, 185193, 912673, 1497375.

(iii) $\gamma(D) = \gamma(-4D) = 4$

for $D = 113$, 3773, 4563, 4913, 6534, 33275, 123462, 274625, 328509, 1442897;

and for $-D =$ 62, 82, 142, 146, 194, 686, 1026, 1242, 1681, 5329, 7546, 7921, 7986, 9522, 9747, 9826, 15842, 18634, 24334, 34295, 59319, 59582, 65910, 71874, 73002, 87750, 166375, 228150, 370386, 593190, 778034, 2185454, 14829750.

(iv) $\gamma(D) = 4$, $\gamma(-4D) = 16$ for $D =$ 4418, 88434, 249018, 598950.

(v) $\gamma(D) = 16$, $\gamma(-4D) = 4$ for $D = 12769$, 41503, 109503;

and for $-D = 20577$, 35937, 45125, 274625, 494325, 1157625, 1173942.

(vi) $\gamma(D) = \gamma(-4D) = 16$ for $-D =$ 137842, 913066, 986078.

(vii) $\gamma(D) = 64$, $\gamma(-4D) = 16$ for $-D =$ 389017, 1442897.

(viii) $\gamma(D) = \gamma(-4D) = 64$ for $-D = 1409938$.

(ix) $\gamma(D) = \gamma(-4D) = 9$

for $D =$ 1849, 2523, 6859, 7803, 8978, 11449, 13778, 15379, 22898, 42875, 50653, 51894, 89373, 107653, 160083, 205379, 391314, 571787, 1030301, 4492125, 7414875;

and for $-D = 1682$, 2662, 7442, 12167, 13182, 18522, 20402, 55902, 132651, 257250, 265302, 297754, 342950, 357911, 549250, 601526, 998250, 1120581, 1228250, 1714750, 2450086, 2965950, 7414875, 12326391, 24652782.

(ix) $\gamma(D) = \gamma(-4D) = 36$ for $D =$ 912673.

(x) $\gamma(D) = \gamma(-4D) = 81$ for $D = 1225043$.

(xi) $\gamma(D) = \gamma(-4D) = 25$ for $D =$ 536238;

and for $-D = 571787$, 1317006, 1507142, 2060602, 4108797.

(xii) $\gamma(D) = \gamma(-4D) = 49$ for $D = 300763$;

and for $-D = 453962$, 1092727.

References

[1] *G. Billing*, Beiträge zur arithmetischen Theorie ebener kubischer Kurven. Nova Acta Reg. Soc. Scient. Upsaliensis (4) **11** (1938), 1—165.

[2] *B. J. Birch* and *H. P. F. Swinnerton-Dyer*, Notes on elliptic curves I. J. reine u. angew. Math. **212** (1963), 7—25.

[3] *B. J. Birch*, Conjectures on elliptic curves, Amer. Math. Soc., Proceedings of Symposia in Pure Mathematics, 8: Theory of Numbers, Pasadena 1963.

[4] *P. F. Byrd* and *M. D. Friedmann*, Handbook of elliptic integrals for engineers and physicists. Berlin-Göttingen-Heidelberg 1954.

[5] *J. W. S. Cassels*, Arithmetic on curves of genus 1. I. On a conjecture of Selmer. J. reine u. angew. Math. **202** (1959), 52—99. II. A general result. J. reine u. angew. Math. **203** (1960), 174—208. III. The Tate-Šafarevič and Selmer groups. Proc. London Math. Soc. (3) **12** (1962), 259—296. IV. Proof of the Hauptvermutung. J. reine u. angew. Math. **211** (1962), 95—112.

[6] *J. W. S. Cassels*, Arithmetic on an elliptic curve. Proc. Intern. Congress Math., Stockholm **1962**, 234—246.

[7] *J. W. S. Cassels*, Arithmetic on curves of genus 1. VIII. On conjectures of Birch and Swinnerton-Dyer. J. reine u. angew. Math. **217** (1965), 180—199.

[8] *H. Davenport* and *H. Hasse*, Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen. J. reine u. angew. Math. **172** (1934), 151—182.

[9] *M. Deuring*, Die Zetafunktion einer algebraischen Kurve von Geschlechte Eins. I, II, III, IV. Nachr. Akad. Wiss. Göttingen (**1953**) 85—94; (**1955**) 13—42; (**1956**) 37—76; (**1957**) 55—80.

[10] *E. Forrest*, Number theory of elliptic curves. M. Sc. thesis, Cambridge 1964.

[11] *R. Fueter*, Vorlesungen über die singulären Moduln und die komplexe Multiplikation der elliptischen Funktionen. Leipzig 1924.

[12] *H. Hasse*, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper. II. Reziprozitätsgesetz. Jahresber. D. M. V. 1930 (Ergänzungsband 6), § 19.

[13] *H. Hasse*, Neue Begründung der komplexen Multiplikation I, II. J. reine u. angew. Math. **157** (1927), 115—139; **165** (1931), 64—88.

[14] *L. Holzer*, Minimal solutions of Diophantine equations. Canadian J. Math. **2** (1950), 238—244.

[15] *E. Hecke*, Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen. II. Math. Zeitschrift **6** (1920), 11—51.

[16] *J. L. Lagrange*, Oeuvres VII, 102—114.

[17] *Carl-Erik Lind*, Untersuchungen über die rationalen Punkte der ebenen kubischen Kurven vom Geschlecht Eins. Thesis, Univ. Uppsala 1940.

[18] *T. Ono*, On the Tamagawa number of algebraic tori. Annals of Math. **78** (1963) 47—73. On the relative theory of Tamagawa numbers. Bull. Amer. Math. Soc. **70** (1964), 325—326.

[19] *C. L. Siegel*, Über die analytische Theorie der quadratischen Formen. I, II, III. Ann. of Math. **36** (1935), 527—606; **37** (1936), 230—263; **38** (1937), 212—291.

[20] *J. Tate*, Duality theorems in Galois cohomology over number fields. Proc. Intern. Cong. Math., Stockholm **1962**, 288—295.

[21] *H. Weber*, Lehrbuch der Algebra, 2. Auflage, Braunschweig 1898.

[22] *A. Weil*, Jacobi sums as "Grössencharaktere". Trans. Amer. Math. Soc. **73** (1952), 487—495.

[23] *A. Weil*, Adèles and algebraic groups. Mimeo notes taken by M. Demazure and T. Ono, Princeton 1961.

[24] *A. Weil*, Sur la théorie des formes quadratiques. Colloque sur la Théorie des Groupes Algebriques, Brussels 1962, 9—22.

[25] *E. T. Whittaker* and *G. N. Watson*, A course of Modern Analysis. Cambridge 1902.

[26] *Ju. I. Manin*, Theory of commutative formal groups over fields of finite characteristic, Uspehi Math. Nauk. (Russian Math. Surveys) **18** (1963), 3—90.

[27] *J. Tate*, Algebric cohomology classes, Lecture delivered at the Summer Research Institute on Algebraic Geometry, Woods Hole 1964.

Eingegangen 25. April 1964