MATH. SCAND. 3 (1955), 68–74

THE DIOPHANTINE EQUATION $\eta^2 = \xi^3 - D$. A NOTE ON CASSELS' METHOD

ERNST S. SELMER

1. In his paper [1] on the rational solutions of the diophantine equation

$$\eta^2 = \xi^3 - D\,, \tag{1}$$

Cassels has given some far-reaching theorems about the number of generators (in the *Mordell-Weil* sense) of the corresponding curve, together with a table of solutions of infinite order for all $|D| \leqq 50$. Within these limits, his congruence conditions turn out to be sufficient for solubility of (1). He conjectured in [1] that his conditions were sufficient for *all* D, but retracted this in an addendum [2], after I had shown him some counterexamples, cf. [3, p. 215].

When D is not a perfect cube, Cassels works in the purely cubic field $K(D^{\frac{1}{3}}) = K(\delta)$, where a "first descent" for the equation (1) leads to a finite number of equations

$$x - t^2\delta = \mu\alpha^2 \tag{2}$$

with rational integer x and t (where $\xi = x/t^2$). Here μ (known) and α (unknown) are numbers from the field $K(\delta)$, and the number of possible μ determines the number of generators in the following way:

Let k be the number of independent generators of *even* order for the class-group of the field $K(\delta)$. To each such generator, we can find an integer γ_i ($i = 1, 2, \ldots, k$) of the field, such that $\gamma > 0$ and $[\gamma]$ (prime to 2) is the square of an ideal, while neither γ nor $\varepsilon\gamma$ is the square of a number from $K(\delta)$. Here ε (>0) is the basic unit, or any unit which is not the square of another unit. The *a priori* possible values of μ are then given by

$$\mu = \varepsilon^a \gamma_i^{a_i}, \qquad i = 1, 2, \ldots, k; \qquad a, a_i = 0, 1\,. \tag{3}$$

When $D \equiv \pm 1 \pmod 9$, the ideal $[3] = \mathfrak{r}^2\mathfrak{s}$, and we must also introduce a

$$[\gamma_0] = \mathfrak{r}\mathfrak{s} \tag{4}$$

Received March 15, 1955.

(possibly with an "auxiliary square" if $\mathfrak{r}\bar{\mathfrak{s}}$ is not a principal ideal), and a corresponding exponent a_0 in (3).

The number of *a priori* possible μ is consequently a power of 2:

$$N_0 = 2^{G_0}; \qquad G_0 = \begin{cases} k+1 & \text{if} \quad D \not\equiv \pm 1 \pmod 9 \\ k+2 & \text{if} \quad D \equiv \pm 1 \pmod 9 . \end{cases}$$

(Note: When D is exactly divisible by a rational cube, there are still further possibilities for γ, with a corresponding increase of the exponent G_0. Since this alternative does not occur in the below applications, we leave it out here.)

After applying the congruence conditions of Cassels, the number of remaining equations (2) is still of the form

$$N = 2^G, \quad G \leqq G_0 .$$

As I show elsewhere [7], a slight extension of Cassels' conditions in some cases will imply that these remaining equations are *possible for all moduli*.

Finally, the number of *soluble* equations (2) is also of the form

$$n = 2^g, \quad g \leqq G .$$

Here g is *the number of generators* (*basic solutions*) *of infinite order* for the given equation (1). ($g=0$, that is $n=1$, corresponds to the only value $\mu=1$, which is possible for all moduli but which can be excluded by the principle of "infinite descent".)

If the congruence conditions of the first descent were *sufficient*, we would of course have $g=G$. As already mentioned, however, there are in fact cases with $g<G$. I have earlier [5] formulated the following *conjecture* concerning rational points on cubic curves:

When a second descent exists, the number of generators is an even number less than what is indicated by the first descent.

In the same connection, it was shown that a second descent is always theoretically possible for a Weierstrass normal form. According to the conjecture, we should consequently always find

$$G-g = \text{an } \textit{even} \text{ number}$$

(including, of course, the most common value 0). This is in fact *verified* in all cases I have examined by Cassels' method. When $g<G$, I have been able to locate the cases

$$(5) \qquad G = 2,\ g = 0; \quad G = 3,\ g = 1 .$$

In a different connection (cf. [5, p. 51]), I have also had cases with none or two existing generators out of four indicated.

2. My examples of the cases (5) originate from the curve

$$X^3 + Y^3 = AZ^3 , \tag{6}$$

which I have earlier [3] [4] treated systematically, using a *different* type of descent and giving the basic solutions for all $A \leqq 500$ (we may clearly assume $A > 0$ and cube-free). It was the study of (6) that first led to my formulation of the above-mentioned conjecture.

It is well known (cf. [3, Ch. I]) that (6) is rationally equivalent to a curve (1) of the form

$$\eta_1^2 = \xi_1^3 - 3^3 2^4 A^2 .$$

This is again birationally connected with the curve

$$\eta^2 = \xi^3 + 2^4 A^2 ,$$

and the two curves have the same number of generators of infinite order. In Cassels' notation, we can consequently choose $D = -2^4 A^2$, and work in the purely cubic field

$$K(D^{\frac{1}{3}}) = K\big((2^4 A^2)^{\frac{1}{3}}\big) = K\big((4A)^{\frac{1}{3}}\big) .$$

This means a simplification if A is even, $A = 2A_1$, $K(D^{\frac{1}{3}}) = K(A_1^{\frac{1}{3}})$. Since a factor 2^6 can be removed from D, we get ($\|$ means "exactly divides"):

$$2 \| A \to 2 \nmid D, \qquad 2^2 \| A \to 2^2 \| D, \qquad 2 \nmid A \to 2^4 \| D . \tag{7}$$

The two first cases are covered by Cassels' Theorems VIII and XI respectively, and the last case by the formulae in his § 20. (As I show in [7], the conditions when $2^2 \| D$ and $2^4 \| D$ can be considerably simplified.) Whenever $D \equiv \pm 1 \pmod 9$ and a γ_0 of the type (4) is used, his conditions mod 3 of § 22 must also be applied.

I denote $4A$ (A odd) or $A_1 = \frac{1}{2}A$ (A even) by m, and the corresponding cubic field by $K(m^{\frac{1}{3}}) = K(\vartheta)$. To simplify the calculations, I have translated Cassels' conditions in the cases (7) into this field:

1) $2 \| A$, $m = \frac{1}{2}A$, $\vartheta = m^{\frac{1}{3}}$:

$$\mu \equiv \quad 1, \quad m\vartheta, \quad \vartheta^2 \pmod 4 ,$$

or

$$\mu \equiv 1 - m\vartheta, \; 2 - m\vartheta, \; 1 + 2\vartheta \pmod{\mathfrak{q}_2^2} ,$$

where $\mathfrak{q}_2$ is the second degree prime ideal factor of 2, and

$$\mathfrak{q}_2^2 = [4, 1 + m\vartheta + \vartheta^2] .$$

2) $2^2 \| A$, $m = \frac{1}{2}A$, $\vartheta = m^{\frac{1}{3}}$:

The coefficient of ϑ in μ must be *even*.

3) $2 \nmid A$, $m = 4A$, $\vartheta = (4A)^{\frac{1}{3}}$, $\overline{\vartheta} = (2A^2)^{\frac{1}{3}}$:

The coefficient of $\overline{\vartheta}$ in μ must be *even*.

When $m \equiv \pm 1 \pmod 9$ and a γ_0 of the type (4) is used, we get the additional conditions:

$$\begin{aligned} &1) \text{ and } 2) \quad \mu \equiv 1 - m\vartheta,\ -1 + \vartheta^2,\ m\vartheta - \vartheta^2 \pmod 3, \\ &3) \quad \mu \equiv 1 - A\vartheta,\ -1 - \overline{\vartheta},\ A\vartheta + \overline{\vartheta} \pmod 3. \end{aligned}$$

Both congruences are mod 3 *in the coefficients*.

When $m \equiv \pm 1 \pmod 9$ and a γ_0 is not used, the coefficients of μ must be *integers* mod 3. (This condition is not stated by Cassels.)

For $m \leqq 50$, the fields $K(m^{\frac{1}{3}}) = K(\vartheta)$ are covered by a table in Cassels' paper [1], giving class-numbers h, basic units ε and the numbers γ for even h. I have recently [6] extended the table to $m \leqq 100$. In my notes, I have further treated the fields with $100 < m \leqq 250$, and for $2^2 \| m$ up to $m \leqq 400$. This means that I can cover the equation (6) by Cassels' method in the cases

$$(8) \qquad A \text{ odd and } < 100; \qquad A \text{ even and } \leqq 500 .$$

For my purpose, only a summary treatment of the fields with $m > 100$ was necessary. It is usually quickly decided whether the class-number h is even or odd; in the latter case, the actual value of h is without interest. — No further examination is necessary if for instance

$$(9) \qquad \begin{cases} 2 \nmid h, & m \not\equiv \pm 1 \pmod 9, \quad g = 1 \\ 2 \nmid h, & m \equiv \pm 1 \pmod 9, \quad g = 2 \\ 2 \| h, & m \not\equiv \pm 1 \pmod 9, \quad g = 2 , \end{cases}$$

since then the *a priori* possible values of μ just suffice to give the correct number g of generators. — When Cassels' conditions must be used for exclusions, the generally complicated determination of the unit can be avoided. If for instance g is reduced by one in the cases (9), it will suffice to find and exclude one $\mu = \overline{\gamma}$ with the ordinary properties of a γ, except that it is unnecessary to examine whether $\varepsilon\overline{\gamma}$ is the square of a number from the field. Such a $\overline{\gamma}$ is usually quickly found, since $N(\overline{\gamma})$ may be the square of any odd number.

3. My calculations show that *the method of Cassels gives the correct number of generators for the curve* (6) *within the limits* (8), *except in twelve insoluble cases where his conditions indicate two generators* ($G=2, g=0$), *and in one case where there is one existing generator out of three indicated* ($G=3, g=1$).

The cases with $G=2$, $g=0$ are given by the following table:

A	m	h	Basic unit ε	γ
41	164	6	$329+22\vartheta-30\overline{\vartheta}$	$5+\vartheta$
59	236	6	$1889-695\vartheta+126\overline{\vartheta}$	$5+\vartheta$
116	58	6	$1-8\vartheta+2\vartheta^2$	$33-8\vartheta$
122	61	6	$1-16\vartheta+4\vartheta^2$	$-39+10\vartheta$
158	79	6	$292+95\vartheta-38\vartheta^2$	$20-\vartheta$
226	113	4	$\frac{1}{3}(-645-176\vartheta+64\vartheta^2)^3$	$\gamma_1 = 2+\vartheta$ $\gamma_2 = -4+\vartheta$
242	11^2	2	$1-2\vartheta+\frac{4}{11}\vartheta^2$	$12+\vartheta$
262	131	2	$\frac{1}{3}(268570+44504\,\vartheta-19175\,\vartheta^2)^3$	$-8+3\vartheta$
298	149	2	$\frac{1}{3}(-59780-19027\,\vartheta+5716\,\vartheta^2)^3$	$17-2\vartheta$
302	151	6	$-8545391+1183490\,\vartheta+79108\,\vartheta^2$	$8-\vartheta$
326	163	3	$-86984-122421\,\vartheta+25326\,\vartheta^2$	$\gamma_0 = -23+8\vartheta$
332	166	6	$1-242\vartheta+44\vartheta^2$	$17+2\vartheta$

The only case with $m\equiv\pm1 \pmod 9$ is $m=163$, where $[\gamma_0]=\mathfrak{p}_{89}^2\,\mathfrak{r}\mathfrak{s}$. The class-group for $m=113$ is non-cyclic, with two generators of order 2, giving $2^3=8$ *a priori* possible values μ. Of these, however, the 4 combinations containing γ_1 are excluded, while the other 4 combinations are possible for all moduli. In the remaining cases of the table, $2\|h$ and $m\not\equiv\pm1 \pmod 9$, that is $2^2=4$ *a priori* values μ, which turn out to be possible for all moduli when checked by Cassels' conditions. On the other hand, the values of A in the table all represent *insoluble* equations (6).

The one case with $G=3$, $g=1$ is

$$A = 428, \quad m = 214, \quad h = 12 \quad \text{(non-cyclic)},$$
$$\varepsilon = 1-54\vartheta+9\vartheta^2, \quad \gamma_1 = -7+2\vartheta, \quad \gamma_2 = 33-2\vartheta\,.$$

All combinations of ε, γ_1 and γ_2 satisfy the condition 2) of Section 2.

From the solution of (6) for $A=428$ (cf. [3, Table 6]), we find the one basic solution

$$\xi = 12, \quad \eta = 218$$

of the corresponding equation (1):

$$\eta^2 = \xi^3 + 214^2 .$$

It is easily seen that this solution results from the choice $\mu=\varepsilon\gamma_2$. The remaining combinations of ε, γ_1 and γ_2, although possible for all moduli, lead to *insoluble* equations (2).

To get some more examples of the case $G=3$, $g=1$, I have examined several values of A beyond the limits (8) such that

$$A \equiv \pm 2, \text{ that is, } m \equiv \mp 1 \pmod 9; \quad g = 1 . \tag{10}$$

If then the class-number h is *even*, there are at least three *a priori* possible generators, which might "survive" the first descent. (There are four such cases within the limits (8), but in all of them Cassels' conditions reduce the number of generators to the correct value 1.)

I first examined the *odd* values of A between 100 and 200 and satisfying (10), but found only odd class-numbers. I then turned to the *even* values of $A>500$. These are not included in the tables of [3], but the methods of that paper lead to a quick determination of the first values of $A>500$ and satisfying (10). The smallest such value with an even class-number did indeed furnish the example I was seeking:

$$A = 718, \; g = 1; \quad m = 359 \equiv -1 \pmod 9, \; h = 2 ,$$

$$\varepsilon = 21429905112 + 2136031295\,\vartheta - 724797018\,\vartheta^2 ,$$

$$\gamma = 12-\vartheta, \quad \gamma_0 = -28+\vartheta^2 .$$

All combinations of ε, γ and γ_0 are possible mod 4, and those containing γ_0 also mod 3.

The solubility of the corresponding equation (6):

$$X^3+Y^3 = 718\,Z^3 = 2\cdot 359\,Z^3 \tag{11}$$

is determined by the one equation

$$x^3+2y^3+359\,z^3 = 0 .$$

This is clearly satisfied by

$$x = 7, \quad y = 2, \quad z = -1 ,$$

with the corresponding values

$$X = 5767471, \quad Y = -3797279, \quad Z = 575834$$

(cf. [3, Theorem I]). This is the one basic solution of (11).

The corresponding solution of the equation (1):

$$\eta^2 = \xi^3 + 359^2$$

is given by

$$\xi = -28, \quad \eta = 327,$$

and will obviously result from the choice $\mu = \gamma_0$. The remaining combinations of ε, γ and γ_0 lead to insoluble equations (2).

REFERENCES

1. J. W. S. Cassels, *The rational solutions of the diophantine equation* $Y^2 = X^3 - D$, Acta Math. 82 (1950), 243–273.
2. J. W. S. Cassels, *The rational solutions of the diophantine equation* $Y^2 = X^3 - D$. *Addenda and Corrigenda*, Acta Math. 84 (1951), 299.
3. E. S. Selmer, *The diophantine equation* $ax^3 + by^3 + cz^3 = 0$, Acta Math. 85 (1951), 203–362.
4. E. S. Selmer, *The diophantine equation* $ax^3 + by^3 + cz^3 = 0$. *Completion of the tables*, Acta Math. 92 (1954), 191–197.
5. E. S. Selmer, *A conjecture concerning rational points on cubic curves*, Math. Scand. 2 (1954), 49–54.
6. E. S. Selmer, *Tables for the purely cubic field* $K(\sqrt[3]{m})$, Submitted for publication to Norske Vid. Akad., Oslo.
7. E. S. Selmer, *On Cassels' conditions for rational solubility of the diophantine equation* $\eta^2 = \xi^3 - D$, Submitted for publication in the Archiv for Math. og Naturvid.

UNIVERSITY OF OSLO, NORWAY