MATH. SCAND. 4 (1956), 281–286

THE RATIONAL SOLUTIONS OF THE DIOPHANTINE EQUATION $\eta^2 = \xi^3 - D$ FOR $|D| \leqq 100$

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 a set of necessary congruence conditions for solubility. I have later [6] extended and completed these conditions. Cassels also gives a table of solutions of infinite order for all $|D| \leqq 50$. Within these limits, the congruence conditions turn out to be *sufficient* for solubility of (1). (This is not always the case, cf. my counterexamples [5].)

Cassels works in the purely *cubic* field $K(D^{\frac{1}{3}})$. Shortly before Cassels' paper appeared, Podsypanin [4] had published a study of the equation (1) in the *quadratic* field $K((-D)^{\frac{1}{2}})$, together with a table of basic solutions for $|D| \leqq 89$. In an addendum [2], Cassels pointed out several errors for $|D| \leqq 50$ in Podsypanin's table.

The rational solutions of (1) correspond to the integer solutions of

$$y^2 = x^3 - Dt^6\,, \tag{2}$$

with $\xi = x/t^2$, $\eta = y/t^3$, $(x, t) = (y, t) = 1$. By combining the tables of Cassels and Podsypanin, and adding some new solutions, I have constructed a table for the equation (2) for $|D| \leqq 100$, appearing below.

2. In my table, the number of solutions given for each D represents the number of *generators* (basic solutions) of *infinite* order; this number does not exceed 2 for $|D| \leqq 100$. As in Cassels' paper, I have not really checked the basic character of the solutions. This could be done, but involves a considerable amount of computation (cf. Cassels' Lemma 11). However, I have checked by Cassels' methods that no solution of the table is the *duplication* of another solution. In the case of two generators, of elliptic parameters u_1 and u_2, it is also verified that $u_1 - u_2$ gives no duplication. In addition to this check (also performed by Cassels for

Received June 1, 1956.

$|D| \leqq 50$), I have used Podsypanin's methods (cf. below) to verify that no solution, including u_1+u_2 and u_1-u_2 for two generators, is a *triplication*.

For several values of D, many solutions are known. In particular, all presently known *integer* solutions of (1) for $|D| \leqq 100$ are listed by Hemer [3]. In such cases, I have also checked that these solutions can all be expressed (as linear combinations of elliptic parameters) in terms of the solutions in my table. I would be very surprised if my solutions were not all fundamental.

The numbers of generators for $50 < |D| \leqq 100$ were found by means of Cassels' conditions, which turned out to be *sufficient within these limits.* The required class-numbers h and units ε of the corresponding cubic fields $K(D^{\frac{1}{3}}) = K(\delta)$ were taken from my table [7]. This does not contain the values of γ (in Cassels' notation) for even h. Since the actual cases all have $2\|h$ ("exactly divides"), essentially only one γ occurs, given by the following table (for cubefree D only):

D	h	γ	D	h	γ	D	h	γ
57	6	$-2+\delta$	65	18	$14+\delta$	79	6	$20-\delta$
58	6	$33-8\delta$	66	6	$1+4\delta$	83	2	$33-4\delta$
61	6	$-39+10\delta$	67	6	$10+3\delta$	89	2	$-4+\delta$
63	6	$9-2\delta$	76	6	$-3+\delta$			

As in the corresponding table of Cassels for $D \leqq 50$, the γ's are chosen as quadratic residues of 4 whenever ε is not such a residue.

3. Podsypanin's methods are based on the well-known birational connection between the equations

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

$$\eta_1^2 = \xi_1^3 + 27D\,. \tag{4}$$

A rational solution of (3) is said to be *generable* if and only if it can be derived from a solution of (4). The necessary and sufficient condition for this is that

$$\eta + (-D)^{\frac{1}{2}} = \alpha^3, \qquad \alpha \in K\big((-D)^{\frac{1}{2}}\big)\,. \tag{5}$$

To verify that a solution is *non*-generable, the equation (5) must be shown impossible modulo some prime $p = 3h+1$ such that p factorizes in $K\big((-D)^{\frac{1}{2}}\big)$, i.e. such that the congruence

$$d^2 + D \equiv 0 \pmod p$$

is soluble. The equation (5) is then impossible if $\eta+d$ is a *cubic non-residue* of p.

No new information is obtained by using both signs of d, since

$$(\eta+d)(\eta-d) = \eta^2-d^2 \equiv \eta^2+D = \xi^3 \pmod{p} .$$

The factors of the left hand side are consequently both cubic residues or both non-residues of p.

Since -3 is a quadratic residue of all primes $p=3h+1$, *the same primes* p will factorize in both fields $K((-D)^{\frac{1}{2}})$ and $K((27D)^{\frac{1}{2}})$, corresponding to the equations (3) and (4) respectively.

As in Podsypanin's table, I indicate for each solution whether it is generable (g) or non-generable (n). In the case of two generators, one of each type, no further problems arise (but it was in some cases, for $D=-15$, -24, -37, 39, necessary to replace a (n)-solution in Cassels' table by a usually more complicated (g)-solution). However, if both solutions are of the same type, say (n), it must also be shown that their sum and difference (in terms of elliptic parameters) are non-generable. For two (g)-solutions, the same check must be performed on the generating solutions.—Since the transformation from (n)- to (g)-solutions corresponds to multiplication of elliptic arguments by $(-3)^{\frac{1}{2}}$, we also get the check on *triplications* mentioned earlier.

4. Cassels' table for $|D|\leqq 50$ is error-free, whereas Podsypanin's table must be characterized as extremely inaccurate. It contains in all 26 errors:

(i) No generators are given for $D=\pm 43$, 50, 51, 57, -67, -68, -69, 75, 84, and insufficient generators for $D=-15$, 39, 83.

(ii) For $D=-28$, Podsypanin's solution $(-3, 1, 1)$ is the duplication of (2, 6, 1). For $D=48$, his second solution is the triplication of the first one. For $D=67$, his first solution is the duplication of (17, 25, 2). For $D=-80$, the first solution is the duplication and the second one the triplication of (4, 12, 1).

(iii) Incorrect values (including sign) of x or y occur in the cases $D=-63$, 66, -76, -77, 89.

(iv) For $D=11$, all solutions are generable. There is one solution of each type for $D=-24$. For $D=26$, the (g)-solution is Cassels', not Podsypanin's second solution. The solution for $D=29$ is generable.

The errors for $D=-15$, 39, ± 43, 48, 50 (but not the duplication for $D=-28$) were also pointed out by Cassels [2].—In addition to the above corrections, I have replaced one of Podsypanin's (correct) solutions by a simpler one for $D=11$ (Cassels), -37, -65, -89. On the other hand, Podsypanin's simpler first solution has replaced the corresponding one of Cassels for $D=47$.

Solutions of $y^2 = x^3 - Dt^6$ of infinite order.

D	(x, y, t)	
2	(3, 5, 1)	*g*
4	(2, 2, 1)	*g*
7	(2, 1, 1)	*n*
11	(3, 4, 1)	*g*
,,	(15, 58, 1)	*g*
13	(17, 70, 1)	*g*
15	(4, 7, 1)	*n*
18	(3, 3, 1)	*n*
19	(7, 18, 1)	*g*
20	(6, 14, 1)	*g*
21	(37, 188, 3)	*g*
22	(71, 119, 5)	*g*
23	(3, 2, 1)	*n*
25	(5, 10, 1)	*n*
26	(3, 1, 1)	*n*
,,	(35, 207, 1)	*g*
28	(4, 6, 1)	*n*
29	(3 133, 175 364, 3)	*g*
30	(31, 89, 3)	*g*
35	(11, 36, 1)	*g*
38	(4 447, 291 005, 21)	*g*
39	(4, 5, 1)	*n*
,,	(43, 226, 3)	*g*
40	(14, 52, 1)	*g*
43	(1 177, 40 355, 6)	*g*
44	(5, 9, 1)	*g*
45	(21, 96, 1)	*n*
47	(6, 13, 1)	*n*
,,	(63, 500, 1)	*g*
48	(4, 4, 1)	*n*
49	(65, 524, 1)	*g*
50	(211, 3 059, 3)	*g*
51	(1 375, 50 986, 3)	*g*
53	(9, 26, 1)	*n*
,,	(4 481, 299 871, 10)	*g*
54	(7, 17, 1)	*g*
55	(4, 3, 1)	*n*
56	(18, 76, 1)	*g*
57	(4 873, 340 165, 6)	*g*
58	(5 393, 387 655, 22)	*g*
59	(6 715, 545 644, 21)	*g*
60	(4, 2, 1)	*n*
61	(5, 8, 1)	*n*
,,	(8 785, 680 698, 39)	*g*
63	(4, 1, 1)	*n*
65	(32 049, 2 573 303, 86)	*g*
66	(357 361, 213 574 985, 84)	*g*
67	(17, 25, 2)	*g*
,,	(23, 110, 1)	*g*
71	(8, 21, 1)	*n*
72	(6, 12, 1)	*n*
74	(99, 985, 1)	*g*
75	(91, 836, 3)	*g*
76	(5, 7, 1)	*g*
,,	(101, 1 015, 1)	*g*
79	(20, 89, 1)	*n*
81	(13, 46, 1)	*g*
83	(27, 140, 1)	*g*
,,	(33, 175, 2)	*g*
84	(46, 190, 3)	*g*
85	(1 552 601, 1 934 117 206, 167)	*g*
87	(7, 16, 1)	*n*
89	(5, 6, 1)	*n*
,,	(233, 1 476, 7)	*g*
91	(25, 99, 2)	*g*
93	(1 249, 29 818, 15)	*g*
94	(11 614 031, 24 303 384 785, 1 477)	*g*
95	(6, 11, 1)	*n*
100	(10, 30, 1)	*n*

Solutions of $y^2=x^3-Dt^6$ of infinite order.

D	(x, y, t)		D	(x, y, t)	
−2	(−1, 1, 1)	*n*	−54	(3, 9, 1)	*n*
−3	(1, 2, 1)	*n*	−55	(9, 28, 1)	*n*
−5	(−1, 2, 1)	*g*	−56	(2, 8, 1)	*n*
−8	(2, 4, 1)	*n*	−57	(7, 20, 1)	*n*
−9	(−2, 1, 1)	*n*	,,	(−2, 7, 1)	*n*
−10	(−1, 3, 1)	*n*	−58	(241, 4 087, 6)	*n*
−11	(−7, 19, 2)	*n*	−61	(−15, 23, 2)	*g*
−12	(−2, 2, 1)	*n*	−62	(1, 63, 2)	*n*
−15	(1, 4, 1)	*n*	−63	(1, 8, 1)	*n*
,,	(−11, 98, 3)	*g*	,,	(−3, 6, 1)	*n*
−17	(−1, 4, 1)	*n*	−65	(−1, 8, 1)	*n*
,,	(−2, 3, 1)	*n*	,,	(−4, 1, 1)	*n*
−18	(7, 19, 1)	*n*	−66	(1, 65, 2)	*n*
−19	(5, 12, 1)	*n*	−67	(49, 1 801, 6)	*n*
−22	(3, 7, 1)	*n*	−68	(−4, 2, 1)	*n*
−24	(−2, 4, 1)	*n*	−69	(−5, 224, 3)	*g*
,,	(−23, 73, 3)	*g*	−71	(5, 14, 1)	*n*
−26	(−1, 5, 1)	*n*	−72	(−2, 8, 1)	*n*
−28	(2, 6, 1)	*n*	−73	(3, 10, 1)	*n*
−30	(19, 83, 1)	*n*	,,	(2, 9, 1)	*n*
−31	(−3, 2, 1)	*n*	−74	(7, 233, 3)	*n*
−33	(−2, 5, 1)	*n*	−76	(−3, 7, 1)	*n*
−35	(1, 6, 1)	*n*	−77	(−61, 988, 5)	*g*
−36	(−3, 3, 1)	*n*	−79	(45, 302, 1)	*n*
−37	(−1, 6, 1)	*n*	,,	(−6 335, 154 088, 39)	*g*
,,	(−7, 45, 2)	*g*	−80	(4, 12, 1)	*n*
−38	(11, 37, 1)	*n*	−82	(−1, 9, 1)	*n*
−39	(217, 3 197, 2)	*n*	−83	(2 641, 135 737, 6)	*n*
−40	(6, 16, 1)	*n*	−89	(−4, 5, 1)	*n*
−41	(2, 7, 1)	*n*	,,	(−2, 9, 1)	*n*
−43	(−3, 4, 1)	*n*	−91	(−3, 8, 1)	*n*
,,	(57, 2 290, 7)	*g*	−92	(2, 10, 1)	*n*
−44	(−2, 6, 1)	*n*	−94	(3, 11, 1)	*n*
−46	(−7, 51, 2)	*n*	−97	(18, 77, 1)	*n*
−47	(17, 89, 2)	*n*	−98	(7, 21, 1)	*n*
−48	(1, 7, 1)	*n*	−99	(1, 10, 1)	*n*
−50	(−1, 7, 1)	*g*	−100	(−4, 6, 1)	*n*
−52	(−3, 5, 1)	*g*			

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. O. Hemer, *Notes on the diophantine equation* $y^2 - k = x^3$, Arkiv för Mat. 3 (No. 3, 1954), 67–77.
4. V. Podsypanin, *On the indeterminate equation* $x^3 = y^2 + Az^6$, Mat. Sbornik N. S. 24 (1949), 391–403. (In Russian.)
5. E. S. Selmer, *The diophantine equation* $\eta^2 = \xi^3 - D$. *A note on Cassels' method*, Math. Scand. 3 (1955), 68–74.
6. E. S. Selmer, *On Cassels' conditions for rational solubility of the diophantine equation* $\eta^2 = \xi^3 - D$, Archiv for Math. og Naturv. 53 (No. 7, 1956), 1–23.
7. E. S. Selmer, *Tables for the purely cubic field* $K(\sqrt[3]{m})$, Avh. Norske Vid. Akad. Oslo. I. 1955, No. 5, 1–32.

UNIVERSITY OF OSLO, NORWAY