MATH. SCAND. 2 (1954), 49–54

A CONJECTURE CONCERNING RATIONAL POINTS ON CUBIC CURVES

ERNST S. SELMER

1. In a previous paper [2], I have studied the cubic curve

$$X^3+Y^3=AZ^3\,, \tag{1}$$

giving the number of generators and the basic rational solutions for nearly all positive (cube-free) integers $A \leqq 500$. The extensive tables contain a few blank spaces, where no solution had been found when [2] was written.

I have later had the opportunity to run my unsolved equations on the electronic computer at the Institute for Advanced Study in Princeton, N. J. With two exceptions, mentioned in section 4 below, the machine found solutions of all my unsolved equations. The numerical results will be published elsewhere [3].

2. It will be useful to repeat shortly the methods for treating (1). We operate in the quadratic field $K(\varrho) = K(e^{2\pi i/3})$, where the left-hand side factorizes. This "*first descent*" takes two different forms:

Type I leads to equations

$$ax^3+by^3+cz^3=0\,, \qquad abc=A\,, \tag{2}$$

where we may assume

$$1 \leqq a < b < c\,, \qquad (a,b)=(a,c)=(b,c)=1\,.$$

Type II leads to equations

$$bu^3+3(a-b)u^2v-3auv^2+bv^3=3A_1w^3\,, \tag{3}$$

$$A_1(a^2-ab+b^2)=A\,,$$

where we may assume

$$b>0\,, \qquad (a,b)=1\,,$$

and where conjugate values $a+b\varrho$ and $a+b\varrho^2=-(b-a+b\varrho)$ are not considered separately.

Received May 11, 1954.

Type I is always *a priori* possible if A (cube-free) contains at least two different prime factors. Type II, however, is only a priori possible with $a \neq 0$ if A contains prime factors $\equiv +1 \pmod 3$, which are the only primes $\neq 3$ contained in a form $a^2 - ab + b^2$. With $a = 0$, $b = 1$, type II is also a priori possible if A is a product of primes $\equiv \pm 1 \pmod 9$, or 9 times such a product.

A solution of (2) or (3) will always lead to a solution of (1), and all solutions of (1) (except the so called "triplications") are generated in this way. *The exclusions of the first descent* are obtained by applying elementary congruence conditions to (2) and (3). The remaining equations (if any), *possible for all moduli*, are then treated by means of a "*second descent*", which also takes two different forms:

For type I, we multiply (2) by a^2 and replace ax by $-x$ to get an equation

$$x^3 - my^3 = nz^3 ,$$

where the left-hand side factorizes in the purely cubic field $K(m^{1/3})$. This descent leads to new and stronger congruence conditions, which can be used for further exclusions.

Type II is treated similarly, in the non-purely cubic field defined by the left-hand side of (3).

3. The number of *possible* equations (for all moduli) of the type (2) or (3) is of the form

$$N_1 = \tfrac{1}{2}(3^{G_1} - 1) \quad \text{or} \quad N_2 = \tfrac{1}{2}(3^{G_2} - 1),$$

respectively, that is $N = 0, 1, 4, 13, 40, \ldots$ for $G = 0, 1, 2, 3, 4, \ldots$. The number of *soluble* equations is also of the same form:

$$n_1 = \tfrac{1}{2}(3^{g_1} - 1) \quad \text{or} \quad n_2 = \tfrac{1}{2}(3^{g_2} - 1) ,$$

where of course $g_1 \leqq G_1$, $g_2 \leqq G_2$. Here

$$g = g_1 + g_2$$

is *the number of generators (basic solutions) of infinite order for the equation* $X^3 + Y^3 = AZ^3$.

Without exception, my numerical calculations have shown the following properties of the second descent (cf. [2, Ch. VII, § 4, and Ch. IX, § 14, the concluding remarks]):

When $N = 1$, the one possible equation can not be excluded by the second descent. When $N = 4$, none or all four equations are excluded. When $N = 13$, none or twelve equations are excluded.

This holds for the types I and II *separately* (I have no simultaneous

exclusions of the two types within my tables, and no case with $N_2 = 13$). I stated in [2] that we always seem to get 12 exclusions when $N_1 = 13$, but later on I discovered several values of A which give rise to 13 possible and *soluble* equations (2), cf. [3].

The above results may be given in condensed form: *When the first descent indicates at most three generators, then none or two of these seem to be excluded by the second descent.*

To get cases also with $N > 13$, I have recently examined the two values $A = 5610 = 2 \cdot 3 \cdot 5 \cdot 11 \cdot 17$ and $A = 11220 = 2^2 \cdot 3 \cdot 5 \cdot 11 \cdot 17$, both giving rise to 40 possible equations (2) (but no equation (3)). For the latter value of A, there are 36 excluded and 4 soluble equations, that is two excluded generators. For $A = 5610$, however, all 40 equations, that is *four generators*, are excluded by the second descent. I therefore feel justified in formulating the following

CONJECTURE (*weaker form*): *The second descent excludes an even number of generators.*

The word "weaker" refers to the fact that nothing is said about actual *solubility* of the non-excluded equations. The conjecture is only a statement on the strength of the congruence conditions resulting from the second descent.

4. The problem of *sufficient* conditions for solubility seems to be extremely difficult. After [2] was written, I have discovered some cases where the conditions of my second descent turn out to be *insufficient.* Details will be given in [3], and I shall only state the results here.

The equation (1) is rationally equivalent to the Weierstrass normal form

$$\eta^2 = 4\xi^3 - 27A^2 ,$$

which can be treated by the methods of *Cassels* [1] in the purely cubic field defined by the right-hand side. I have earlier (cf. [2, Ch. I, § 6]) used the above equivalence to show the *insufficiency* of Cassels' conditions in some cases. On the other hand, his methods imply that my conditions of the second descent are insufficient for the values

$$A = 473 = 11 \cdot 43 \quad \text{and} \quad A = 1886 = 2 \cdot 23 \cdot 41 ,$$

which can be shown insoluble by Cassels' methods. (The latter value results from the unsolved equation $x^3 + 41y^3 + 46z^3 = 0$ in Table 2^a of [2].) In both cases, my methods indicate *two* generators:

For $A = 473$, there is one possible equation of *each* type (2) and (3), and these equations are not excluded by the second descent.—Another

example of the same kind is $A = 508 = 2^2 \cdot 127$ (the first value of $A > 500$ where my methods fail).

For $A = 1886$, there are four possible equations (2), all of which "survive" the second descent.

Considering the above conjecture, it is striking that my methods fail to indicate the loss of an *even* number of generators. This has led me to formulate a similar

CONJECTURE (*stronger form*): *When a second descent exists, the number of generators is an even number less than what is indicated by the first descent.*

This form is stronger, since it implies actual *solubility* when the first descent indicates an *odd* number of generators.—If my conditions of the second descent had been sufficient, the weaker and stronger forms of the conjecture would of course have been equivalent.

The cases $A = 473$ and $A = 508$, where one generator from each type of descent was lost, show that the stronger conjecture can be valid only for the *total* number of generators. The types I and II must no longer be considered separately.

5. The real importance of the stronger conjecture stems from the fact that it seems to hold (at least in certain cases) *also for the Weierstrass normal form*

$$\eta^2 = \xi^3 - C\xi - D\,.$$

We must first show that *a second descent is really possible.*—It is well known how the *first* descent is performed: The rational solutions (ξ, η) correspond to the integer solutions (x, y, t) of

$$y^2 = x^3 - Cxt^4 - Dt^6 = N(x - t^2\theta)\,, \tag{4}$$

where the norm refers to the cubic field $K(\theta)$ defined by

$$\theta^3 - C\theta - D = 0 \tag{5}$$

(here assumed *irreducible*, to simplify the arguments). This leads to one or more ideal-equations

$$[x - t^2\theta] = \mathfrak{m}\mathfrak{a}^2\,,$$

where $\mathfrak{m}$ is an ideal from a finite set. This equation can sometimes be proved insoluble by class-number considerations, but will otherwise lead to a finite number of equations between integers of $K(\theta)$:

$$x - t^2\theta = \mu\alpha^2 = (e + f\theta + g\theta^2)(u + v\theta + w\theta^2)^2\,. \tag{6}$$

The coefficients of μ (known) and α (unknown) are rational numbers, and their common denominator must divide the discriminant of the equation (5).

A solution (u, v, w) of (6) must satisfy certain congruence conditions, which can be found by examining *the quadratic residues in the cubic field* $K(\theta)$ (cf. Cassels' treatment [1] of the case $C = 0$). The exclusions of the first descent are obtained from these conditions, and the remaining equations (6) (if any) are *possible for all moduli.*

Multiplying out the right-hand side of (6), and equating the coefficients of θ and θ^2 to $-t^2$ and 0, respectively, we get two simultaneous "*resulting equations*"

$$f_2(u, v, w) = t^2 , \qquad g_2(u, v, w) = 0 , \tag{7}$$

with quadratic forms f_2 and g_2. These equations are also possible for all moduli, and it is clear that they are soluble in real numbers (since this is the case for the original equation (4)). Both equations (7) are consequently *separately soluble*, but this does not necessarily imply a *common* solution.

Ordinary elimination of one of the unknowns u, v or w in (7) will result in one homogeneous ternary quartic equation, to which a further descent is at least very difficult to apply. But since $g_2(u, v, w) = 0$ is soluble, we can express the solutions u, v and w as rational quadratic forms in two parameters r and s. Substituting this in the first equation (7), we get

$$t^2 = F_4(r, s) ,$$

where F_4 is a rational quartic form. This equation represents a curve of genus one, and we can apply a *second descent* in the quartic field defined by the right-hand side. The calculations involved may be very laborious, but the theoretical possibility of a second descent is in itself of great interest.

6. To verify the first, weaker conjecture for the Weierstrass normal form, one must actually carry through the cumbersome calculations of the second descent. The *stronger* conjecture, however, is often more easily verified, namely when there are *two different methods* of treating the same equation. If one method shows insolubility of a given equation, and the *first* descent of another method indicates a number $g > 0$ of generators, then the stronger conjecture is verified for the latter method if g is *even*. Similarly, we can get a verification if the two methods indicate different numbers > 0 of generators (and the smaller number is attained by numerical computations).

I have already explained how Cassels' methods show the insufficiency of my conditions in some cases, which led to the formulation of the stronger conjecture. On the other hand, I can check Cassels' conditions by my

methods in many cases, and these calculations all *verify the stronger conjecture.* The results will be submitted for later publication in the Mathematica Scandinavica.

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. E. S. Selmer, *The diophantine equation* $ax^3 + by^3 + cz^3 = 0$, Acta Math. 85 (1951), 203–362.
3. E. S. Selmer, *The diophantine equation* $ax^3 + by^3 + cz^3 = 0$. *Completion of the tables,* Submitted for publication in the Acta Mathematica.

UNIVERSITY OF OSLO, NORWAY