MATH. SCAND. 1 (1953)

SUFFICIENT CONGRUENCE CONDITIONS FOR THE EXISTENCE OF RATIONAL POINTS ON CERTAIN CUBIC SURFACES

ERNST S. SELMER

1. It is well known that the elementary congruence conditions (e.c.c.) —together with solubility in real numbers—are sufficient for the solubility in integers of a homogeneous quadratic equation in any number of variables. In the cubic case, however, sufficient solubility conditions are much more difficult to establish. I have recently [3] shown the *insufficiency* of the e.c.c. for homogeneous ternary cubic equations, i.e. for the existence of rational points on cubic curves.

In the case of homogeneous cubic equations in four variables (surfaces), it is known that the existence of *one* rational point implies that there is an infinity of such points. Mordell [2] has conjectured that the e.c.c. are *sufficient* for solubility in this case.

I shall prove Mordell's conjecture for the purely cubic equation

$$a_1x_1^3+a_2x_2^3+a_3x_3^3+a_4x_4^3 = 0, \quad a_1a_2a_3a_4 \neq 0\,, \tag{1.1}$$

satisfying the additional condition that (for instance)

$$\frac{a_3a_4}{a_1a_2} = \text{a rational cube.} \tag{1.2}$$

My method does not apply to the general case (1.1), but numerical evidence indicates that Mordell's conjecture still holds.

I shall finally show how the method can be extended to prove the conjecture for the more general equation

$$f_3(x, y) = n \cdot f_3(u, v)\,, \tag{1.3}$$

where f_3 is an arbitrary binary cubic form.

Received April 14, 1953.

The results of this paper were first presented by the author at a meeting of the Amer. Math. Soc. in Pasadena, Calif., on Dec. 1, 1951. A preliminary report is contained in Bull. Amer. Math. Soc. 58 (1952), 64–65.

2. We may suppose that the coefficients of (1.1) are *cubefree* integers, and that

$$(a_1, a_2, a_3) = (a_1, a_2, a_4) = (a_1, a_3, a_4) = (a_2, a_3, a_4) = 1 .$$

The only equations which can be shown insoluble by e.c.c. are then typified by one of the following combinations (arbitrary signs):

$$(2.1)\qquad \left\{\begin{array}{ll} a_1 \equiv 0,\ a_2 \equiv \pm 1,\ a_3 \equiv \pm 2,\ a_4 \equiv \pm 4 \pmod 9 & \\ a_1 = r^i a_1',\ a_2 = r^{3-i} a_2',\ \dfrac{a_3}{a_4}(N)r, \text{ or} & i = 1 \text{ or } 2, \\ a_1 = r^i a_1',\ a_2 = r^i a_2',\ \dfrac{a_1'}{a_2'} \text{ and } \dfrac{a_3}{a_4}(N)r & r \nmid a_1' a_2' . \end{array}\right.$$

Here $r \equiv +1 \pmod 3$ is a prime, for which (N) denotes cubic non-residuacity in rational numbers (with the notation of [3], Ch. II, § 1).

The equation (1.1) can be written as

$$x_1^3 + \left(\frac{a_3 a_4}{a_1 a_2}\right) \cdot \frac{a_2}{a_4} x_3^3 + \frac{a_4}{a_1}\left(x_4^3 + \frac{a_2}{a_4} x_2^3\right) = 0 .$$

If (1.2) is satisfied, we can therefore transform the equation into

$$(2.2)\qquad x^3 + my^3 = n(u^3 + mv^3)$$

with integer, cubefree m and n (but not necessarily $(m, n) = 1$). We shall first prove Mordell's conjecture for this equation.

The e.c.c. for solubility of (2.2) are given by:

$$(2.3)\qquad m(R)r \text{ if } r \mid n,\ r \nmid m$$

$$(2.4)\qquad n(R)r \text{ if } r \mid m,\ r \nmid n$$

$$(2.5)\qquad m'n'(R)r \text{ if } m = r^i m',\ n = r^{3-i} n' \qquad i = 1 \text{ or } 2,$$

$$(2.6)\qquad \frac{m'}{n'}(R)r \text{ if } m = r^i m',\ n = r^i n' \qquad r \nmid m'n'.$$

Here (R) denotes cubic residuacity. There are no conditions mod 9, since the first combination of (2.1) is inconsistent with (1.2).

We note that the equation (2.2) is really *symmetric* in m and n, which consequently may be interchanged in the arguments below.

3. We shall treat (2.2) in the purely cubic field $K(m^{1/3}) = K(\vartheta)$. Because of the condition (2.3), the natural primes dividing n will all *factorize* in this field (cf. [3], Ch. III, § 1).

We consider the ideal equation

$$(3.1)\qquad [x + y\vartheta] = \mathfrak{n} \cdot [u + v\vartheta] ,$$

where $\mathfrak{n}$ is a product of ideal factors such that $N(\mathfrak{n}) = n$. The equation

implies that $\mathfrak{n}$ must be *principal*, and is in fact easily solved if we can find such an ideal:

$$\mathfrak{n} = [e+f\vartheta+g\vartheta^2], \tag{3.2}$$

i.e.

$$N(\mathfrak{n}) = e^3+mf^3+m^2g^3-3mefg = n\ . \tag{3.3}$$

We may choose $u = f$, $v = -g$, so that the term with ϑ^2 disappears in the product

$$(e+f\vartheta+g\vartheta^2)(f-g\vartheta) = ef-mg^2+(f^2-eg)\vartheta\ .$$

A solution of (3.1), and thereby of (2.2), is then clearly given by

$$x = ef-mg^2,\ y = f^2-eg,\ u = f,\ v = -g\ . \tag{3.4}$$

If the ideal $\mathfrak{n}$ is *non-principal*, the method still works if the class-number h_m is *prime to* 3. We can then always find an ideal $\mathfrak{d}$ such that $\mathfrak{n}\mathfrak{d}^3$ is principal,

$$\mathfrak{n}\mathfrak{d}^3 = [e+f\vartheta+g\vartheta^2], \text{ where } N(\mathfrak{n}\mathfrak{d}^3) = nd^3$$

(an "auxiliary cube", cf. [3], Ch. 3, § 7). The only consequence for the solution of (2.2) is a factor d in the expressions (3.4) for u and v.

When $3|h_m$, however, the case is more complicated.

4. We first note that the $\mathfrak{n}$ of (3.2) may be a *fractional* ideal:

$$\mathfrak{n} = \left[\frac{X+Y\vartheta+Z\vartheta^2}{U+V\vartheta+W\vartheta^2}\right] = \left[\frac{\eta}{\delta}\right], \tag{4.1}$$

i.e.

$$X^3+mY^3+m^2Z^3-3mXYZ = n(U^3+mV^3+m^2W^3-3mUVW). \tag{4.2}$$

We can come back to (3.2) if we multiply numerator and denominator of (4.1) by the *conjugate* of the denominator, which is then replaced by the rational integer $N(\delta) = d$. This will only have the same effect as the auxiliary cube mentioned in section 3.

An equivalent approach, but involving less calculations, is the following: Find a number $\alpha = a+b\vartheta+c\vartheta^2$ such that the terms with ϑ^2 disappear in both products

$$\begin{cases} \alpha\eta = \underbrace{aX+mcY+mbZ}_{x} + \underbrace{(bX+aY+mcZ)}_{y}\vartheta + \underbrace{(cX+bY+aZ)}_{0}\vartheta^2 \\ \alpha\delta = \underbrace{aU+mcV+mbW}_{u} + \underbrace{(bU+aV+mcW)}_{v}\vartheta + \underbrace{(cU+bV+aW)}_{0}\vartheta^2. \end{cases} \tag{4.3}$$

As indicated, we then get a solution (x, y, u, v) of (3.1), and thereby of (2.2).

The two linear, homogeneous equations for a, b, and c have the solution

$$a = XV - YU,\ b = ZU - XW,\ c = YW - ZV\ . \tag{4.4}$$

We get $\alpha = 0$ only when η and δ have proportional coefficients, i.e. if n is a rational cube. In this case, however, the equation (2.2) is trivially soluble with $y = v = 0$.

Substituting (4.4) in (4.3), we get x, y, u, and v expressed as *rational cubic forms* in X, Y, Z, U, V, and W. Since clearly a solution of (2.2) is also a solution of (4.2), we see that *these two equations are simultaneously soluble or insoluble.*

5. We now return to the case when $3|h_m$. Let us first assume that $h_m = 3$, resulting from one (and only one) prime factor $r \equiv +1 \pmod 3$ of m. Let generally $\mathfrak{a}$ denote an ideal such that $N(\mathfrak{a}) = a$, and let Π be the class of principal ideals. It is easily seen that

$$\text{if } r|m,\ r \nmid a, \text{ then } a(R)r \rightleftarrows \mathfrak{a} \in \Pi\ . \tag{5.1}$$

Proof: It follows from (3.2–3) (the term e^3) that the norm of a principal ideal is always a cubic residue of r. If two ideals $\mathfrak{a}_1$ and $\mathfrak{a}_2$ belong to the same class, then $\mathfrak{a}_1/\mathfrak{a}_2$ is principal, and consequently

$$\frac{N(\mathfrak{a}_1)}{N(\mathfrak{a}_2)} = \frac{a_1}{a_2}\,(R)r\ .$$

The norms of all ideals in one class do therefore belong to the same "cubic residuacity class" mod r (cf. [3], p. 216). Since there are three such classes, and three classes of ideals, there must be a *one-one correspondence.*

The possibility of (3.2) now follows immediately from (2.4) if $r \nmid n$. In the case (2.5), we get

$$\mathfrak{m}'\mathfrak{n}' \in \Pi\ \&\ \mathfrak{r}^3 \in \Pi \to \underbrace{\mathfrak{r}^i\mathfrak{m}'}_{\mathfrak{m}=[\vartheta]} \cdot \underbrace{\mathfrak{r}^{3-i}\mathfrak{n}'}_{\mathfrak{n}} \in \Pi \to \mathfrak{n} \in \Pi\ ,$$

and in the case (2.6):

$$\frac{\mathfrak{m}'}{\mathfrak{n}'} \in \Pi \to \frac{\mathfrak{r}^i\mathfrak{m}'}{\mathfrak{r}^i\mathfrak{n}'} = \frac{[\vartheta]}{\mathfrak{n}} \in \Pi \to \mathfrak{n} \in \Pi\ .$$

In all cases, we can therefore find $\mathfrak{n}$ as a *principal* ideal. — If $3\|h_m > 3$ ("exactly divides"), an *auxiliary cube* may be necessary to get a principal ideal.

Let next m contain M different prime factors r, i.e. $3^M|h_m$. If in particular $h_m = 3^M$, we have the following generalization of (5.1):

If $r_i | m$, $r_i \nmid a$, $i = 1, 2, \ldots, M$, then $a(R)$ all $r_i \rightleftarrows \mathfrak{a} \in \Pi$. As above, it is easily concluded that we can always find $\mathfrak{n}$ as a principal ideal if $3^M \| h_m$, possibly with an auxiliary cube if $h_m > 3^M$.

So far, the solubility of (2.2) has been established in all cases. The method fails, however, if

$$3^{M+\Delta} \| h_m \, , \Delta > 0 \, , \tag{5.2}$$

i. e. if the class-number is divisible by a higher power of 3 than can be concluded from the number of prime factors r of m. To illustrate the difficulty, let us consider the simplest case:

$$h = 3, \text{ no prime } r \text{ dividing } m \text{ or } n \, .$$

The class to which the ideal $\mathfrak{n}$ belongs is then uniquely determined, and may well be non-principal, e.g. $\mathfrak{n} \in \Gamma$, where Γ, Γ^2, and $\Gamma^3 = \Pi$ are the three classes of ideals. The only way to establish the solubility of (2.2) is then by an argument of the following kind:

Suppose that we can find a prime r which factorizes in $K(\vartheta)$ (i.e. $m(R)r$), and where the three prime ideal factors of r all belong to *different classes*:

$$[r] = \mathfrak{r}\mathfrak{r}'\mathfrak{r}'', \mathfrak{r} \in \Pi \, , \mathfrak{r}' \in \Gamma, \mathfrak{r}'' \in \Gamma^2 \, . \tag{5.3}$$

(The only alternative is that the factors all belong to the *same* class, principal or not.) We then obtain a *fractional*, principal ideal by (for instance)

$$\mathfrak{n}_1 = \frac{\mathfrak{n}\mathfrak{r}}{\mathfrak{r}'} \in \Pi \, , N(\mathfrak{n}_1) = N(\mathfrak{n}) = n \, .$$

To this ideal, we can apply the methods of section 4, and consequently find a solution of (2.2) also in this case.

The question is: do primes of the type (5.3) always exist? It follows from section 6 below that the answer is affirmative, but I can see no elementary way to prove this statement or the similar, more complicated statements arising from (5.2) with $M > 0$ and/or $\Delta > 1$.

6. To prove Mordell's conjecture for the equation (2.2) in all cases, we can use a deep result of Hasse ([1], with further references): Let K be an algebraic number field, and let Ω be a *cyclic* field over K. A number n in K is then the norm of a (fractional) number in Ω if and only if the congruence

$$N(\xi) \equiv n (\mathrm{mod}\ \mathfrak{m})$$

is soluble with $\xi \in \Omega$ for any modulus $\mathfrak{m} \in K$. — In other words, the congruence conditions are *sufficient* for the solubility of such a norm-equation.

The purely cubic field $K(m^{1/3}) = K(\vartheta)$ is *not* cyclic over the field of rational numbers. We overcome this by choosing $K(\varrho)$ as our basic field, where ϱ is a complex cube root of unity. The resulting field $\Omega(m^{1/3}) = \Omega(\vartheta)$ over $K(\varrho)$ is then cyclic (cf. [3], Ch. IV, § 4), and it follows from Hasse's result that the equation (4.2) is soluble in $K(\varrho)$ when the congruence conditions (2.3–6) are satisfied. (These conditions imply the solubility of the congruence corresponding to (4.2) in *rational* numbers, and with $Z = W = 0$.)

As described in section 4, we can then deduce a solution of (2.2) in numbers from $K(\varrho)$, i.e. a complex point on the corresponding surface. Since the coefficients m and n are supposed to be absolutely rational, a *chord* through this point and the *conjugate* point will cut the surface in a third point with absolutely rational coordinates.

This completes the proof of Mordell's conjecture for the equation (2.2). Based on Hasse's result, the argument was independent of class-number considerations. I did, however, include the above section 5 to show the possibilities and limitations of such considerations. It would be very interesting if *all* cases could be covered by similar elementary means.

7. The above method fails for the more general equation (1.1), when (1.2) is not satisfied. I have *verified* the solubility in all cases (not of the type (2.1)) for which

$$|a_1a_2a_3a_4| \leqq 500 .$$

It seems to me very likely that Mordell's conjecture still holds, for the following reason: A solution of (1.1) is clearly obtained from a solution of the two simultaneous equations

$$a_1x_1^3+a_2x_2^3 = by_1^3,\ a_3x_3^3+a_4x_4^3 = by_2^3 , \tag{7.1}$$

with *arbitrary* b. When the e.c.c. for (1.1) are satisfied, we can choose an infinity of values b for which both equations (7.1) are possible for all moduli. From my earlier experience with such ternary equations (cf. [3], p. 205), the e.c.c. seem to be sufficient for solubility in about 70 % of all cases. The possibility of (7.1) is therefore strongly suggested by considerations of probability.

8. The above proof of Mordell's conjecture applies also to the equation (1.3) (a generalization of (2.2)). By a linear substitution, we can transform this equation into

$$x^3+m_1xy^2+m_2y^3 = n(u^3+m_1uv^2+m_2v^3) . \tag{8.1}$$

The corresponding field $K(\theta)$ is defined by

$$\theta^3+m_1\theta+m_2 = 0\,. \tag{8.2}$$

A solution of (8.1) can then be deduced from a solution of the norm-equation

$$N\left(\frac{X+Y\theta+Z\theta^2}{U+V\theta+W\theta^2}\right) = N\left(\frac{\eta}{\delta}\right) = n\,. \tag{8.3}$$

As in section 4, we determine a factor $\alpha = a+b\theta+c\theta^2$ such that the terms with θ^2 disappear in both products $\alpha\eta$ and $\alpha\delta$.

We note that we may assume (8.2) to be *irreducible*, since a rational linear factor on both sides of (8.1) would immediately lead to a solution.

The field $K(\theta)$ is cyclic only if it is a *Galois* field, i.e. when the discriminant of (8.2),

$$D = -4m_1{}^3-27m_2{}^2\,,$$

is a perfect square. This can always be obtained by taking $K(D^{1/2})$ as the basic field of rationality. We can then apply Hasse's result again, showing that the congruence conditions for (8.1) and (8.3) (in rationals) imply the solubility of these equations in $K(D^{1/2})$, and consequently (by the chord process) also in rationals.

Incidentally, the argument shows that Hasse's result is valid for *any* cubic field, cyclic or not.

REFERENCES

1. H. Hasse, *Beweis eines Satzes und Widerlegung einer Vermutung über das allgemeine Normenrestsymbol*, Nachr. Ges. Wiss. Göttingen, Math. Phys. Kl. 1931, 64–69.
2. L. J. Mordell, *Rational points on cubic surfaces*, Publ. Math. Debrecen 1 (1949), 1–6.
3. E. S. Selmer, *The diophantine equation* $ax^3+by^3+cz^3 = 0$, Acta Math. 85 (1951), 203–362.

UNIVERSITY OF OSLO, NORWAY