ON CUBIC EQUATIONS $z^2=f(x, y)$ WITH AN INFINITY OF INTEGER SOLUTIONS

L. J. MORDELL

1. Let $g(x, y, z)$ be a cubic polynomial in x, y, z with integer coefficients. I put forward the following conjecture.

CONJECTURE. *If the equation $g(x, y, z)=0$ has one integer solution, there exists an infinity of integer solutions when $g(x, y, z)-a$ is irreducible for all constants a.*

A proof or disproof seems very difficult. In fact, even in the simple case of

$$x^3 + y^3 + z^3 = 3,$$

I do not know if there are an infinity of integer solutions.

It may be remarked that if the equation represents a cone, the question becomes a two-dimensional one and assumes a different character. Thus the equation

$$(x + p)^3 + (y + q)^3 + (z + r)^3 = 0,$$

where p, q, r are given integers, has an infinity of integer solutions given by

$$x = t - p, \qquad y = - t - q, \qquad z = - r,$$

where t is an arbitrary integer, and two similar expressions, and these are the only integer solutions.

2. I have proved [1][1] this conjecture for some equations and in particular for some of the form

$$hz^2 = f(x, y), \tag{1}$$

where

$$\begin{aligned} f(x, y) = a_0 + \lambda x + \mu y + ax^2 + bxy + cy^2 \\ + Ax^3 + Bx^2y + Cxy^2 + Dy^3, \end{aligned} \tag{2}$$

and all coefficients are integers. In reconsidering my result, a further slight contribution to the subject arises.

We may without loss of generality assume that the known integer solution is $x=y=0$, and then we can put $a_0=hp^2$ where p is an

Presented to the Society, September 7, 1951; received by the editors June 25, 1951.

[1] Numbers in brackets refer to the bibliography at the end of the paper.

integer. By making a unimodular substitution, we may assume that $\mu=0$. Then we have the following theorem.

THEOREM I. *When, in* (1), $h=1$, $a_0=p^2\neq 0$, $\mu=0$, *the equation* (1) *has an infinity of integer solutions in the special case* $c=2p$ *provided that* $p^2(b^2-4ac)+\lambda^2 c$ *is positive and not a square.*

The condition excludes the case $a=b=c=0$, when it does not seem easy to find worth while results.

When $p=0$, some results have been found by Segre [3]. Thus when $f(x, y)$ is irreducible and the curve $f(x, y)=0$ has a point of inflexion at $x=y=0$, he shows that the equation (1) has an infinity of integer solutions. I note that we may sometimes find a solution without requiring the given point, that is, $x=y=0$, to be a point of inflexion. Thus when $p=0$, we take $\mu=0$, and then put $x=0$ and so

$$hz^2 = y^2(c + Dy).$$

We have an infinity of integer solutions if, for example, $(h, D)=1$ and hc is a quadratic residue of D, and in particular when $c=0$ and then $x=y=0$ is a point of inflexion.

The same idea leads to another result, really implicit in Segre's work, namely:

THEOREM II. *Let* L_1, M_1 *be homogeneous functions in* x, y, z *of the first degree,* L_2, M_2 *similarly of the second degree, all with integer coefficients. Then the equation*

$$L_1 + L_2 + M_1^3 + L_1M_2 = 0 \tag{3}$$

has an infinity of integer solutions provided the equations $L_1=0$, $M_1=1$ *are solvable in integers* x, y, z.

If $L_1=d(\lambda x+\mu y+\nu z)$ where $(\lambda,\mu,\nu)=1$, and $M_1=px+qy+rz$ where $(p, q, r)=1$, this will be so if $(\mu r-q\nu, \nu p-r\lambda, \lambda q-p\mu)=1$.

Then $L_1=0$, $M_1=1$ have an infinity of integer solutions, say X, Y, Z. We put $x=tX$, $y=tY$, $z=tZ$ and so $L_2(X, Y, Z)+t=0$ gives an infinity of solutions of (3).

In §4, I show that sometimes the knowledge of a *rational* solution of $f(x, y)=0$ may lead to an infinity of integer solutions of (1).

3. The proof of Theorem I requires two lemmas.

LEMMA 1. *Let* $ax^2+bxy+cy^2$ *be an indefinite quadratic form with rational coefficients, and let* b^2-4ac *be positive and not a square. Then the equation*

(4) $$ax^2 + bxy + cy^2 = m \ (\neq 0)$$

has an infinity of integer solutions if it has one.

There is no loss of generality in supposing that a, b, c are integers. Then the result is an obvious consequence of the infinity of automorphs of the quadratic form.

LEMMA 2. *If there exists an integer solution of*

$$ax^2 + bxy + cy^2 = \pm 1,$$

where a, b, c are as in Lemma 1, then the equation

(5) $$(aX^2 + bXY + cY^2)^2 = AX^3 + BX^2Y + CXY^2 + DY^3,$$

where A, B, C, D are integers, has an infinity of integer solutions.

The result follows from Lemma 1 on putting $X=tx$, $Y=ty$ where

$$t = Ax^3 + Bx^2y + Cxy^2 + Dy^3.$$

The result still holds when A, B, C, D are rational numbers provided that t is an integer for the integer values of x, y now satisfying (4) and that now $t \equiv 0 \pmod{m^2}$.

Now write equation (1), when $h=1$, as

$$z^2 = p^2 + L_1 + L_2 + L_3,$$

where L_1, L_2, L_3 are respectively homogeneous forms in x, y of dimensions one, two, three. Put

$$z = p + L_1/2p + S,$$

where S is a binary quadratic form with rational coefficients. Then

$$z^2 = p^2 + L_1 + L_1^2/4p^2 + 2pS + L_1S/p + S^2.$$

Define S by

(6) $$L_2 = L_1^2/4p^2 + 2pS,$$

and then x, y satisfy

(7) $$S^2 + L_1S/p = L_3.$$

Suppose now that S satisfies the conditions of Lemma 1. To apply Lemma 2 to (7), we must ensure the solvability of

(8) $$2pS = ax^2 + bxy + cy^2 - (\lambda x + \mu y)^2/4p^2 = \pm 2p,$$

and now we can take $\mu=0$. There is then a solution $x=0$, $y=k$, if $ck^2 = \pm 2p$ and in particular when $c = \pm 2p$. The conditions on S in

Lemma 1 are that $p^2(b^2-4ac)+\lambda^2 c$ should be positive and not a square. Since that values of x, y found from (8) make L_1/p an integer in (7), the theorem follows at once.

It is clear that other results can sometimes be derived by taking $m=2$ in (4), for example if $x\equiv 0 \pmod 2$, $y\equiv 1 \pmod 2$, we require $Cx+Dy\equiv 0 \pmod 4$, and so on.

4. I now come to the result mentioned at end of §2. It will suffice to take the particular equation

$$z^2 = ax^3 + by^3 + c, \tag{9}$$

where a, b, c are integers, and the rational solution $x=p/r$, $y=q/r$, $z=0$ is known and so

$$ap^3 + bq^3 + cr^3 = 0. \tag{10}$$

Put

$$rx = p + tbq^2, \qquad ry = q - tap^2, \tag{11}$$

where t is a parameter. Then

$$r^3z^2 = 3t^2(ab^2pq^4 + a^2bqp^4) + t^3(ab^3q^6 - ba^3p^6),$$

and so

$$r^3z^2/t^2 = 3abpq(-\,cr^3) + ab(bq^3 - ap^3)(-\,cr^3)t,$$

or

$$z^2/abct^2 = t(ap^3 - bq^3) - 3pq.$$

Hence $z=tv$ where

$$abc\{t(ap^3 - bq^3) - 3pq\} = v^2. \tag{12}$$

Also t must satisfy the congruences

$$p + tbq^2 \equiv 0 \pmod r, \qquad q - tap^2 \equiv 0 \pmod r. \tag{13}$$

It is easy to prescribe conditions such that (12) and (13) are solvable for t. Suppose that a, b, c are square free and relatively prime in pairs. We can then without loss of generality suppose that $(p, q, r)=1$, and so, from (10), $(q, r)=1$, $(p, r)=1$. Then $(b, r)=1$, $(a, r)=1$. For if δ is a prime factor of (b, r), then, from (10), $\delta | ap^3$ and so either $\delta | a$ or $\delta | p^3$ and hence $\delta=1$. Since

$$ap^2(p + tbq^2) + bq^2(q - tap^2) = -\,cr^3,$$

it suffices to make t satisfy only one of (13). In (12), we must have $v=abcu$ where u is an integer and so

(14) $$t(ap^3 - bq^3) - 3pq = abcu^2.$$

We can express the conditions for the solvability of (13) and (14) in terms of quadratic residues, but it will suffice to consider one instance. Take

$$p = 1, \qquad q = 1, \qquad a - b = 2, \qquad r = 2\rho,$$

so that

$$a + b + 8c\rho^3 = 0,$$

and so

$$a = 1 - 4c\rho^3, \qquad b = -1 - 4c\rho^3.$$

Then for the first of (13)

$$1 + t(-1 - 4c\rho^3) \equiv 0 \pmod{2\rho},$$

and so $t = 1 + 2\rho T$ where T is an integer. Also from (14)

$$2t - 3 = (16c^2\rho^6 - 1)cu^2,$$
$$4\rho T - 1 = (16c^2\rho^6 - 1)cu^2,$$

and

(15) $$cu^2 \equiv 1 \pmod{4\rho}.$$

Take now $c = 1$, $u = 2\rho w \pm 1$ where w is an arbitrary integer and so

$$T = 4\rho^5(2\rho w \pm 1)^2 - (\rho w^2 \pm w),$$

and the values of x, y are then given by (11). In particular if

$$p = q = 1, \qquad r = 4, \qquad a = -31, \qquad b = -33, \qquad c = 1,$$

and so

$$z^2 = -31x^3 - 33y^3 + 1,$$
$$t = 1 + 4T, \qquad 8T - 1 = 31 \cdot 33u^2.$$

But from (15), we can now write $u = 2w + 1$ and

$$t = 1 + \{1023(2w + 1)^2 + 1\}/2.$$

Then $4x = 1 - 33t$, $4y = 1 + 31t$, and so x, y are integers if $t \equiv 1 \pmod 4$. This is so since $(2w+1)^2 \equiv 1 \pmod 8$.

5. A more difficult problem than that in §1 is to find cubic equations which have integer solutions when none are obvious a priori. Thus I recently proved [2] the following theorem.

THEOREM III. *The equation*

$$z^3 = ax^2 + by^2 + c$$

has an infinity of integer solutions in x, y, z *if* a, b, c *are odd integers,* a *is prime to* b, *and* $ab \not\equiv 0 \pmod 7$. *Results can be found similarly for*

$$z^3 + pz^2 + qz = ax^2 + hxy + by^2 + c.$$

It would be of interest to find other classes of solvable equations.

Appendix (July 23, 1951). I notice that interesting results exist in the excluded case $a = b = c = 0$ of Theorem I. We have now the following theorem.

THEOREM IV. *The equation*

$$z^2 = p^2 + \lambda x + \mu y + Ax^3 + Bx^2y + Cxy^2 + Dy^3,$$

where the constants are integers, $p \neq 0$, λ *and* μ *are not both zero, and* $(\lambda, \mu) = 1$, *has an infinity of integer solutions.*

More generally, since we can take $\mu = 0$, $\lambda = 1$, this result is included in the following theorem.

THEOREM V. *The equation*

$$z^2 = p^2 + \lambda x + Ax^3 + Bx^2y + Cxy^2 + Dy^3,$$

where the constants are integers and $p\lambda \neq 0$, *has an infinity of integer solutions when the congruence*

$$2\lambda^3 + 2p(8Ap^3 + 4Bp^2Z + 2CpZ^2 + DZ^3) \equiv 0 \pmod{\lambda^4}$$

is solvable for Z.

We require the following lemma.

LEMMA 3. *The equation*

$$EX^4 = AX^3 + BX^2Y + CXY^2 + DY^3,$$

where $E \neq 0$, A, B, C, D *are integers, has an infinity of integer solutions when the congruence*

$$A + BZ + CZ^2 + DZ^3 \equiv 0 \pmod E$$

is solvable.

For put $Y = ZX$ where Z is a solution of the congruence. Then

$$EX = A + BZ + CZ^2 + DZ^3,$$

and hence we have the result.

To prove the theorem, put

$$x = 4p^2X, \qquad y = 2pY.$$

Then

$$z^2 = p^2 + 4p^2\lambda X + 64Ap^6X^3 + 32Bp^5X^2Y + 16Cp^4XY^2 + 8Dp^3Y^3.$$

Take $z=p+2\lambda pX-2\lambda^2pX^2$, and so

$$z^2 = p^2 + 4\lambda p^2X - 8\lambda^3p^2X^3 + 4\lambda^4p^2X^4.$$

Then

$$\lambda^4X^4 = (2\lambda^3 + 16Ap^4)X^3 + 8Bp^3X^2Y + 4Cp^2XY^2 + 2DpY^3,$$

and the theorem follows from Lemma 3.

I remark that in the particular case when $p=\lambda=0$, I gave the general integer solution in a paper written nearly forty years ago, *Indeterminate equations of the third and fourth degree*, The Quarterly Journal of Pure and Applied Mathematics (1914) pp. 170–186. Thus if $(x, y)=1$, all the integer values of x and y are given by a finite number of binary quartics in integer variables p and q.

Finally, I observe that results similar to Theorems IV, V hold for the equation

$$z^3 = p^3 + \lambda x + \mu y + ax^2 + bxy + cy^2,$$

where p, λ, μ, a, b, c are integers. If $p=0$, there are obviously an infinity of integer solutions given by taking $\lambda x+\mu y=0$. We may suppose then that $p\neq 0$ and have the following theorem.

THEOREM VI. *The equation above has an infinity of integer solutions if* $(\lambda, \mu)=1$.

Since we may take $\lambda=1$, $\mu=0$, the result follows by putting

$$x = 3p^2X, \qquad z = p + \lambda X.$$

So we have:

THEOREM VII. *The equation above when* $\lambda\neq 0$, $\mu=0$ *has an infinity of integer solutions when the congruence*

$$(9a + 3bZ + cZ^2)p^4 - 3\lambda^2p \equiv 0 \pmod{\lambda^3}$$

is solvable.

BIBLIOGRAPHY

1. L. J. Mordell, *Note on cubic diophantine equations* $z^2=f(x, y)$ *with an infinity of integral solutions*, J. London Math. Soc. vol. 17 (1942) pp. 199–203.

2. ———, *Note on cubic equations in three variables with an infinity of integer solutions*, Annali di Matematica Pura ed Applicata (4) vol. 29 (1949) pp. 301–305; or Colloques Internationaux du Centre National de la Recherche Scientifique, vol. 24, Paris, 1950, pp. 77–79.

3. B. Segre, *Sur les points entiers des surfaces cubiques*, Colloques Internationaux du Centre National de la Recherche Scientifique, vol. 24, Paris, 1950, pp. 81–82.

St. John's College, Cambridge University

ON THE SET OF VALUES OF A NONATOMIC, FINITELY ADDITIVE, FINITE MEASURE

R. J. NUNKE AND L. J. SAVAGE

A countably additive, nonatomic, finite measure takes on every value from zero to its maximum, inclusive, where, as throughout this note, it is to be understood that measures are non-negative.[1] The purpose of this note is to exhibit a counter-example, expressed as a theorem, which shows that finitely additive measures are as queer in this respect as in many others.[2]

THEOREM. *If a Boolean algebra $\mathfrak{X}$ with identity X carries any finitely additive, nonatomic measure at all, it carries one such measure, say m, such that $m(X)=4$, but none of the values of m lie in the interval* $(1, 3)$.

PROOF. Let p be a nonatomic, finitely additive measure. Without loss of generality it may be assumed that $p(X)=1$.

By Zorn's Lemma there exists a nonvacuous subset Υ of $\mathfrak{X}$ maximal with respect to the properties:

1. If $p(A)=0$, $A \in \Upsilon$.
2. If $A, B \in \Upsilon$, $A \cup B \in \Upsilon$.
3. If A is in Υ and B is in $\mathfrak{X}$, $A \cap B \in \Upsilon$.

That is, there is a maximal ideal containing the ideal of elements of p-measure 0. Denote the complement of Υ by $\mathfrak{Z}$. In virtue of its maximality with respect to properties 1–3, Υ has also the following properties:

Received by the editors February 26, 1951.

[1] See for example Lemma 2 of P. R. Halmos. *On the set of values of a finite measure*, Bull. Amer. Math. Soc. vol. 53 (1947) pp. 138–144.

[2] Attention is called to the papers of A. Sobczyk and P. C. Hammer, Duke Math. J. vol. 11 (1944) pp. 839–846 and pp. 847–851 respectively, which are closely related to and more extensive than the present note but do not happen to cover the same point.