THE CONGRUENCE $ax^3+by^3+c\equiv 0 \pmod{xy}$, AND INTEGER SOLUTIONS OF CUBIC EQUATIONS IN THREE VARIABLES.

By

L. J. MORDELL

CAMBRIDGE, ENGLAND.

I have recently[1] proposed the following

Conjecture: *Let $f(x, y, z)$ be a cubic polynomial in x, y, z with integer coefficients such that $f(x, y, z) - a$ is irreducible for all a. Then if the equation*

$$f(x, y, z) = 0 \tag{1}$$

does not represent a cone in three dimensional space and has one solution in integers, there exists an infinity of integer solutions.

This conjecture, as far as I know, has not been proved for even simple equations such as

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

but was proved for some equations and in particular for

$$z^2 - k^2 = lx + my + Ax^3 + Bx^2y + Cxy^2 + Dy^3,$$

where the coefficients are integers and l is prime to m, the known solution being $x = 0$, $y = 0$, $z = k$. The case $l = m = 0$ seems more difficult, but interesting results can be found for some equations of the form

$$z^2 - k^2 = Ax^3 + By^3. \tag{2}$$

I find that integer solutions of (2) can be deduced from the integer solutions of some very simple equations included in (1), namely,

$$ax^3 + by^3 + c = xyz, \tag{3}$$

[1] "On cubic equations $z^2 = f(x, y)$ with an infinity of integer solutions" *Proceedings of the American Mathematical Society* 3 (1952), 210—217.

Here some solutions of (3) are obvious since we can take $x = \pm 1$, and for y, any divisor of $c \pm a$. The conjecture suggests that there should be an infinity of integer solutions of (3) and this will be proved. Hence there exist equations[1] of the form (2) with an infinity of integer solutions as is shown by

Theorem I.

The equation

$$z^2 - 27^2 a^2 b^2 j^2 = a b^2 x^3 + y^3 \tag{4}$$

where a, b, j are integers, has an infinity of integer solutions.

The known types of formulae giving an infinity of integer solutions for equations included in (1) are as follows. They may involve one integer parameter t_1 or two integer parameters t_1, t_2. In the first case, the solutions are expressed as polynomials in t_1 or polynomials in $\theta_1^{t_1}$, $\varphi_1^{t_1}$, $\psi_1^{t_1}$ where θ_1 is some constant, e. g. a quadratic or cubic irrationality and φ_1, ψ_1 are conjugates of θ_1. In the second case, we have polynomials in t_1, t_2, or polynomials in $\theta_1^{t_1} \theta_2^{t_2}$, $\varphi_1^{t_1} \varphi_2^{t_2}$, $\psi_1^{t_1} \psi_2^{t_2}$, where θ_1, θ_2 are constant cubic irrationalities, and φ_1, ψ_1 are conjugates of θ_1 etc. The irrationalities arise as the units of quadratic or cubic fields. We may also have two parameter solutions as polynomials in $\theta_1^{\pm t_1}$ where θ_1 is a variable quadratic irrationality of norm unity as occurs with $x^2 + y^2 + z^2 + 2\,xyz = 1$.

In Theorem I, the infinity of solutions are given by polynomials in a, b, c with integer coefficients but of variable degrees in a, b, c. The polynomials are associated with an integer sequence $t = 1, 2, 3, \ldots$, and their degrees are associated with θ^t where $\theta^2 - 3\,\theta + 1 = 0$, and so really with alternate Fibonacci numbers.

We consider first the equation (3). If a prime p is a common divisor of x and y, then p^2/c, and so there can only be a finite number of values for p. Writing $p\,x$, $p\,y$ for x, y, we have

$$a\,p\,x^3 + b\,p\,y^3 + c/p^2 = x\,y\,z.$$

Hence we can find all the integer solutions of (3) from a finite number of equations of the same form in which $(x, y) = 1$.

We write (3) as a congruence and prove

Theorem II.

The congruence

$$a\,x^3 + b\,y^3 + c \equiv 0 \pmod{x\,y}, \tag{4}$$

[1] I have previously found some equations of this kind in a paper "Note on cubic diophantine equations $z^2 = f(x, y)$ with an infinity of integral solutions". (*Journal of the London Mathematical Society 17 (1942), 199–203*).

where a, b, c are given integers, has an infinite number of solutions for which $(cx, y)=1$, and we can give x, y as polynomials in a, b, c.

More generally, it will be seen that the same method proves the existence of an infinity of solutions of

$$ax^m+by^n+c\equiv 0 \pmod{xy},$$

where m, n are given positive integers, and also of

$$f(x)+g(y)+c\equiv 0 \pmod{xy},$$

where

$$f(x)=a_0x^m+a_1x^{m-1}+\cdots+a_{m-1}x,$$

and

$$g(y)=b_0y^n+b_1y^{n-1}+\cdots+b_{n-1}y,$$

and the a's and b's are integers.

The working is simpler if we write x_1, x_2 for x, y respectively. Since $(x_1, x_2)=1$, (4) is equivalent to the two congruences

$$bx_2^3+c\equiv 0 \pmod{x_1}, \tag{5}$$

$$ax_1^3+c\equiv 0 \pmod{x_2}. \tag{6}$$

We can satisfy (5) by putting

$$bx_2^3+c=x_1x_3, \tag{7}$$

where x_1 is any divisor of bx_2^3+c and x_2, prime to c, is still to be determined. We suppose x_1 can be taken so that $(x_2, x_3)=1$, and it will suffice for this if $(x_3, c)=1$. To satisfy (6), we require from (7),

$$a\left(\frac{bx_2^3+c}{x_3}\right)^3+c\equiv 0 \pmod{x_2}.$$

Since $(x_2, x_3)=1$, this will be satisfied if

$$ac^3+cx_3^3\equiv 0 \pmod{x_2},$$

or since we have assumed that $(x_2, c)=1$, if

$$x_3^3+ac^2\equiv 0 \pmod{x_2}. \tag{8}$$

From (7),

$$bx_2^3+c\equiv 0 \pmod{x_3}. \tag{9}$$

Hence (8), (9) are two congruences in x_2, x_3 similar to (5), (6), the two congruences in x_1, x_2.

A particular solution of (8) is given by taking

$$x_2=x_3^3+ac^2,\ b(x_3^3+ac^2)^3+c\equiv 0 \pmod{x_3}.$$

Since $(x_3, c)=1$, it suffices if $x_3 \mid (b a^3 c^5+1)$ and so $(x_3, c)=1$; and in particular if $x_3=b a^3 c^5+1$. Then $x_2=(b a^3 c^5+1)^3+a c^2$, and

$$x_3 x_1=b(x_3^3+a c^2)^3+c,$$

and so

$$x_1=b x_3^8+3 b a c^2 x_3^5+3 b a^2 c^4 x_3^2+c.$$

We can deal more generally with (8), (9) by writing (8) as

$$x_3^3+a c^2=x_2 x_4. \tag{10}$$

Then from (9)

$$b\left(\frac{x_3^3+a c^2}{x_4}\right)^3+c \equiv 0 \pmod{x_3}.$$

Suppose now $(x_3, x_4)=1$, which from (10) is so if $(x_4, a c)=1$. Then

$$x_4^3+b a^3 c^5 \equiv 0 \pmod{x_3}, \tag{11}$$

and from (10)

$$x_3^3+a c^2=0 \pmod{x_4}. \tag{12}$$

These two congruences in x_3, x_4 are similar to those in x_2, x_3 given in (8), (9).

A particular solution of (11), (12) is given by

$$x_3=x_4^3+b a^3 c^5;\ b^3 a^8 c^{13}+1 \equiv 0 \pmod{x_4}.$$

We can take $x_4=1+b^3 a^8 c^{13}$ and so $(x_4, a c)=1$. Then

$$\begin{aligned} x_3 &= (1+b^3 a^8 c^{13})^3+b a^3 c^5 \equiv 1 \pmod{c}, \\ x_4 x_2 &= (x_4^3+b a^3 c^5)^3+a c^2, \\ x_2 &= x_4^8+3 b a^3 c^5 x_4^5+3 b^2 a^6 c^{10} x_4^2+a c^2 \equiv 1 \pmod{a c}. \end{aligned}$$

We can continue this process. Thus for $\varrho=1, 2, 3, \ldots$, we define exponents λ_ϱ μ_ϱ, ν_ϱ by the recurrences formulae,

$$\lambda_{\varrho+2}=3 \lambda_{\varrho+1}-\lambda_\varrho,\ \mu_{\varrho+2}=3 \mu_{\varrho+1}-\mu_\varrho,\ \nu_{\varrho+2}=3 \nu_{\varrho+1}-\nu_\varrho, \tag{13}$$

and

$$\begin{aligned} &\lambda_1=0,\ \lambda_2=1,\ \lambda_3=3,\ \lambda_4=8,\ \lambda_5=21, \ldots \\ &\mu_1=-1,\ \mu_2=0,\ \mu_3=1,\ \mu_4=3,\ \mu_5=8, \ldots \\ &\nu_1=1,\ \nu_2=2,\ \nu_3=5,\ \nu_4=13,\ \nu_5=34, \ldots \end{aligned} \tag{14}$$

It may be remarked that the Fibonacci numbers are 1, 2, 3, 5, 8, 13, 21, ..., so that (14) consists essentially of sequences of alternate Fibonacci numbers.

Also

$$x_{\sigma+1}^3+a^{\lambda_\sigma} b^{\mu_\sigma} c^{\nu_\sigma}=x_\sigma x_{\sigma+2}, \text{ for } \sigma=2, 3, \ldots \tag{15}$$

We suppose $x_1, x_2, \ldots x_\varrho$ determined from these equations and then $x_{\varrho+1}, x_{\varrho+2}$ satisfy

$$x_{\varrho+2}^3 + a^{\lambda_{\varrho+1}} b^{\mu_{\varrho+1}} c^{\nu_{\varrho+1}} \equiv 0 \pmod{x_{\varrho+1}}, \tag{16}$$

$$x_{\varrho+1}^3 + a^{\lambda_\varrho} b^{\mu_\varrho} c^{\nu_\varrho} \equiv 0 \pmod{x_{\varrho+2}}. \tag{17}$$

Then we can take as a particular solution

$$x_{\varrho+1} = x_{\varrho+2}^3 + a^{\lambda_{\varrho+1}} b^{\mu_{\varrho+1}} c^{\nu_{\varrho+1}}, \tag{18}$$

and

$$x_{\varrho+2} = a^{3\lambda_{\varrho+1} - \lambda_\varrho} b^{3\mu_{\varrho+1} - \mu_\varrho} c^{3\nu_{\varrho+1} - \nu_\varrho} + 1 = a^{\lambda_{\varrho+2}} b^{\mu_{\varrho+2}} c^{\nu_{\varrho+2}} + 1. \tag{19}$$

Clearly $(x_{\varrho+2}, abc) = 1$ and so $(x_{\varrho+2}, x_{\varrho+1}) = 1$. Since $x_{\varrho+2} \equiv 1 \pmod{abc}$, $x_{\varrho+1} \equiv 1 \pmod{abc}$, then $x_\varrho \equiv 1 \pmod{abc}$. Hence $(x_{\varrho+1}, x_\varrho) = 1$, $(x_\varrho, x_{\varrho-1}) = 1$ etc.

It may be remarked that we might take as other particular solutions

$$-x_{\varrho+1} = x_{\varrho+2}^3 + a^{\lambda_{\varrho+1}} b^{\mu_{\varrho+1}} c^{\nu_{\varrho+1}},$$

and then

$$\pm x_{\varrho+2} = -a^{\lambda_{\varrho+2}} b^{\mu_{\varrho+2}} c^{\nu_{\varrho+2}} + 1.$$

The values of $x_{\varrho+1}, x_{\varrho+2}$ in (18), (19) give a value for x_1, x_2. We show now that x_2 is a polynomial in a, b, c, of degree $\lambda_{\varrho+2}^2$ in a. Since the coefficients are positive and the degrees are steadily increasing with ϱ, it follows that the values of x_2 found in this way are all different and so we have an infinity of solutions in x_1, x_2.

Let the degrees in a of $x_{\varrho+2}, x_{\varrho+1}, \ldots$ be $A_{\varrho+2}, A_{\varrho+1}, \ldots$. Then from (19), $A_{\varrho+2} = \lambda_{\varrho+2}$, and from (18), $A_{\varrho+1} = 3\lambda_{\varrho+2}$ since $3\lambda_{\varrho+2} > \lambda_{\varrho+1}$. Also from (15),

$$A_\sigma + A_{\sigma+2} = \max(3A_{\sigma+1}, \lambda_\sigma),$$

if $3A_{\sigma+1} \neq \lambda_\sigma$. Hence

$$A_\varrho = 3A_{\varrho+1} - A_{\varrho+2} = 8\lambda_{\varrho+2} = \lambda_4 \lambda_{\varrho+2}$$

$$A_{\varrho-1} = \max(3\lambda_4 \lambda_{\varrho+2}, \lambda_{\varrho-1}) - A_{\varrho+1}$$

$$= 21 A_{\varrho+2} = \lambda_5 A_{\varrho+2}.$$

We easily prove by induction that for $\tau = -2, -1, 0, \ldots \varrho-2$,

$$A_{\varrho-\tau} = \lambda_{\tau+4} A_{\varrho+2}.$$

For if the result is true for $\tau, \tau+1$, it is true for $\tau+2$ since

$$A_{\varrho-\tau-2} + A_{\varrho-\tau} = \max(3A_{\varrho-\tau-1}, \lambda_{\varrho-\tau-2}),$$

or

$$A_{\varrho-\tau-2} + \lambda_{\tau+4} A_{\varrho+2} = 3\lambda_{\tau+5} A_{\varrho+2}$$

since

$$3A_{\varrho-\tau-1} \geq 3A_{\varrho+2} = 3\lambda_{\varrho+2} > \lambda_{\varrho-\tau-2}.$$

Hence from (13),

$$A_{\varrho-\tau-2} = \lambda_{\tau+6} A_{\varrho+2}$$

and so for $\tau = \varrho - 4$,

$$A_2 = \lambda_{\varrho+2} A_{\varrho+2} = \lambda^2_{\varrho+2}.$$

We now come to Theorem 1. Consider the equation

$$z^2 - k^2 = a\,b\,(x^3 + c\,y^3), \quad c \neq 0. \tag{20}$$

Denote by θ, φ, ψ the roots of $t^3 = c$.

Take

$$z + k = a \prod_{\theta,\,\varphi,\,\psi} (p + q\,\theta + r\,\theta^2), \tag{21}$$

$$z - k = b \prod_{\theta,\,\varphi,\,\psi} (p_1 + q_1\,\theta + r_1\,\theta^2), \tag{22}$$

where p, q, r, p_1, q_1, r_1 are integers. Then multiplying (21), (22) and replacing θ^3 by c and θ^4 by θc, we have equation (20), where

$$x = p\,p_1 + (q\,r_1 + q_1\,r)\,c, \;\; y = p\,q_1 + p_1\,q + c\,r\,r_1.$$

Also $p\,r_1 + p_1\,r + q\,q_1 = 0$, and

$$2\,k = a\,(p^3 + c\,q^3 + c^2\,r^3 - 3\,c\,p\,q\,r) - b\,(p_1^3 + c\,q_1^3 + c^2\,r_1^3 - 3\,c\,p_1\,q_1\,r_1).$$

Take $r_1 = 0$, $p_1 = q$, $q_1 = -r$. Then

$$x = p\,q - c\,r^2, \;\; y = -p\,r + q^2, \;\; z - k = b\,(q^3 - c\,r^3),$$

and

$$2\,k = a\,(p^3 + c\,q^3 + c^2\,r^3 - 3\,c\,p\,q\,r) - b\,(q^3 - c\,r^3).$$

Take now $c = b/a$, and so

$$z^2 - k^2 = a\,b\,x^3 + b^2\,y^3,$$

and

$$2\,k = a\,p^3 + \frac{2\,b^2}{a}\,r^3 - 3\,b\,p\,q\,r.$$

It is easy to impose conditions upon a, b so that this equation has integer solutions in p, q, r and

$$x = p\,q - \frac{b}{a}\,r^2, \;\; y = -p\,r + q^2, \;\; z = k + b\,q^3 - \frac{b^2}{a}\,r^3,$$

are integers. In particular, take $p = 3\,b\,P$, $r = 3\,R\,a$, $k = 27\,a\,b^2\,j$, where j is an integer. Then x, y, z are integers and

$$2\,j = b\,P^3 + 2\,a\,R^3 - P\,R\,q.$$

From Theorem II, this has an infinity of integer solutions in P, R, q. Since $b|x$ and $b|z$, on putting bx for x, and bz for z, we see that

$$z^2-(27\,abj)^2=ab^2x^3+y^3$$

has integer solutions given by

$$x=3Pq-9aR^2,\quad y=-9abPR+q^2,$$
$$z=27abj+q^3-27a^2bR^3,$$

where
$$2j=bP^3+2aR^3-PRq.$$

The infinity of integer solutions in P, R, q gives an infinity of integer solutions in x, y, z since the value of z shows at once by Thue's theorem that if z were bounded, then also q, R would be bounded.

It may be noted that if in (20) we take $a=b=1$, $p_1=-p$, $q_1=0$, $r_1=r$, we see that integer solutions of

$$z^2-k^2=x^3+cy^3$$

are given in terms of integer solutions of

$$2p^3+cq^3-3cpqr=2k \tag{23}$$

by means of

$$x=-p^2+cqr,\quad y=-pq+cr^2,$$
$$z-k=-p^3+c^2r^3.$$

We can easily impose conditions other than $k\equiv 0 \pmod{27\,c}$ to make obvious some solutions of (23) for p, q, r.

Postscript. — The conjecture is false in the simple nontrivial case

$$x^2+y^2+z^2+4xyz=1.$$

After I spoke to Dr Cassels about this equation, he proved very simply that the only integer solutions were those typified by $y=z=0$.

Note added in reading the proofs, Aug. 1952. — Hurwitz has proved that if a is an integer $\neq 1,3$, the only integer solution of the equation

$$x^2+y^2+z^2+axyz=0$$

is $x=y=z=0$.

See his *Mathematische Werke* 2, p. 420.

St John's College, Cambridge, England.