ACTA ARITHMETICA
IX (1964)

The rational integral solution of the equation $a(x^3+y^3) = b(u^3+v^3)$ and allied Diophantine equations

by

A. Oppenheim (Kuala Lumpur)

Dedicated to L. J. Mordell on his seventy-fifth birthday

1. I give in this note the complete solution in rational integers of the cubic Diophantine equation

$$a(x^3+y^3) = b(u^3+v^3) \tag{1}$$

where a and b are given coprime integers which may be assumed positive. The case $a = b = 1$ is of course classical but so far as I am aware the complete solution in rational integers has not been given in the manner described below. For a brief account reference may be made to Hardy and Wright [2].

The method applies also to such equations as

$$aL^n(x, y)Q(x, y) = bL^n(u, v)Q(u, v) \tag{2}$$

wherein (i) L is an integral linear form, (ii) Q is an integral quadratic form and (iii) n is any integer other than -2. The method can also be used for such equations as

$$p(x, u)Q(x, y) = q(x, u)Q(u, v) \tag{3}$$

where p and q are integers which depend on x and u. A linear transformation reduces the solution of (3) to that of a ternary quadratic Diophantine equation and two congruences.

It will be plain also that the same method can be applied if L and Q are forms in more than two variables.

A brief account of the method was presented at the International Congress of Mathematicians, Stockholm, 1962.

2. We dispose first of trivial solutions of (1). These are of two kinds, those for which $x+y = 0$ (and so $u+v = 0$) and those such that $a(x+y)^3 = b(u+v)^3$. The second set can occur only if a and b are perfect cubes,

a_0^3 and b_0^3. We arrive at the following trivial solutions

$$x = -y, \quad u = -v,$$
$$x = b_0 m, \quad y = b_0 n, \quad u = a_0 m, \quad v = a_0 n,$$
$$x = b_0 m, \quad y = b_0 n, \quad u = a_0 n, \quad v = a_0 m,$$

for any integers m and n. The reason for the exclusion of the second set of solutions will appear below.

3. The trivial solutions being excluded, we can write

$$(4) \qquad (x+y, u+v) = k \geqslant 1, \quad x+y = k\lambda, \quad u+v = k\mu,$$
$$(\lambda, \mu) = 1, \quad \lambda\mu \neq 0, \quad a\lambda^3 - b\mu^3 \neq 0.$$

The crux of the method now lies in the linear equations

$$(5) \qquad g(x-y) = e\lambda + bf\mu^2,$$
$$g(u-v) = e\mu + af\lambda^2,$$

which determine unique integers g, e, f such that

$$(6) \qquad g \geqslant 1, \quad (g, e, f) = 1$$

since $a\lambda^3 - b\mu^3 \neq 0$. (It is for this reason that solutions if any such that $a(x+y)^3 = b(u+v)^3$ are excluded.)

Now use the elementary algebraic identity

$$(7) \qquad 4g^2\{a(x^3+y^3) - b(u^3+v^3)\} = k(a\lambda^3 - b\mu^3)\{(gk)^2 + 3e^2 - 3ab\lambda\mu f^2\}.$$

It follows therefore that if (x, y, u, v) is a non-trivial solution of (1) then the integers gk, e, f satisfy the ternary quadratic Diophantine equation

$$(8) \qquad (gk)^2 + 3e^2 - 3ab\lambda\mu f^2 = 0.$$

Suppose now that (x, y, u, v) is a primitive admissible set, i.e. coprime integers giving a non-trivial solution of (1). Then the greatest common divisor, t, of gk, e, f is either 1 or 2.

The proof is simple. If an odd prime p divides t, then p divides each of k, e, f but not g (since g, e, f are coprime). Hence p divides each of $x+y$, $x-y$, $u+v$, $u-v$; p divides each of $2x, 2y, 2u, 2v$ which contradicts primitivity.

Similarly if 4 divides t, then 4 divides each of $2x, 2y, 2u, 2v$ so that 2 divides each of x, y, u, v; again a contradiction.

Thus $t = 1$ or $t = 2$. We define unique integers α, β, γ (coprime, $\alpha \geqslant 1$) by the relations

$$(9) \qquad t\alpha = gk, \quad t\beta = e, \quad t\gamma = f.$$

To sum up: a primitive admissible set which satisfies (1) leads by the process described to unique integers (α, β, γ) (coprime, $\alpha \geqslant 1$) such that

$$(10) \qquad \alpha^2 + 3\beta^2 - 3ab\lambda\mu\gamma^2 = 0$$

where $(\lambda, \mu) = 1$, $\lambda\mu \neq 0$, $a\lambda^3 - b\mu^3 \neq 0$.

Implicit in this statement must be the solvability of the ternary quadratic Diophantine equation (10) in α, β, γ: this (general) problem was solved by Legendre (see, e.g. Dickson [1]). Application of this theorem shows that $ab\lambda\mu$ must be expressible in form m^2+3n^2 or, to put the matter in another way, that any prime p which divides the positive integer $ab\lambda\mu$ to an odd power must be either 3 or congruent to 1 modulo 6.

A pair of integers (λ, μ) satisfying such conditions (as well as $(\lambda, \mu) = 1$, $\lambda\mu \neq 0$, $a\lambda^3 - b\mu^3 \neq 0$) will be called *admissible*.

Thus an admissible quartet (x, y, u, v) which satisfies (1) leads to a unique admissible pair (λ, μ) and to a unique set (α, β, γ) (coprime, $\alpha \geqslant 1$) which satisfies (10).

4. The converse is also true as the following arguments show. Begin with an admissible pair (λ, μ): take any primitive solution (α, β, γ) (with $\alpha \geqslant 1$) of (10). Compute the four integers

$$(11) \qquad X = a\lambda + \beta\lambda + b\gamma\mu^2, \quad U = a\mu + \beta\mu + a\gamma\lambda^2,$$
$$Y = a\lambda - \beta\lambda - b\gamma\mu^2, \quad V = a\mu - \beta\mu - a\gamma\lambda^2.$$

Let $G = (X, Y, U, V)$ and define (x, y, u, v) by the relations

$$(12) \qquad Gx = X, \quad Gy = Y, \quad Gu = U, \quad Gv = V.$$

Then (x, y, u, v) is a primitive admissible set which satisfies

$$(13) \qquad a(x^3+y^3) = b(u^3+v^3), \quad \mu(x+y) = \lambda(u+v).$$

Moreover the parameters $\lambda, \mu, a, \beta, \gamma$ belong to (x, y, u, v) as described in the section above.

The brief table below for $x^3+y^3 = u^3+v^3$ illustrates the process:

λ	μ	a	β	γ	x	y	u	v	G	$\lvert\lambda^3-\mu^3\rvert$
1	7	9	1	2	6	−5	4	3	18	342
1	7	57	−10	13	6	−5	3	4	114	342
1	4	63	11	19	6	−4	5	3	63	63
1	4	3	−1	1	6	−4	3	5	3	63
1	3	39	−9	14	6	−3	4	5	26	26
1	3	3	0	1	6	−3	5	4	2	26

It will be observed that $G \mid (2\lambda^3 - 2\mu^3)$ and that $g \mid (\lambda^3 - \mu^3)$ as well as $G \mid 2a$. In all cases naturally a is a multiple of 3 but it seems preferable to leave (10) as it is.

We can of course derive without difficulty from (10) and (11) the standard rational solution of Euler (as given in Hardy and Wright [2]) but it seems to me better to leave the connections in the form stated rather than bring in parametric solutions of (10).

5. Instead of giving in detail the general equation (2) I state without proof the results for the special case connected with equal sums of two cubes,

$$x^3 + y^3 = u^3 + v^3, \tag{14}$$

given by the equation

$$(x+y)^n(x^2 - xy + y^2) = (u+v)^n(u^2 - uv + v^2) \tag{15}$$

for any odd integer n or for any even integer n other than -2.

If (λ, μ) runs through all admissible pairs for (14), i.e. if λ and μ are coprime, both positive or both negative and if the equation

$$a^2 + 3\beta^2 - 3\lambda\mu\gamma^2 = 0 \tag{16}$$

is solvable in coprime integers (α, β, γ) with $\alpha \geqslant 1$, then every integral quartet (x, y, u, v) which satisfies (15) is proportional to the four integers

$$a\lambda^{m+1}\mu^m \pm (\beta\lambda^{m+1}\mu^m + \gamma\mu^{n+1}), \quad a\lambda^m\mu^{m+1} \pm (\beta\lambda^m\mu^{m+1} + \gamma\lambda^{n+1}) \tag{17}$$

if $n = 2m+1$, $m \geqslant 1$, or to the four integers

$$a\lambda^s\mu^{s-1} \pm (\beta\lambda^s\mu^{s-1} + \gamma\lambda^{2s-1}\mu), \quad a\lambda^{s-1}\mu^s \pm (\beta\lambda^{s-1}\mu^s + \gamma\lambda\mu^{2s-1}) \tag{18}$$

if $n = 1-2s$, $s \geqslant 1$, for appropriate primitive solutions of (16).

The parameters λ, μ, α, β, γ are given uniquely by the corresponding admissible quartet (x, y, u, v).

As before the case $\lambda^{n+2} - \mu^{n+2} = 0$ is excluded.

One curious result may be noted; the solutions of

$$(X+Y)^{-n-4}(X^2 - XY + Y^2) = (U+V)^{-n-4}(U^2 - UV + V^2) \tag{19}$$

are connected with those of (15) by the relation

$$X : Y : U : V = \lambda^2 u : \lambda^2 v : \mu^2 x : \mu^2 y \tag{20}$$

where (as usual) $\lambda : \mu = (x+y) : (u+v)$. And of course conversely.

The case $n = 1$ has special interest.

As an example beginning with

$$20^3 + (-14)^3 = 17^3 + 7^3$$

we find that $(\lambda, \mu) = (1, 4)$, $(\alpha, \beta, \gamma) = (3, 1, 1)$ and so arrive at

$(4, -1, 10, 2)$, primitive solution for $n = -1$,

$(272, -248, 65, 31)$, primitive solution for $n = 3$,

$(17, 7, 320, -224)$, primitive solution for $n = 5$,

$(5, 1, 32, -8)$, primitive solution for $n = -3$.

For (15) when n is an even integer (other than -2) there is no restriction on (λ, μ) other than $\lambda^{n+2} - \mu^{n+2} \neq 0$ (i.e. $\lambda \neq \pm\mu$) and of course λ, μ coprime.

If $n = 2m$ $(m \geqslant 1)$, primitive integral quartets which satisfy (15) are proportional to the four integers

$$a\lambda^{m+1}\mu^m \pm (\beta\lambda^{m+1}\mu^m + \gamma\mu^{2m+1}), \quad a\lambda^m\mu^{m+1} \pm (\beta\lambda^m\mu^{m+1} + \gamma\lambda^{2m+1}) \tag{21}$$

for appropriate primitive integral solutions (α, β, γ) $(\alpha \geqslant 1)$ of the equation

$$a^2 + 3\beta^2 - 3\gamma^2 = 0 \tag{22}$$

which now replaces (16). Equation (22) has the following complete parametric solution (subject to conditions stated)

$$a = 6pq, \quad \beta = \pm(3q^2 - p^2), \quad \gamma = \pm(3q^2 + p^2) \tag{23}$$

(p, q arbitrary integers of different parity, $(p, 3q) = 1$, $p \geqslant 1$, $q \geqslant 1$),

$$a = 3pq, \quad \beta = \pm\tfrac{1}{2}(3q^2 - p^2), \quad \gamma = \pm\tfrac{1}{2}(3q^2 + p^2) \tag{24}$$

(p, q arbitrary odd integers, $(p, 3q) = 1$, $p \geqslant 1$, $q \geqslant 1$).

If $n = -2m$ $(m = 2, 3, \ldots)$ the solutions of (15) are given by rational multiples of the four integers,

$$a\lambda^{m+1}\mu^m \pm (\beta\lambda^{m+1}\mu^m + \gamma\lambda^{2m+1}\mu), \quad a\lambda^m\mu^{m+1} \pm (\beta\lambda^m\mu^{m+1} + \gamma\lambda\mu^{2m+1}) \tag{25}$$

where (α, β, γ) runs through the primitive solutions of (22) with $\alpha \geqslant 1$. Here too must be excluded the cases $\lambda = \pm\mu$.

6. I conclude with the reduction of equation (3),

$$p(x, u)Q(x, y) = q(x, u)Q(u, v), \tag{26}$$

to a ternary quadratic equation and two congruences.

Suppose that a solution (x, y, u, v) of (20) exists such that

$$x^2 p(x, u) - u^2 q(x, u) \neq 0. \tag{27}$$

Let $Q(x, y) = Ax^2 + Bxy + Cy^2$; use the linear transformation

$$\begin{aligned} ay &= \beta x + \gamma q u, \\ av &= \beta u + \gamma p x, \end{aligned} \tag{28}$$

which determines unique integers (α, β, γ), coprime with $\alpha \geqslant 1$. Then

$$\{pQ(x,y)-qQ(u,v)\}\alpha^2 = (px^2-qu^2)\{A\alpha^2+B\alpha\beta+C\beta^2-Cpq\gamma^2\}. \tag{29}$$

Thus a solution of (26) which satisfies (27) gives rise to a unique set of coprime integers (α, β, γ) $(\alpha \geqslant 1)$ such that

$$A\alpha^2+B\alpha\beta+C\beta^2-Cpq\gamma^2 = 0. \tag{30}$$

For special values of x and u it may happen that (30) is properly solvable. But the solutions α, β, γ must also be such that

$$\beta x+\gamma qu \equiv 0 \pmod{\alpha}, \tag{31}$$

$$\beta u+\gamma qx \equiv 0 \pmod{\alpha}. \tag{32}$$

If, for appropriate x and u, equation (30) and the two congruences (31) and (32) can be solved, we reach solutions of (26). This method is often useful in proving the existence of infinitely many solutions of equations of the form (26).

References

[1] L. E. Dickson, *Introduction to the Theory of Numbers*, (Dover), p. 117.

[2] G. H. Hardy and E. M. Wright, *Introduction to the Theory of Numbers*, 4th Ed., Oxford 1960, pp. 199-201.

Reçu par la Rédaction le 13. 11. 1963

ACTA ARITHMETICA
IX (1964)

Sur quelques catégories d'équations diophantiennes résolubles par des identités

par

T. NAGELL (Uppsala)

Dédié au 75ième anniversaire de L. J. Mordell

1. Courbes unicursales. Il est bien connu que la solution complète de l'équation diophantienne

$$x^2+y^2-z^2 = 0 \tag{1}$$

dans un corps quelconque Ω est donnée par les formules

$$x = t(t_1^2-t_2^2), \quad y = 2tt_1t_2, \quad z = t(t_1^2+t_2^2), \tag{2}$$

les paramètres t, t_1, t_2 parcourant tous les nombres du corps Ω, indépendamment entre eux; voir p. ex. Nagell [1](1), p. 217. Ainsi la *solution complète* de (1) en Ω est donnée par une *identité*.

Ce résultat n'est qu'un cas particulier de la proposition plus générale (voir p.ex. Nagell [1], p. 216):

Soit $C(x,y,z) = 0$ l'équation d'une conique en coordonnées homogènes x, y, z à coefficients appartenant au corps Ω. Si celle-ci admet un point (ξ, η, ζ), où ξ, η, ζ appartiennent à Ω, toutes les solutions de l'équation $C(x,y,z) = 0$ en nombres x, y, z appartenant à Ω sont données par un système de formules

$$\begin{aligned} x &= t(at_1^2+bt_1t_2+ct_2^2), \\ y &= t(a_1t_1^2+b_1t_1t_2+c_1t_2^2), \\ z &= t(a_2t_1^2+b_2t_1t_2+c_2t_2^2), \end{aligned} \tag{3}$$

où $a, b, c, a_1, b_1, c_1, a_2, b_2, c_2$ sont des nombres de Ω, et où les paramètres t, t_1, t_2 parcourent tous les nombres de Ω, indépendamment entre eux. Ainsi la solution complète en Ω est donnée par une identité.

(1) Les numéros figurant entre crochets renvoient à la bibliographie placée à la fin de ce travail.