On the lattice points on unicursal cubic curves

CHRISTOPHER HOOLEY[1])

University College of South Wales and Monmouthshire, U.K.

The theory of rational points on a plane unicursal curve

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

and their determination through a parametric representation is essentially complete due to the work of Poincaré, the special case of the conic having been considered earlier by Gauss in the *Disquisitiones Arithmeticae*. This theory, however, does not answer fully the problem of determining all integer solutions of (A) through an algebraic parametric representation, since, as Cantor [1] remarked in respect of the conic, the transition from a rational solution to a corresponding integral solution may lead to the latter being affected by a common factor that is not directly expressible algebraically. Having in a previous paper [2] discussed Cantor's remark and obtained in the case of the conic a parametric representation for the integer solutions of (A) in terms of triplets of quadratic forms with invariants related to f, we turn in the present communication to the corresponding problem for the unicursal cubic curve. By a method more geometrical in nature than that used in [2] but applicable in principle to unicursal curves of any degree we shew that for the unicursal cubic curve there is also a complete parametric representation of the integer solutions of (A) by a set of triplets of binary forms, these being now of degree 3.

The theory is analogous to that for the conic in that firstly the invariants of the representing triplets are related to the coefficients of f and in that secondly each primitive solution, except that corresponding to the double point, is obtained precisely once. Moreover, again, triplets with given invariants belong to a finite number of classes. On the other hand the theory of the class number contains features that are not presented in the quadratic case or indeed in most situations relating to homogeneous forms, there being for example the fact that for any given (possible) invariant system there exists a proportional invariant system for which

[1]) Supported in part by Air Force Office of Scientific Research grant AF-AFOSR-69-1712.

the class number of triplets is 1. In consequence the properties of the class number have been discussed in rather more detail than is needed for the proof of the principal result on the Diophantine equation.

We note finally that the method provides an alternative proof for the main theorem in [2] since it is straightforward to reformulate this theorem in terms of an invariant system of the type used here.

As a beginning it is necessary to make some remarks on triplets of cubic forms and on the invariants and covariants of the ternary cubic forms with which it will be seen that these triplets are associated.

Let us write, for $i = 1, 2, 3$, $u_i(r, s) = a_i r^3 + b_i r^2 s + c_i rs^2 + d_i s^3$, $U_i(R, S) = A_i R^3 + B_i R^2 S + C_i RS^2 + D_i S^3$. Then, if the binary cubic forms $u_1(r, s)$, $u_2(r, s)$, $u_3(r, s)$ transform simultaneously into the forms $U_1(R, S)$, $U_2(R, S)$, $U_3(R, S)$ through a real substitution

$$r = \alpha R + \beta S, \quad s = \gamma R + \delta S$$

of non-vanishing modulus, then we shall say that the triplet u_1, u_2, u_3 is *equivalent under a real substitution* to the triplet U_1, U_2, U_3. If, however, as in the cases of most interest to us here, the substitution have integral coefficients and be of modulus $+1$, we shall merely use the term *equivalent*, it being of importance to observe that it is appropriate here *to distinguish between proper and improper equivalence* in contrast to the corresponding theory for quadratic forms. In the theory to follow all triplets will be assumed to be such that their constituent cubic forms neither have a common non-constant factor nor are linearly dependent.

A triplet u_1, u_2, u_3 gives rise through the formation of the eliminant of

$$x_1 = u_1(r, s), \quad x_2 = u_2(r, s), \quad x_3 = u_3(r, s) \tag{1}$$

to a ternary cubic equation

$$\phi\,(x_1, x_2, x_3) = \sum_{k_1+k_3+k_2=3} \Delta_{k_1, k_2, k_3}\, x_1^{k_1} x_2^{k_2} x_3^{k_3} = 0\,,$$

which is in fact the equation of the unicursal curve given parametrically by (1). This procedure is immediately seen to yield a set of simultaneous invariants of the triplet u_1, u_2, u_3 since the eliminant ϕ is evidently unaltered apart possibly from a constant factor if u_1, u_2, u_3 be replaced by an equivalent triplet U_1, U_2, U_3. The coefficients Δ_{k_1, k_2, k_3}, the mode of formation of which will be considered more fully presently, will be merely termed the invariants of u_1, u_2, u_3, since as will be apparent later they form a fundamental system in the sense that all other invariants are essentially determined by them.

The invariants S and T of a general ternary cubic form

$$f(x_1, x_2, x_3) = \sum_{k_1+k_2+k_3=3} D_{k_1, k_2, k_3}\, x_1^{k_1} x_2^{k_2} x_3^{k_3}$$

will also be required. These are defined precisely as in Salmon's Higher Plane Curves but do not when regarded as polynomials in D_{k_1, k_2, k_3} have integral coefficients, since the coefficients of f have not here been affected by multinomial coefficients. When $f = 0$ is a singular curve[1]) the discriminant of the form vanishes and the consequent equation

$$T^2 + 64S^3 = 0$$

implies that we may write

$$T = (2M)^3, \quad S = -M^2. \tag{2}$$

It will be necessary also to introduce in connection with cubic forms corresponding to unicursal curves a certain arithmetical invariant, which is analogous in some respects to the determinant or discriminant of a ternary quadratic (the discriminant of a general ternary cubic being analogous in other respects to the determinant or discriminant of a ternary quadratic) and which we name the *determinant* of the form. To form this invariant we use the contravariant

$$TQ + 96S^2P,$$

the vanishing of whose coefficients is seen by comparison with Salmon, art 240, to be the condition that the form either have a cusp or break up into a line and a conic. Using (2) we are led to introduce the associated contravariant

$$F(\alpha_1, \alpha_2, \alpha_3) = \tfrac{27}{4}(Q + 12MP),$$

the coefficients of which will be seen later to be integers, not all zero, when f is a form with integer coefficients that corresponds to a unicursal curve. For forms f of the latter type the determinant Δ is then defined to be the positive highest common factor of the coefficients of F, the invariance of Δ with respect to integral unimodular substitutions for the indeterminates of f being a consequence of the contravariance of F.

Having introduced the invariants that will be needed, we must discuss briefly the genesis of the fundamental system Δ_{k_1, k_2, k_3} and its rôle as a resultant system for u_1, u_2, u_3. To find the eliminant $\phi(x_1, x_2, x_3)$ of

$$x_1 = u_1(r, s), \quad x_2 = u_2(r, s), \quad x_3 = u_3(r, s) \tag{3}$$

we consider two distinct lines (using homogeneous coordinates)

$$\lambda_1 x_1 + \lambda_2 x_2 + \lambda_3 x_3 = 0, \quad \mu_1 x_1 + \mu_2 x_2 + \mu_3 x_3 = 0$$

and observe that the condition that they intersect on the curve given by (3) is the vanishing of the resultant

[1]) A singular cubic being any cubic with zero discriminant. By a unicursal curve is meant here a non-degenerate singular cubic.

$$R(\lambda_1 u_1 + \lambda_2 u_2 + \lambda_3 u_3,\ \ \mu_1 u_1 + \mu_2 u_2 + \mu_3 u_3), \tag{4}$$

the coefficients of which when regarded as a form in the indeterminates $\lambda_1, \lambda_2, \lambda_3, \mu_1, \mu_2, \mu_3$ form the resultant system of u_1, u_2, u_3 in accordance with Kronecker's theory and which do not all vanish in virtue of the restrictions placed on u_1, u_2, u_3. The fundamental system is thus just an equivalent resultant system, since by Bezout's method it is evident that (4) is a polynomial in $\lambda_2\mu_3 - \lambda_3\mu_2$, $\lambda_3\mu_1 - \lambda_1\mu_3$, $\lambda_1\mu_3 - \lambda_2\mu_1$ and that hence $\phi(x_1, x_2, x_3)$ is obtained by replacing $\lambda_2\mu_3 - \lambda_3\mu_2$, $\lambda_3\mu_1 - \lambda_1\mu_3$, $\lambda_1\mu_2 - \lambda_2\mu_1$ in this polynomial by x_1, x_2, x_3, respectively. Furthermore it is easy to see that when μ_1, μ_2, μ_3 have integral coefficients the h.c.f. of the initial resultant system is equal to the h.c.f. of the fundamental system. Formed in this manner ϕ is immediately seen to have a covariant property with respect to linear substitutions that replace u_1, u_2, u_3 by linear combinations u_1', u_2', u_3', it being clear from (4) that, if $u_1, u_2, u_3; x_1, x_2, x_3$ transform cogrediently by means of a unimodular substitution into $u_1', u_2', u_3'; x_1', x_2', x_3'$ and ϕ' be defined in terms of u_1', u_2', u_3' as ϕ was in terms of u_1, u_2, u_3, then $\phi(x_1, x_2, x_3) = \phi'(x_1', x_2', x_3')$. It is important too to note here that when u_1, u_2, u_3 is transformed into U_1, U_2, U_3 by a substitution of modulus K the fundamental system of U_1, U_2, U_3 is obtained by multiplying that of u_1, u_2, u_3 by K^9. We note also that through setting $\lambda_1 = \mu_1 = 0$ we have $\Delta_{3,0,0} = R(u_2, u_3)$.

Although the ternary form $f(x_1, x_2, x_3)$ has been interpreted through the corresponding unicursal curve in two dimensional projective space, *solutions* of the *equation* $f(x_1, x_2, x_3) = 0$ are to regarded as being distinct unless their corresponding components be all equal, rational and integral solutions being those in which x_1, x_2, x_3 are, respectively, rationals and integers. It follows from the theory of unicursal curves that, if $x_i = u_i(r, s)$ be a parametric representation of $f(x_1, x_2, x_3) = 0$, then each solution of $f = 0$ apart from that corresponding to the double point is obtained from a unique pair of values r, s; also, proportional solutions, that is those that appertain to the same point on the curve, correspond to proportional pairs r, s.

We are now in a position to prepare for the proofs of our final results by proving a number of simple lemmata. Triplets throughout will have integral coefficients although the indeterminates in them may on occasion take non-integral values.

LEMMA 1. *Triplets of binary cubic forms with proportional invariants are equivalent under real substitutions the coefficients of which are of the form* $r_1\theta, r_2\theta, r_3\theta, r_4\theta$, *where* r_1, r_2, r_3, r_4 *are rational and* θ *is the real cube root of an integer.*

We require the principle that, if $x_i = w_i(t)$ be a parametrization of a unicursal cubic, where $w_i(t)$ has integral coefficients, then, excluding from consideration the double point and its parameters, any point which can be represented by rational co-ordinates corresponds to a rational value of t and conversely.

Let $u_1(r, s)$, $u_2(r, s)$, $u_3(r, s)$ and $U_1(R, S)$, $U_2(R, S)$, $U_3(R, S)$ have proportional invariants. Then, since the functions $v_i(t) = u_i(t, 1)$ and $V_i(T) = U_i(T, 1)$ furnish two parametric representations of the same unicursal curve, the equations

$$\frac{v_1(t)}{V_1(T)} = \frac{v_2(t)}{V_2(T)} = \frac{v_3(t)}{V_3(T)} \tag{5}$$

give rise to an algebraic correspondence between t and T that is one-one save for the exceptional values of t and T that relate to the double point, rational values of t being in correspondence with rational values of T. Therefore (5) is equivalent to an homography

$$t = \frac{\alpha T + \beta}{\gamma T + \delta}$$

with rational values of $\alpha, \beta, \gamma, \delta$, and we have the identity

$$\frac{u_1(\alpha T + \beta, \gamma T + \delta)}{U_1(T, 1)} = \frac{u_2(\alpha T + \beta, \gamma T + \delta)}{U_2(T, 1)} = \frac{u_3(\alpha T + \beta, \gamma T + \delta)}{U_3(T, 1)}$$

in which the common value of the terms is a rational constant λ since the denominators have no common factors. This constant can be taken to be 1 by dividing $\alpha, \beta, \gamma, \delta$ by $\sqrt[3]{\lambda}$ and the lemma then follows on substituting $T = R/S$.

We note in passing that this lemma justifies our previous statement that the system Δ_{k_1, k_2, k_3} of invariants may be regarded as a fundamental one.

LEMMA 2. *Let* $f = 0$ *be a unicursal curve, where*

$$f(x_1, x_2, x_3) = \sum_{k_1+k_2+k_3=3} D_{k_1, k_2, k_3} x_1^{k_1} x_2^{k_2} x_3^{k_3}$$

is a primitive ternary cubic form of determinant Δ. *Then there exists a triplet* u_1, u_2, u_3 *with invariants* $\Delta D_{k_1, k_2, k_3}$.

The proposition being covariant with respect to integral unimodular substitutions for x_1, x_2, x_3, it is enough to consider any form f^* to which f is equivalent. If (ν_1, ν_2, ν_3) be the coordinates of the double point expressed in terms of relatively prime integers, there exists an integral unimodular substitution

$$x_i = \lambda_i x_1' + \mu_i x_2' + \nu_i x_3' \ ; \quad i = 1, 2, 3,$$

which transforms the double point into (0, 0, 1) and hence f into the equivalent form

$$f^*(x_1', x_2', x_3') = \psi(x_1', x_2') - x_3' \chi(x_1', x_2') \ ,$$

where $$\psi(x_1', x_2') = c_0x_1'^3 + c_1x_1'^2x_2' + c_2x_1'x_2'^2 + c_3x_2'^3$$

and $$\chi(x_1', x_2') = d_0x_1'^2 + d_1x_1'x_2' + d_2x_2'^2 .$$

Reverting now to x_1, x_2, x_3 to indicate the indeterminates in f^* it is seen by a familiar method that

$$x_1 = u_1(r, s) = r\chi(r, s), x_2 = u_2(r, s) = s\chi(r, s), x_3 = u_3(r, s) = \psi(r, s)$$

is a parametrization of the curve. Since the eliminant $\phi^*(x_1, x_2, x_3)$ of the above system is proportional to f^*, it remains to discover the coefficient of proportionality and to substantiate an earlier assertion that made it possible for Δ to be defined.

Let the coefficients c_i, d_j of f^* be regarded for the present as indeterminates. Then the contravariant $F^*(\alpha_1, \alpha_2, \alpha_3)$ of f^* is rational and integral in these indeterminates, since

$$T^* = \left(\frac{2d_0d_2}{9} - \frac{d_1^2}{36}\right)^3 .$$

Also, as is shewn in art 135 of Salmon's Modern Higher Algebra, the coefficients of F^* are zero except for the coefficient C, say, of α_3^3. Now, comparing the coefficients of x_1^3 in f^* and ϕ^*, we have

$$\frac{\phi^*}{f^*} = \frac{R(s\chi(r, s), \psi(r, s))}{c_0} = \frac{R(s, \psi(r, s))R(\chi(r, s), \psi(r, s))}{c_0} = R(\chi(r, s), \psi(r, s)).$$

But the vanishing of $R(\chi, \psi)$ implies that of C, since f^* factorizes if ψ and χ have a common factor. Therefore, as $R(\chi, \psi)$ is irreducible and is of the same degree as C,

$$R(\chi, \psi) = \mathcal{K}C$$

for some constant $\mathcal{K}$. Specialising f^* to be $c_0x_1^3 - d_2x_2^2x_3$, for which it may be verified that $R(\chi, \psi)$ and C are both $c_0^2d_2^3$, we deduce that $\mathcal{K} = 1$. We conclude from its contravariance that F not only always has integer coefficients but that also the determinant Δ is the measure of the absolute ratio of ϕ^* to f^*. Since the sign of the ratio can be changed if requisite by substituting $-u_i(r, s)$ for $u_i(r, s)$, the proof of the lemma is complete.

Before enunciating the next lemma we define a *primitive* representation of integers m_1, m_2, m_3 by a triplet u_1, u_2, u_3 to mean the simultaneous expression of m_i by $u_i(r, s)$ with common relatively prime integers r, s for $i = 1, 2, 3$.

LEMMA 3. *Given integers m_1, m_2, m_3 are represented primitively by at most k classes of triplets with given invariants, where $k =$ h.c.f. (m_1, m_2, m_3).*

We recall the familiar principle that, if $m = f(\alpha, \gamma)$ be a primitive representation of m by a binary form $f(r, s)$, then there is a substitution depending only on α, γ

that transforms $f(r, s)$ into an equivalent form having leading coefficient m. Thus, if u_1, u_2, u_3 and U_1, U_2, U_3 with the same invariants both represent primitively m_1, m_2, m_3, then they are equivalent, respectively, to v_1, v_2, v_3 and V_1, V_2, V_3 in both of which triplets the leading coefficients are m_1, m_2, m_3. By Lemma 1 we have

$$v_i(r, s) = V_i(R, S),$$

where $r = \alpha R + \beta S$, $s = \gamma R + \delta S$, the substitution being of modulus unity as the invariants are equal. Since $r = 1$, $s = 0$ and $R = 1$, $S = 0$ give the same solution, we infer (viz. introductory remarks) that $\alpha = 1, \beta$ rational, $\gamma = 0$, $\delta = 1$ and therefore that

$$V_i(R, S) = v_i(R + \beta S, S). \tag{6}$$

Examination of the coefficient $v_i(\beta, 1)$ of S^3 in $v_i(R + \beta S, S)$ shews that the denominator of β expressed as a fraction in lowest terms divides m_i and hence k. Since triplets V_1, V_2, V_3 corresponding to values of β that differ by an integer are equivalent, (6) gives rise to at most k inequivalent triplets V_1, V_2, V_3 and the lemma follows.

We are now in a position to prove our four theorems concerning class numbers and the representation of integer points on cubic curves.

THEOREM 1. *Triplets with assigned invariants Δ_{k_1, k_2, k_3} are distributed into a finite number of classes.*

Let (ξ_1, ξ_2, ξ_3) be the co-ordinates expressed through relatively prime integers of some rational point, other than the double point, on the corresponding cubic curve. Then for any triplet $u_1(r, s)$, $u_2(r, s)$, $u_3(r, s)$ with the given invariants there is a unique positive integer λ for which the triplet can represent primitively $\lambda\xi_1, \lambda\xi_2, \lambda\xi_3$ (see the remarks before Lemma 1 and at the beginning of the proof of that lemma). Since the simultaneous congruence $u_1(r, s) \equiv u_2(r, s) \equiv u_3(r, s)$, mod λ, is soluble for $(r, s) = 1$, the members of the fundamental resultant system for u_1, u_2, u_3 are all divisible by λ and hence $\lambda | \Theta$, where $\Theta = \text{h.c.f.}\, \Delta_{k_1, k_2, k_3}$. The number of possible values of λ being limited by this and the number of classes which can primitively represent $\lambda\xi_1, \lambda\xi_2, \lambda\xi_3$ being limited by Lemma 3, the class-number of triplets with given invariants is finite (in fact not greater than $\sigma(\Theta)$, the sum of the positive divisors of Θ).[1]

As an analogue of Theorem 1 in [2] we now consider

THEOREM 2. *Let $f(x_1, x_2, x_3) = 0$ be a unicursal cubic curve, where*

$$f(x_1, x_2, x_3) = \sum_{k_1+k_2+k_3=3} D_{k_1, k_2, k_3} x_1^{k_1} x_2^{k_2} x_3^{k_3}$$

[1] A sharper estimate can be derived through an easily obtained improvement in Lemma 3.

is a primitive ternary cubic form of determinant Δ. *Then there is a finite set of triplets* $u_1^{(j)}, u_2^{(j)}, u_3^{(j)}$ *with invariants of the form* $\Delta\lambda_j^3 D_{\alpha_1,\alpha_2,\alpha_3}$, *where* $\lambda_j|\Delta$ *and* $\lambda_j > 0$, *with the property that the general primitive solution of*

$$f(x_1, x_2, x_3) = 0$$

is given by

$$x_1 = u_1^{(j)}(r, s),\quad x_2 = u_2^{(j)}(r, s),\quad x_3 = u_3^{(j)}(r, s),$$

where, for each j, *the integers* r, s *run through all values for which* h.c.f .$(u_1^{(j)}, u_2^{(j)}, u_3^{(j)}) = 1$. *Each primitive solution with the exception of that relating to the double point is obtained thus precisely once.*

The general solution in integers of the equation is

$$x_1 = \mathcal{K}u_1^{(j)}(r, s),\quad x_2 = \mathcal{K}u_2^{(j)}(r, s),\quad x_3 = \mathcal{K}u_3^{(j)}(r, s),$$

where r, s *run through all integer values and* $\mathcal{K}$ *through all cube-free values. Each solution apart from that relating to the double point is obtained (but possibly more than once).*

It is enough to consider the first part of the theorem as all solutions can be derived from primitive ones by using cube-free multipliers $\mathcal{K}$ and by allowing r and s to have common factors greater than 1.

Let u_1, u_2, u_3, which as will be clear may be regarded as $u_1^{(1)}, u_2^{(1)}, u_3^{(1)}$, be a triplet with invariants $\Delta D_{k_1,k_2,k_3}$ in accordance with Lemma 2. Then, for any primitive solution ξ_1, ξ_2, ξ_3 of $f = 0$, there is one positive divisor λ of Δ for which there is a primitive representation of $\lambda\xi_1, \lambda\xi_2, \lambda\xi_3$ by u_1, u_2, u_3. Letting α, γ be the values of the variables in this representation, choose integers β, δ so that $\alpha\delta - \beta\gamma = 1$ and transform the forms $u_i(r, s)$ into the equivalent forms

$$U_i(R, S) = \lambda\xi_i R^3 + B_i R^2 S + C_i R S^2 + D_i S^3 \tag{7}$$

by the substitution

$$r = \alpha R + \beta S,\quad s = \gamma R + \delta S$$

of modulus unity. Then the forms

$$U_i^*(R, S) = \frac{1}{\lambda} U_i(R, \lambda S) \tag{8}$$

have integral coefficients, the triplet U_1^*, U_2^*, U_3^* by considerations of weight has invariants $\Delta\lambda^3 D_{k_1,k_2,k_3}$, and U_1^*, U_2^*, U_3^* primitively represents ξ_1, ξ_2, ξ_3. Conversely all relatively prime triplets of numbers represented (primitively) by U_1^*, U_2^*, U_3^* are primitive solutions of $f = 0$. Since $\lambda|\Delta$ the forms U_1^*, U_2^*, U_3^* thus obtained for each primitive solution of $f = 0$ belong to a finite number of classes by Theorem 1 and by choosing one representative triplet in each of these classes we form a system of triplets $(u_1^{(j)}, u_2^{(j)}, u_3^{(j)})$ that yield all primitive solutions of the equation and only primitive solutions of the equation.[1]) It remains to shew that each primitive solution is given but once. A primitive representation of a primitive solution η_1, η_2, η_3 by a triplet $u_1^{(j)}, u_2^{(j)}, u_3^{(j)}$ equivalent to the triplet given by (8) corresponds to a primitive representation of $\lambda\eta_1, \lambda\eta_2, \lambda\eta_3$ by (u_1, u_2, u_3), since $(R, \lambda) = 1$ from (7) and (8) as otherwise η_1, η_2, η_3 would all be divisible by a divisor of λ exceeding 1. Therefore η_1, η_2, η_3 cannot be primitively represented by two triplets appertaining to different values of λ. Suppose then η_1, η_2, η_3 be primitively represented by two triplets of the system appertaining to the same value of λ. These triplets being equivalent, respectively, to triplets of the form $U_1^*, U_2^*, U_3^*; V_1^*, V_2^*, V_3^*$, we have by the above method again

$$\lambda\eta_i = U_i(\varrho_0, \lambda\sigma_0) = V_i(R_0, \lambda S_0),$$

where $(\varrho_0, \lambda\sigma_0) = (R_0, \lambda S_0) = 1$ and where, as U_1, U_2, U_3; V_1, V_2, V_3 are both equivalent to u_1, u_2, u_3,

$$U_i(\alpha l + \beta m, \gamma l + \delta m) = V_i(l, m)$$

for some integers $\alpha, \beta, \gamma, \delta$ such that $\alpha\delta - \beta\gamma = 1$. Hence

$$\varrho_0 = \alpha R_0 + \beta\lambda S_0, \quad \lambda\sigma_0 = \gamma R_0 + \delta\lambda S_0$$

and so $\lambda|\gamma$. Therefore the unimodular integral substitution

$$\varrho = \alpha R + (\beta\lambda)S, \quad \sigma = (\gamma/\lambda)R + \delta S$$

transforms $U_i^*(\varrho, \sigma) = U_i(\varrho, \lambda\sigma)/\lambda$ into $V_i^*(R, S) = V_i(R, \lambda S)/\lambda$ for $i = 1, 2, 3$. Hence U_i^*, U_2^*, U_3^* and V_1^*, V_2^*, V_3^* are equivalent and so the two triplets of the system are the same. Since a given triplet cannot represent a solution more than once the proof of the theorem is complete.

THEOREM 3. *Let* $f(x_1, x_2, x_3) = 0$ *be a unicursal cubic curve, where*

$$f(x_1, x_2, x_3) = \sum_{k_1+k_2+k_3=3} D_{k_1, k_2, k_3}\, x_1^{k_1} x_2^{k_2} x_3^{k_3}.$$

is primitive. Then there exists λ *such that there is only one class of triplets with invariants* $\lambda D_{k_1, k_2, k_3}$.

We confine our attention to the case where $(\Delta, 6) = 1$ in order not to prolong the proof.

Choose the minimal positive value of λ such that $(\lambda, 6) = 1$ and such that there is a triplet with invariants $\lambda D_{k_1, k_2, k_3}$, it being obvious that $1 \leq \lambda \leq \Delta$,

[1]) If the main end in view were merely a system of forms with this property, then the finiteness of the system could be more easily deduced from the fact that a general integral substitution of modulus λ can be obtained by compounding a unimodular substitution with one of a finite number of substitutions of modulus λ.

and suppose that the class number of triplets with these invariants exceeds 1. Let u_1, u_2, u_3; v_1, v_2, v_3 be inequivalent triplets with these invariants. Then for any prime divisor p of λ at least one form, $u_{i_p}(r, s)$, say, from the triplet u_1, u_2, u_3 is not identically zero, $\bmod p$, since otherwise p would divide all the coefficients of all the forms in the triplet and there would be a triplet $(u_1/p, u_2/p, u_3/p)$ with integral invariants $(\lambda/p^6)D_{k_1,k_2,k_3}$ contrary to hypothesis. The congruence

$$u_{i_p}(r, 1) \equiv 0, \mod p,$$

being of degree at most 3 in r, has at most 3 roots, $\bmod p$, and so there exists an integer r_p such that

$$u_{i_p}(r_p, 1) \not\equiv 0, \mod p.$$

Next, defining r to a solution of the simultaneous congruences

$$r = r_p, \mod p; \qquad p \mid \lambda$$

and writing $\xi_i = u_i(r, l)$, we deduce that h.c.f. $(\xi_1, \xi_2, \xi_3) = 1$ since λ is the highest common factor of the resultant system for u_1, u_2, u_3. Also there exists a positive number μ such that $\mu\xi_1, \mu\xi_2, \mu\xi_3$ is primitively represented by v_1, v_2, v_3, where $\mu \neq 1$ by Lemma 3.

Replace the triplets by equivalent triplets $U_1(\varrho, \sigma)$, $U_2(\varrho, \sigma)$, $U_3(\varrho, \sigma)$ and $V_1(R, S)$, $V_2(R, S)$, $V_3(R, S)$ so that the solutions ξ_1, ξ_2, ξ_3 and $\mu\xi_1, \mu\xi_2, \mu\xi_3$ are given, respectively, by $\varrho = 1$, $\sigma = 0$ and $R = 1$, $S = 0$. Then, letting

$$\varrho = \alpha R + \beta S, \quad \sigma = \gamma R + \delta S$$

be the real substitution of modulus 1 that transforms U_1, U_2, U_3 into V_1, V_2, V_3 in accordance with Lemma 1, we have that $\alpha/\mu_1 = 1$, $\gamma = 0$, where $\mu_1 = \mu^{1/3}$, and hence that $\alpha = \mu_1$, $\gamma = 0$, $\delta = 1/\mu_1$, since $\alpha\delta - \beta\gamma = 1$. Furthermore, $\alpha, \beta, \gamma, \delta$ being in rational ratio, μ_1^2 is rational; hence μ_1 is an integer $k > 1$ so that $\mu = k^3$, and β is rational.

We consider the effect of this transformation on $U_i(\varrho, \sigma)$, which we write as $a_i\varrho^3 + b_i\varrho^2\sigma + c_i\varrho\sigma^2 + d_i\sigma^3$, where $a_i = \xi_i$. We have

$$\begin{aligned} V_i(R, S) &= U_i(kR + \beta S, S/k) \\ &= a_ik^3R^3 + kR^2S(3a_i\beta k + b_i) + \frac{RS^2}{k}(3a_i\beta^2k^2 + 2b_i\beta k + c_i) \\ &\qquad + \frac{S^3}{k^3}(a_i\beta^3k^3 + c_i\beta^2k^2 + c_i\beta k + d_i) \,. \end{aligned}$$

An examination of the coefficient of S^3/k^3 for $i = 1, 2, 3$ leads first to the conclusion that βk is an integer on account of h.c.f. $(a_1, a_2, a_3) = 1$ and then to the conclusion that the coefficient of R^2S in V_i is divisible by k. Hence

$$W_i(R, S) = kV_i(R/k, S)$$

has integral coefficients and there is a triplet W_1, W_2, W_3 with invariants $(\lambda/k^3)D_{k_1,k_2,k_3}$. Since this is not in accordance with the definition of λ, the class number associated with $\lambda D_{k_1,k_2,k_3}$ is 1.

THEOREM 4. *In the notation of Theorem 3 let the class numbers of triplets with invariants* $\lambda_1 D_{k_1,k_2,k_3}$ *and those with invariants* $\lambda_2 D_{k_1,k_2,k_3}$ *be both* 1, *where* $(\lambda_1\lambda_2, 6) = 1$. *Then* λ_1, λ_2 *have the same prime factors.*

Let $u_1(r, s)$, $u_2(r, s)$, $u_3(r, s)$ and $v_1(R, S)$, $v_2(R, S)$, $v_3(R, S)$ be triplets with invariants $\lambda_1 D_{k_1,k_2,k_3}$ and $\lambda_2 D_{k_1,k_2,k_3}$, respectively. Then, by the argument used in the proof of Theorem 3, there is a triplet of relatively prime numbers ξ_1, ξ_2, ξ_3 such that u_1, u_2, u_3 primitively represents ξ_1, ξ_2, ξ_3 and v_1, v_2, v_3 represents $\mu_2\xi_1, \mu_2\xi_2, \mu_2\xi_3$ for some positive divisor μ_2 of λ_2. Also, by having chosen u_1, u_2, u_3 and v_1, v_2, v_3 to be appropriate representatives in the classes to which they belong, we may assume that these primitive representations are given by $r = 1$, $s = 0$ and $R = 1$, $S = 0$. Furthermore, as in the proof of Theorem 2, ξ_1, ξ_2, ξ_3 is primitively represented by the triplet w_1, w_2, w_3 through values $R = 1$, $S = 0$, where

$$w_i(R, S) = \frac{1}{\mu_2} v_i(R, \mu_2 S)$$

and w_1, w_2, w_3 has invariants $\mu_2^3\lambda_2 D_{k_1,k_3,k_3}$. By a previous argument

$$u_i(\alpha R + \beta S, \gamma R + \delta S) = w_i(R, S), \tag{9}$$

in which $\alpha = 1$, $\gamma = 0$, $\delta = (\mu_2^3\lambda_2/\lambda_1)^{1/9}$ because the modulus $\alpha\delta - \beta\gamma$ of the transforming substitution must be $(\mu_3^2\lambda_2/\lambda_1)^{1/9}$; furthermore β and δ are rational. Writing $u_i(r, s)$ as $a_i r^3 + b_i r^2 s + c_i r s^2 + d_i s^3$, we express (9) in the form

$$w_i(R, S) = a_i R^3 + R^2 S(3a_i\beta + b_i\delta) + RS^2(3a_i\beta^2 + 2b_i\beta\delta + c_i\delta^2)$$
$$+ S^3(a_i\beta^3 + b_i\beta^2\delta + c_i\beta\delta^2 + d_i\delta^3),$$

from the coefficient of S^3 in which we infer, in virtue of h.c.f. $(a_1, a_2, a_3) = 1$, that the denominator of β expressed in lowest terms is a divisor of the denominator of δ expressed in lowest terms. Hence there exist integers l, m such that $\beta = l\delta + m$ and hence the substitution $r = \alpha R + \beta S$, $S = \gamma R + \delta S$ is compounded of the substitutions

$$\begin{array}{lll} r = r_1 + ls_1 & r_1 = R_1 & R_1 = R + mS \\ s = s_1 & s_1 = \delta s_1 & S_1 = S, \end{array}$$

of which the first and the third are both unimodular. Moreover, since the first substitution takes $r = 1$, $s = 0$ into $r_1 = 1$, $s_1 = 0$, it is clear that we can assume that the triplet u_1, u_2, u_3 was so chosen that $l = 0$ and that hence

$$u_i(R_1, \delta S_1) = a_i R_1^3 + b_i\delta R_1^2 S_1 + c_i\delta^2 R_1 S_1^2 + d_i\delta^3 S_1^3$$

has integral coefficients. If $\mathcal{K}$ be the denominator of δ (in lowest terms), then $\mathcal{K}|b_i$, $\mathcal{K}^2|c_i$, $\mathcal{K}^3|d_i$ and $u_i(r, s)$ is of the form

$$a_i r^3 + \mathcal{K} b_i' r^2 s + \mathcal{K}^2 c_i' r s^2 + \mathcal{K}^3 d_i' s^3, \tag{10}$$

from which we infer that $\mathcal{K} = 1$ in view of the fact that any substitution of the form $r = \varrho$, $s = \sigma + (\eta/\mathcal{K})\varrho$, where $0 < \eta < \mathcal{K}$, transforms the triplet given by (10) into an inequivalent integral triplet with the same invariants.

We thus have that δ is an integer and hence $\lambda_1 | \mu_2^3 \lambda_2$. Therefore all prime factors of λ_1 divide λ_2 since $\mu_2 | \lambda_2$. Similarly all prime factors of λ_2 divide λ_1 and the theorem therefore is true.

Theorems 3 and 4 may be illustrated by a reference to the special curve $x_1^2 x_3 = l x_2^3$, where $l = p^2 q^2$ and p, q are distinct primes. Here the non-zero values of D_{k_1, k_2, k_3} are $D_{0,3,0} = l$ and $D_{2,0,1} = -1$. Corresponding to the invariant systems $\lambda_i pq D_{k_1, k_2, k_3}$ for $\lambda_1 = 1$, $\lambda_2 = p^3$, $\lambda_3 = q^3$ there is for each λ_i just one class of triplets; the simplest representatives of the single classes are as follows;

$$\begin{array}{llll} x_1 = pqr^3, & x_2 = r^2 s, & x_3 = s^3 & (\lambda_2 = 1) \\ x_1 = pr^3, & x_2 = r^2 s, & x_3 = q^2 s^3 & (\lambda_2 = q^3) \\ x_1 = qr^3, & x_2 = r^2 s, & x_3 = p^2 s^3 & (\lambda_3 = p^3)\,. \end{array}$$

References

1. Cantor, G., De aequationibus Secundi gradus indeterminatis, reproduced in the *Collected Works*.

2. Hooley, C., On the Diophantine equation $ax^2 + by^2 + cz^2 + 2fyz + 2gzx + 2hxy = 0$, *Arch. Math.* 19 (1968), 472—478.

Received January 20, 1971.

Christopher Hooley
Department of Pure Mathematics
University College of South Wales and Monmouthshire
Cardiff
United Kingdom.