

# A DIOPHANTINE EQUATION OVER A FUNCTION FIELD

J. W. S. CASSELS

Dedicated to Kurt Mahler on his 75th birthday

(Received 9 January 1978)

Communicated by J. H. Coates

## Abstract

Let  $x_0, x_1, x_2, x_3$  be polynomials in a variable  $t$  and with coefficients in a field  $k$  of characteristic 0. If  $x_0^2 + x_1^2 = t(x_2^2 - x_3^2)$  and  $t(x_0^2 x_1^2) = x_2^2 + x_3^2$ , then  $x_0 = x_1 = x_2 = x_3 = 0$ . This partially answers a question of Pjatetskii-Šapiro and Šafarevič about the  $K3$ -surface  $x_0^4 + x_3^4 = x_1^4 + x_2^4$ . The proof uses a technique of M. R. Christie.

*Subject classification (Amer. Math. Soc. (MOS) 1970):* 14 J 25

## 1. Introduction

**THEOREM 1.** *Let  $k$  be a field of characteristic 0 and let  $t$  be transcendental over  $k$ . Then there are no  $k(t)$ -rational points  $(x_0, x_1, x_2, x_3)$  on the curve*

$$x_0^2 + x_1^2 = t(x_2^2 - x_3^2), \quad (1.1)$$

$$t(x_0^2 - x_1^2) = x_2^2 + x_3^2. \quad (1.2)$$

This partially answers a question raised by Pjatetskii-Šapiro and Šafarevič (1971). Dem'janenko (1977) claims to have proved Theorem 1 without the restriction on the characteristic of  $k$ , but his argument appears to be incomplete (see Section 5 below). I cannot decide whether Theorem 1 remains true in prime characteristic. Theorem 1 will be deduced from:

**THEOREM 2.** *Let  $k, t$  be as in the enunciation of Theorem 1. If  $\xi, \eta \in k(t)$  satisfy*

$$\xi(\xi - 1)(\xi - t^4) = \eta^2, \quad (1.3)$$

then

$$\xi = 0, 1, t^2 \text{ or } t^4. \quad (1.4)$$

Theorem 2 will be proved by a technique of M. R. Christie (1976). There is clearly no loss of generality in proving Theorems 1 and 2 under the additional assumption that  $k$  is algebraically closed.

## 2. Deduction of Theorem 1 from Theorem 2

Put

$$a = x_0 + ix_1, \quad b = x_0 - ix_1, \quad (2.1)$$

$$c = x_2 + x_3, \quad d = x_2 - x_3, \quad (2.2)$$

so that (1.1) and (1.2) become

$$ab = tcd, \quad (2.3)$$

$$t(a^2 + b^2) = c^2 + d^2. \quad (2.4)$$

Put

$$\alpha = a/c, \quad \beta = a/d. \quad (2.5)$$

so that by (2.3) we have

$$a : b : c : d = \alpha\beta : t : \beta : \alpha. \quad (2.6)$$

Then (2.5) becomes

$$\alpha^2 + \beta^2 = t(t^2 + \alpha^2\beta^2), \quad (2.7)$$

that is

$$(\alpha^2 - t^3) = \beta^2(t\alpha^2 - 1). \quad (2.8)$$

Put

$$\xi = t\alpha^2. \quad (2.9)$$

Then

$$\xi(\xi - 1)(\xi - t^4) = \eta^2, \quad (2.10)$$

where

$$\eta = t\alpha\beta(t\alpha^2 - 1). \quad (2.11)$$

If now  $\xi$  is given by (1.4), then there is clearly no  $\alpha$  satisfying (2.9).

## 3. Theorems of Christie and Hellegouarch

We enunciate some results which we shall need later.

Let  $K$  be any field of characteristic 0, let  $k$  be any algebraically closed field containing  $K$  and let  $t$  be transcendental over  $k$ . Suppose that

$$u, v \in K[t], \quad (3.1)$$

that

$$u \neq 0, \quad v \neq 0, \quad (3.2)$$

and that

$$u/v \notin K. \quad (3.3)$$

Then

$$\xi(\xi-u)(\xi-v) = \eta^2 \quad (3.4)$$

is an elliptic curve defined over  $K(t)$  but not  $k(t)$ -equivalent to an elliptic curve defined over  $k$ . We denote by  $G$  the group of points on (3.4) defined over  $k(t)$ , so  $G$  is finitely generated by the function-field analogue of the Mordell–Weil Theorem.

For  $d \in K^*$ , we consider also the curve

$$x(x-u)(x-v) = dy^2 \quad (3.5)$$

and denote the group of points defined over  $K(t)$  by  $H(d)$ . We shall identify  $H(d)$  with a subgroup of  $G$  by putting  $\xi = x$ ,  $\eta = d^{1/2}y$ .

**THEOREM 3** (Christie (1976), Proposition 2). *Suppose that  $u, v$  and  $u-v$  all split into the product of linear factors in  $K[t]$ . Then there is a finite set  $D \subset K^*$  such that the  $H(d)$ ,  $d \in D$  generate a group of finite index in  $G$ .*

Christie considers only the case when  $k$  is the field of complex numbers and  $K$  is algebraic over  $\mathbb{Q}$  but his argument is clearly general. He writes  $k$  for our  $K$  and works with  $a, b$  where  $u = a + 2b$ ,  $v = a - 2b$ .

We need only the

**COROLLARY.** *Suppose that  $G$  is infinite. Then  $H(d)$  is infinite for some  $d \in K^*$ .*

We also require:

**THEOREM 4** (Hellegouarch (1970), Théorème 8). *Let  $t$  be transcendental over the field  $k$  of characteristic 0 and let  $u \neq 0$ ,  $v \neq 0$  be elements of  $k[t]$  such that  $u/v \notin k$ . Then the group of points  $(\xi, \eta)$  on (3.4) defined over  $k(t)$  has no  $p$ -torsion, where  $p$  is any prime other than 2 or 3.*

**COROLLARY.** *Suppose that  $G$  has  $p$ -torsion for some  $p \neq 2$ . Then there is a point  $(\alpha, \beta)$  on (3.4) with  $\alpha, \beta \in k(t)$  and*

$$3\alpha^4 - 4(u+v)\alpha^3 + 6uv\alpha^2 + u^2v^2 = 0. \quad (3.6)$$

For, as Christie (1976) remarks (end of his Section 3), this is the condition that  $(\alpha, \beta)$  have order 3.

We also recall for convenience

LEMMA 1. Let  $L$  be a field of characteristic  $\neq 2$  and let  $M = M(\sqrt{s})$  for  $s \in L$ . Suppose that there are infinitely many points defined over  $M$  on the elliptic curve

$$f(\xi) = \eta^2, \quad (3.7)$$

where  $f(\xi) \in L[\xi]$  is a cubic polynomial. Then there are infinitely many points defined over  $L$  either on (3.7) or on

$$f(\xi) = s\eta^2. \quad (3.8)$$

LEMMA 2. Let  $e_1, e_2, e_3$  be distinct elements of a field  $L$  of characteristic  $\neq 2$  and let  $G$  be the Mordell–Weil group of the elliptic curve

$$(\xi - e_1)(\xi - e_2)(\xi - e_3) = \eta^2.$$

For  $j = 1, 2, 3$  let  $\varphi_j$  be the map from  $G$  to  $L^*/(L^*)^2$  defined by

$$\varphi_j(\xi, \eta) = \begin{cases} (\xi - e_j)(L^*)^2 & \text{if } \xi \neq e_j \\ (e_l - e_j)(e_m - e_j)(L^*)^2 & \text{if } \xi = e_j, \text{ where } l \neq m \neq j \neq l. \end{cases}$$

Then  $\varphi_j$  is a group homomorphism. Further,

$$2G = \bigcap_{j=1}^3 \text{Ker}(\varphi_j).$$

#### 4. Proof of Theorem 2

The points on (1.4) with  $\xi = 0, 1, t^4$  are of order 2 and those with  $\xi = t^2$  are of order 4. It is routine to show using Lemma 2 that there is no further 2-torsion and an application of Theorem 4, Corollary shows that there is no further torsion. We shall suppose that there are infinitely many points on (1.4) defined over  $k(t)$  and will ultimately arrive at a contradiction.

We first apply Lemma 1 with  $s = t^2$  and  $L = k(s)$ . There will thus be infinitely many points defined over  $k(s)$  on at least one of the curves

$$\xi(\xi - 1)(\xi - s^2) = \eta^2, \quad (4.1)$$

$$\xi(\xi - 1)(\xi - s^2) = s\eta^2. \quad (4.2)$$

To (3.4) we apply the same argument. If it has infinitely many  $k(s)$ -points, then there are infinitely many  $k(r)$ -points on one of

$$\xi(\xi - 1)(\xi - r) = \eta^2, \quad (4.3)$$

$$\xi(\xi - 1)(\xi - r) = r\eta^2, \quad (4.4)$$

where  $r = s^2 = t^4$  is transcendental over  $k$ .

The curve (4.4) reduces to (4.3) on taking  $r^{-1}\xi, r^{-1}\eta, r^{-1}$  for  $\xi, \eta, r$  respectively. Hence we need consider only (4.2) over  $k(s)$  and (4.3) over  $k(r)$ . We suppose, as we may, that  $k$  is algebraically closed.

The equation (4.3) requires no deep machinery. On considering possible common factors on the left-hand side we have

$$\xi = r^\alpha \lambda^2, \quad (4.5)$$

$$\xi - 1 = (r-1)^\beta \mu^2, \quad (4.6)$$

$$\xi - r = r^\alpha (r-1)^\beta \nu^2, \quad (4.7)$$

where  $\lambda, \mu, \nu \in k(r)$  and  $\alpha, \beta = 0$  or  $1$ . Hence, by Lemma 2,  $G^*/2G^*$  has order at most  $2^2$ , where  $G^*$  is the group of points defined over  $k(r)$ . Since all the points of order 2 are defined over  $k(r)$ , there can thus be no points of infinite order.

There remains (4.2). We put

$$X = s\xi, \quad Y = s^2\eta \quad (4.8)$$

and so have to consider

$$X(X-s)(X-s^3) = Y^2 \quad (4.9)$$

over  $k(s)$ . On considering common factors of the factors on the left-hand side we have

$$X = s^\alpha \lambda^2, \quad (4.10)$$

$$X-s = s^\beta (s-1)^\delta (s+1)^\epsilon \mu^2, \quad (4.11)$$

$$X-s^3 = s^\gamma (s-1)^\delta (s+1)^\epsilon \nu^2, \quad (4.12)$$

where  $\lambda, \mu, \nu \in k(s)$  and  $\alpha, \beta, \gamma, \delta, \epsilon = 0$  or  $1$  with  $\alpha + \beta + \gamma \equiv 0 \pmod{2}$ . On considering  $(X, Y) + (X_0, Y_0)$  if necessary, where  $Y_0 = 0$  and  $X_0 = 0, s$  or  $s^3$ , we may suppose by Lemma 2 without loss of generality that

$$\alpha = \beta = \gamma = 0. \quad (4.13)$$

We now apply Theorem 3 Corollary with  $K = \mathbf{Q}$ ,  $s$  instead of  $t$ , and  $u = s, v = s^3$ . If there are infinitely many points on (4.9) over  $k(s)$  then there is some  $d \in \mathbf{Q}^*$  such that there are infinitely many points over  $\mathbf{Q}(s)$  on

$$x(x-s)(x-s^3) = dy^2. \quad (4.14)$$

By (4.10)–(4.13) we need consider only the following four cases, in all of which

$$l, m, n \in \mathbf{Q}^*, \quad lmn \in d(\mathbf{Q}^*)^2 \quad (4.15)$$

and

$$U, V, W \in \mathbf{Q}(s): \quad (4.16)$$

$$\left. \begin{aligned} x &= lU^2, \\ x-s &= mV^2, \\ x-s^3 &= nW^2; \end{aligned} \right\} \quad (\text{I})$$

$$\left. \begin{aligned} x &= lU^2 \\ x-s &= m(s^2-1)V^2, \\ x-s^3 &= n(s^2-1)W^2; \end{aligned} \right\} \quad (\text{II})$$

$$\left. \begin{aligned} x &= lU^2, \\ x-s &= m(s-1)V^2, \\ x-s^3 &= n(s-1)W^2; \end{aligned} \right\} \quad (\text{III})$$

$$\left. \begin{aligned} x &= lU^2 \\ x-s &= m(s+1)V^2 \\ x-s^3 &= n(s+1)W^2. \end{aligned} \right\} \quad (\text{IV})$$

We consider these in turn.

*Case I.* We have

$$lU^2 - s = mV^2.$$

On localizing at  $s = 0$ , this is clearly seen to imply that

$$l/m \in (\mathbf{Q}^*)^2.$$

Similarly

$$l/n \in (\mathbf{Q}^*)^2;$$

and so by (4.15),

$$l, m, n \in d(\mathbf{Q}^*)^2.$$

Hence  $(x, y) = 2(x_1, y_1)$  by Lemma 2, where  $(x_1, y_1)$  is a point on (4.14) defined over  $\mathbf{Q}(s)$ . Since the group of points on (4.14) over  $\mathbf{Q}(s)$  is finitely generated, if there are infinitely many such points, then there will be some of them not in Case I.

*Case II.* We have

$$lU^2 - s = m(s^2-1)V^2.$$

On localizing at  $s = 1$ , we have

$$l \in (\mathbf{Q}^*)^2$$

and on localizing at  $s = -1$  we have

$$-l \in (Q^*)^2.$$

Hence Case II cannot occur.

*Case III.* We have

$$lU^2 - s = m(s-1)V^2.$$

On localizing at  $s = 1$ , we have

$$l \in (Q^*)^2$$

and on localizing at  $s = 0$  we have

$$-l/m \in (Q^*)^2.$$

Similarly,

$$lU^2 - s^3 = n(s-1)W^2;$$

and so

$$-l/n \in (Q^*)^2.$$

Hence, on absorbing elements of  $Q^*$  into  $U, V, W$ , we need consider only

$$U^2 - s = (1-s)V^2,$$

$$U^2 - s^3 = (1-s)W^2.$$

On specializing  $s$  to 2 we have

$$u^2 - 2h^2 = -v^2, \quad (4.17)$$

$$u^2 - 8h^2 = -w^2, \quad (4.18)$$

where  $u, v, w, h \in Q$  and are not all zero. By homogeneity we may suppose that  $u, h$  are integers without common factor. Then (4.17) implies that  $u$  is odd, whereas (4.18) implies that  $u$  is even. The contradiction shows that Case III cannot occur.

*Case IV.* This reduces to Case III on changing the signs of  $X$  and  $s$ .

This concludes the proof of Theorem 2.

Hellegouarch's proof of Theorem 4 is somewhat obscure and so we note that it is not really essential to our argument for the following two reasons.

(i) We could have used the analogue of the Nagell–Lutz Theorem for  $k(t)$ . This asserts that if  $f(\xi)$  is a cubic with coefficients in  $k[t]$  and top coefficients 1, and if  $\xi, \eta$  is a point of finite order defined over  $k(t)$  on  $y^2 = f(\xi)$ , then  $\xi, \eta \in k[t]$  and either  $\eta = 0$  or  $\eta^2$  divides the discriminant of  $f$ . This reduces the determination of

the torsion on (1.3) to a rather tedious case-by-case discussion. (It is enough to look at the odd torsion on (4.2) and (4.9).)

(ii) So far as the proof of Theorem 1 is concerned, it would, in any case, be enough to have the weaker form of Theorem 2 which asserts that there are no points of infinite order on (1.3) and that the 2-torsion is given by (1.4). It then follows from Lemma 2 that  $\xi$  is a square for all torsion points: so (2.9) cannot hold.

### 5. Dem'janenko's argument

By a process similar to that in our Section 2, Dem'janenko deduces Theorem 1 from the assertion that the points  $(u, v, w)$  defined over  $k(t)$  on

$$u^4 - 2(2t^4 - 1)u^2w^2 + w^4 = v^2 \quad (5.1)$$

satisfy

$$u = 0 \quad \text{or} \quad w = 0 \quad \text{or} \quad u^2 + w^2 = 0. \quad (5.2)$$

By homogeneity we may suppose that  $u, v, w \in k[t]$ . Dem'janenko then considers a point  $(u, v, w)$  for which  $u \neq 0$ ,  $w \neq 0$  and

$$\deg u + \deg w$$

is minimal. By a descent argument he shows that then (5.2) holds. This does not, however, imply that (5.2) holds for *every* solution  $u, v, w$ . It does not seem to me that Dem'janenko's argument can be modified so as to give a proof. Since (5.1) is isogenous to (1.3) we have, however, shown that Dem'janenko's assertion is true in characteristic 0.

ADDED IN PROOF. Professor Swinnerton-Dyer has shown me a geometric proof of Theorem 1 which extends to some (but not all) finite characteristics.

### References

- M. R. Christie (1976), "Positive definite functions of two variables which are not the sum of three squares", *J. Number Theory* **8**, 224–232.
- V. A. Dem'janenko (1977), "An indeterminate equation" (Russian), *Zap. Naučn. Sem. Leningrad. Otdel. Mat. Inst. Steklov (LOMI)*, **67**, 163–166.
- Y. Hellegouarch (1970), "Étude des points d'ordre fini des variétés abéliennes de dimension un définies sur un anneau principal", *J. reine. angew. Math.* **244**, 20–36.
- I. I. Pjatetskii-Šapiro and I. R. Šafarevič (1971), "Torelli's theorem for K3 algebraic surfaces" (Russian), *Izv. Akad. Nauk SSSR (ser. mat.)* **35**, 530–572, especially the last section.

Department of Pure Mathematics and Mathematical Statistics  
16 Mill Lane  
Cambridge CB2 1SB  
United Kingdom