SOME QUARTIC DIOPHANTINE EQUATIONS OF GENUS 3

L. J. MORDELL

Let $f(x)=f(x_1, x_2, \cdots, x_n)$ be a polynomial in the x_i with integer coefficients. Consider the diophantine equation

$$f(x_1, x_2, \cdots, x_n) = 0. \tag{1}$$

Two questions arise:

(I) to find integer solutions,

(II) to find rational solutions.

If for (II), we put $x_1=X_1/X_{n+1}, \cdots, x_n=x_n/X_{n+1}$, then $f(x)=0$ becomes a homogeneous equation, say,

$$f(X_1, X_2, \cdots, X_{n+1}) = 0, \tag{2}$$

where $X_{n+1}\neq 0$. We ignore the trivial solution $(X)=0$ of any homogeneous equation and consider solutions (X), (kX), k a constant, as identical, and so we always suppose that $(X_1, X_2, \cdots, X_{n+1})=1$. Thus question (II) is included in (I).

An interesting and important problem is to find conditions under which the equation $f(x)=0$ has only a finite number of integer solutions. A further question would be to find estimates for the magnitude of the solutions in terms of the coefficients of $f(x)$. Several methods are known. Thus (1) is impossible if there exists a number M for which the congruence $f(x)\equiv 0 \pmod{M}$ is impossible, but when $f(x)$ is homogeneous, we also require that the x have no common divisor with M.

Results may sometime [1], [2] be obtained by writing $f(x)=0$ in the form

$$F(x)G(x) = H^h(x), \qquad h \geqq 1, \tag{3}$$

where $F(x)$, $G(x)$, $H(x)$ are polynomials in x with integer coefficients. Some values of x may be excluded by congruence conditions, and the others, except perhaps for a finite number, if the divisors of $H(x)$ have special linear forms and $G(x)$ is not of such a form. This happens for instance when $H(x)=H(x_1, x_2)$ is a norm form in a quadratic field, and sometimes when $H(x)=H(x_1, x_2, x_3)$ in special cubic fields. Again from (3) when $h>1$, we can deduce either $H(x)=0$ or simultaneous equations such as

Received by the editors August 11, 1965.

$$F(x) = k_1 H_1^h(x), \qquad G(x) = k_2 H_2^h(x), \tag{4}$$

where k_1, k_2 are constants, finite in number; but usually $F(x)$, $G(x)$, $H(x)$ are homogeneous functions, $n=3$, and $H(x)=H(x_1, x_2, x_3)$ in (3).

Of course, by Siegel's theorem, there are only a finite number of integer solutions if $n=2$ and the genus of the equation exceeds one. The situation, however, is very different when rational solutions are required, or integer solutions when the equation is written in the homogeneous form. Very little indeed is known about this. We have a conjecture of mine enunciated nearly 45 years ago.

CONJECTURE. *There are only a finite number of rational solutions of a polynomial equation $f(x)$ in two variables and of genus >1.*

Some instances are known for the quartic equation of genus 3,

$$Ax^4 + By^4 + Cz^4 = 0,$$

which includes Fermat's equation $x^4+y^4-z^4=0$ as a special case. Results are usually found on replacing z^2 by z; then a curve of genus 1 arises.

Three theorems, relevant to the conjecture, are now proved for some quartics which in general are of genus 3 since they have no double points.

THEOREM I. *The equation*

$$k_1(ax^2 + by^2 + cz^2)(a'x^2 + b'y^2 + c'z^2) = k_2(px^2 + qy^2 + rz^2)^2, \tag{5}$$

or say,

$$k_1 FG = k_2 H^2,$$

where $(k_1, k_2)=1$, k_2 is square free, $k_1>0$, $k_2>0$ and have only divisors $\equiv 1 \pmod 8$, has no integer solutions with $(x, y, z)=1$ provided that the coefficients are integers such that

(I) $a \equiv b \equiv c \equiv -1 \pmod 8$,

and that either

(IA) $a>0$, $b>0$, $c>0$, *or*

(IB) $a'>0$, $b'>0$, $c'>0$, *or*

(IC) $-aa' \geqq 0$, $a(ab'-a'b) \geqq 0$, $a(ac'-a'c) \geqq 0$.

(II) *All odd divisors of*

$$\Delta = \begin{vmatrix} a, & b, & c, \\ a', & b', & c', \\ p, & q, & r, \end{vmatrix} \tag{6}$$

are $\equiv 1 \pmod 8$, and either

(III) *Δ is odd, or*

(IV) Δ *is even and either*
(IVA) $a' \equiv 0 \pmod 2$, $b' \equiv c' \equiv 1 \pmod 2$, $b'+c' \equiv 4, 6 \pmod 8$, *or*
(IVB) $a' \equiv 1 \pmod 8$, $a'b - ab' \equiv a'c - ac' \equiv -2 \pmod{16}$, *or*
(IVC) $a' \equiv ka$, $b' \equiv kb$, $c' \equiv kc$, $k \equiv -1 \pmod 4$.

Any common factors of F, G can only be divisors of k_1k_2, and of H, and so must be divisors of Δ.

We first consider the solutions for which $px^2+qy^2+rz^2 \neq 0$. Then we cannot have both $F<0$, $G<0$. It suffices to prove this for (IC).

If $ax^2+by^2+cz^2 = -\epsilon < 0$, then

$$a^2(a'x^2 + b'y^2 + c'z^2) = a(-a'\epsilon + (ab' - a'b)y^2 + (ac' - a'c)z^2)$$
$$\geqq 0,$$

a contradiction.

Suppose next that Δ is odd. Then if $H \neq 0$,

$$F = k_3w^2, \qquad G = k_4w_1^2, \tag{7}$$

where $k_3 \equiv k_4 \equiv 1 \pmod 8$, are taken from a finite set and w, w_1 are integers. Here $F = k_3w^2$ is impossible, for taking a congruence (mod 8), we have

$$x^2 + y^2 + z^2 + w^2 \equiv 0 \pmod 8,$$

and this requires $x \equiv y \equiv z \equiv w \equiv 0 \pmod 2$.

Suppose next that Δ is even. Then in addition to (7) which is still impossible, we have also

$$F = 2k_3w^2, \qquad G = 2k_4w_1^2, \tag{8}$$

where $k_3 \equiv k_4 \equiv 1 \pmod 8$, are taken from a finite set. We now deal with $F = 2k_3w^2$. Clearly w is not even since then $x^2+y^2+z^2 \equiv 0 \pmod 8$ and so $x \equiv y \equiv z \equiv 0 \pmod 2$. Hence w is odd and then $x \equiv 0 \pmod 4$, $y \equiv z \equiv 1 \pmod 2$, etc. The second equation in (8),

$$a'x^2 + b'y^2 + c'z^2 = 2k_4w_1^2$$

leads now to the corresponding congruences

$$b' + c' \equiv 2w_1^2 \pmod 8, \qquad a' + c' \equiv 0 \pmod 2, \qquad a' + b' \equiv 0 \pmod 2,$$

all of which are impossible from (IVA).

For (IVB), on eliminating x^2 in (8), we have

$$(a'b - ab')y^2 + (a'c - ac')z^2 = 2k_3a'w^2 - 2k_4aw_1^2.$$

This becomes

$$-2y^2 - 2z^2 \equiv 2w^2 + 2w_1^2 \pmod{16},$$

and this is impossible.

For (IVC), we have

$$kw_1^2 - w^2 \equiv 0 \pmod 8,$$

and is impossible since w is odd.

We now consider the solutions with $px^2+qy^2+rz^2=0$. Since $a\equiv b\equiv c\equiv -1 \pmod 8$, $ax^2+by^2+cz^2\neq 0$, and so $a'x^2+b'y^2+c'z^2=0$. This excludes (IB).

Suppose that $(x, y, z)=(x_0, y_0, z_0)$ is a solution. Then

$$\frac{x_0^2}{b'r-c'q} = \frac{y_0^2}{c'p-a'r} = \frac{z_0^2}{a'q-b'p},$$

and so we may take

$$b'r - c'q = dx_0^2, \qquad c'p - a'r = dy_0^2, \qquad a'q - b'p = dz_0^2.$$

Hence $\Delta = a(b'r-c'q)+\cdots = d(ax_0^2+by_0^2+cz_0^2) = d\Delta_0$, and so the odd factors of d and Δ_0 are $\equiv 1 \pmod 8$. Also

$$\Delta_0 \equiv -x_0^2 - y_0^2 - z_0^2 \pmod 8.$$

We now examine the cases (IA), (IC). We exclude $x_0\equiv y_0\equiv z_0\equiv 1 \pmod 2$ since then $\Delta_0\equiv -3 \pmod 8$, and if $\Delta_0 \not\equiv -1$, we exclude $x_0\equiv 1$, $y_0\equiv z_0\equiv 0 \pmod 2$: and if $\Delta_0 \not\equiv -2$, we exclude $x_0\equiv y_0\equiv 1 \pmod 2$, $z_0\equiv 0 \pmod 4$, since then $\Delta_0\equiv -2 \pmod 8$. Hence we have $x_0\equiv y_0\equiv 1 \pmod 2$, $z_0\equiv 2 \pmod 4$, etc. Now $\Delta_0\equiv 2 \pmod 8$, and there are three possibilities $b'+c'+4a'\equiv 0 \pmod 8$, etc. These contradict (IVA), (IVC), and also (IVB), which gives $b'\equiv c'\equiv -1 \pmod 8$. Hence there are no solutions[1] with (IA), i.e., $a>0$, $b>0$, $c>0$, and $\Delta_0\neq -1, -2$, in case (IC).

We now examine the possibilities $\Delta_0=\pm 1, \pm 2$. The first is typified by $(x, y, z)=(1, 0, 0)$. Then $a'=0$, $p=0$, $\Delta_0=a$, and so $a=-1$ and $\Delta=-(b'r-c'q)$. The condition (IC) gives $b'\geqq 0$, $c'\geqq 0$. We have from (III) and (IVA) the

THEOREM II. *The equation*

[1] I owe this result to Dr. J. W. S. Cassels. I had thought there might be solutions of $px^2+qy^2+rz^2=0$, $a'x^2+b'y^2+c'z^2=0$.

$$(-x^2 + by^2 + cz^2)(b'y^2 + c'z^2) = (qy^2 + rz^2)^2$$

has only the solution (1, 0, 0) *if* $b \equiv c \equiv -1 \pmod 8$; $b' \geqq 0$, $c' \geqq 0$, *and either* $b'r - c'q$ *is divisible only by odd primes* $\equiv 1 \pmod 8$, *or is also divisible by* 2 *if* b', c' *are odd and* $b' + c' \equiv 4, 6 \pmod 8$.

No results arise from $\Delta_0 = 2$.

In the proof of Theorem I, we have used the impossibility of integer solutions of

$$px^2 + qy^2 + rz^2 + sw^2 = 0, \tag{9}$$

when p, q, r, s are odd and $p \equiv q \equiv r \equiv s \pmod 8$. By a theorem of Meyer, there are other instances when (9) is impossible and this would lead to new results. It would suffice to take such an equation with $s = -1$, and then the equation (9) would still be insoluble if s were replaced by $s' \equiv -1 \pmod M$ for an easily assigned M depending on p, q, r. Then we impose the condition that the new Δ should have only factors typified by M.

THEOREM III. *The equation*

$$\left(\frac{br - cq}{a}\right)^3 x^4 + \left(\frac{cp - ar}{b}\right)^3 y^4 + \left(\frac{aq - bp}{c}\right)^3 z^4 = 0 \tag{10}$$

has no integer solution, if

(I) $a > 0$, $b > 0$, $c > 0$; $a \equiv b \equiv c \equiv -1 \pmod 8$; $(b, c) = (c, a) = (a, b) = 1$,

(II) $p \equiv 0 \pmod 8$, $q \equiv r \equiv -1 \pmod 8$,

(III) $(br - cq)/a \equiv (cp - ar)/b \equiv (aq - bp)/c \equiv 0 \pmod 1$, *and the positive odd factors of these three terms are all* $\equiv 1 \pmod 8$.

To reduce (5) with $k_1 = k_2$, to the form (4), we impose the conditions $b'c + bc' = 2qr$, $c'a + ca' = 2rp$, $a'b + ab' = 2pq$, and so

$$bca' = -aqr + brp + cpq, \tag{11}$$

etc. Then a', b', c' will be integers if p, q, r satisfy the congruences

$$cq - br \equiv 0 \pmod a, \quad ar - cp \equiv 0 \pmod b, \quad bp - aq \equiv 0 \pmod c,$$

and these congruences are compatible since $(a, b) = 1$, etc. The equation (5) now takes the form

$$(aa' - p^2)x^4 + (bb' - q^2)y^4 + (cc' - r^2)z^4 = 0,$$

or

$$\left(\frac{a^2qr - abrp - acpq}{bc} + p^2\right)x^4 + \cdots = 0,$$

or

$$a(pb - aq)(pc - ar)x^4 + \cdots = 0.$$

On replacing x by $(qc-rb)x/a$, etc., we have the equation

$$\left(\frac{qc - rb}{a}\right)^3 x^4 + \left(\frac{ra - pc}{b}\right)^3 y^4 + \left(\frac{pb - qa}{c}\right)^3 z^4 = 0.$$

Now

$$-\Delta = \begin{vmatrix} -\dfrac{aqr + brp + cpq}{bc}, & \cdots, & \cdots \\ a, & \cdots, & \cdots \\ p, & \cdots, & \cdots \end{vmatrix}.$$

On multiplying the columns by bc, ca, ab, and dividing the second row by abc, we have

$$-abc\,\Delta = \begin{vmatrix} -aqr + brp + cpq, & \cdots, & \cdots \\ 1, & \cdots, & \cdots \\ pbc, & \cdots, & \cdots \end{vmatrix}$$

$$abc\,\Delta = 2\begin{vmatrix} aqr, & brp, & cpq \\ 1, & 1, & 1 \\ pbc, & qca, & rab \end{vmatrix}$$

$$= 2\sum a^2qr(br - cq),$$

and so

$$\Delta = -2\left(\frac{br - cq}{a}\right)\left(\frac{cp - ar}{b}\right)\left(\frac{aq - bp}{c}\right). \tag{12}$$

Hence the odd factors of Δ are $\equiv 1 \pmod 8$. Since Δ is even, we have to consider both (7) which is still impossible and (8). From (11) we write (8) in the form

$$\frac{-aqr + brp + cpq}{bc}x^2 + \cdots = 2k_4w_1^2,$$

or

$$(aqr + brp + cpq)\left(\frac{x^2}{bc} + \frac{y^2}{ca} + \frac{z^2}{ab}\right) - 2\left(\frac{aqr}{bc}x^2 + \frac{brp}{ca}y^2 + \frac{cpq}{ab}z^2\right) = 2k_4w_1^2. \tag{13}$$

Since $ax^2+by^2+cz^2=2k_3w^4$, (13) becomes

$$\frac{(aqr+brp+cpq)k_3w^2}{abc}-\left(\frac{aqr}{bc}x^2+\frac{brp}{ca}y^2+\frac{cpq}{ab}z^2\right)=k_4w_1^2.$$

Hence

$$(14)\qquad (qr+rp+pq)w^2+qrx^2+rpy^2+pqz^2\equiv w_1^2 \pmod 8.$$

Since $x^2+y^2+z^2\equiv -2w^2 \pmod 8$, one of x, y, z must be even, say x, and then $y\equiv z\equiv w\equiv 1 \pmod 2$, and $x\equiv 2 \pmod 4$. Then (14) becomes

$$5qr+2rp+2pq\equiv w_1^2 \pmod 8.$$

If we take $y\equiv 2 \pmod 4$ etc., we might also have

$$5rp+2pq+2qr\equiv w_1^2 \pmod 8$$

$$5pq+2qr+2rp\equiv w_1^2 \pmod 8.$$

All these are impossible if we take $p\equiv 0 \pmod 8$, and $qr\equiv 1, 3, 7 \pmod 8$.

We now examine the condition that $(qc-rb)/a$, $(ra-pc)/b$ and $(pb-qa)/c$ should be divisible only by 2 or by primes $\equiv 1 \pmod 8$. We take arbitrary q, r such that the odd factors of $(qc-rb)/a$ are $\equiv 1 \pmod 8$, and also $q\equiv r\equiv -1 \pmod 8$. We take p so great that $bY=pc-ra>0$, $cX=pb-qa>0$, and $p\equiv 0 \pmod 8$. On putting $p=8bcP+P_1$ say, then

$$X=(pb-qa)/c=8b^2P+P_2,\qquad Y=(pc-ra)/b=8c^2P+P_3,$$

say, where $P_2\equiv P_3\equiv 1 \pmod 8$. Our problem now is to find P such that X, Y are divisible only by primes $\equiv 1 \pmod 8$ and $X>0$, $Y>0$. There should be no difficulty in finding numerical instances.

The question of the existence of an infinity of values for P is equivalent to that of the existence of an infinity of solutions of $AX+BY=C$ where X, Y have only prime factors with an assigned residue mod M_1, mod M_2 respectively. If X, Y are to be primes, this becomes a very difficult unsolved problem.

References

1. L. J. Mordell, *The diophantine equation* $y^2=ax^3+bx^2+cx+d$ *or fifty years after*, J. London Math. Soc. **38** (1963), 454–458.

2. ———, *The diophantine equation* $y^2=ax^3+bx^2+cx+d$, Rend. Circ. Mat. Palermo (2) **13** (1964), 249–256.

University of Illinois and
St. Johns College, Cambridge, England