ON SOME SEXTIC DIOPHANTINE EQUATIONS OF GENUS 2

L. J. MORDELL

Some forty-five years ago, I enunciated a still unproved

CONJECTURE. *A curve of genus greater than one, defined by a polynomial equation $f(x, y) = 0$ with rational coefficients, has only a finite number of rational points, that is, there are only a finite number of rational solutions of $f(x, y) = 0$.*

A particular case of the conjecture is given by the hyperelliptic equation,

$$(1) \quad z^2 = a_0x^6 + a_1x^5y + a_2x^4y^2 + a_3x^3y^3 + a_4x^2y^4 + a_5xy^5 + a_6y^6,$$

where the a and x, y are integers. On putting $y=1$, this becomes a curve of genus 2 if the right-hand side has no squared polynomial factor.

There are, as far as I know, very few nontrivial results for such equations. It may therefore be of interest to give some instances. The results are proved by elementary means on applying an idea that I have previously used, namely, that some congruences

$$(2) \quad g(x, y, z, w) \equiv c \pmod{2^\alpha},$$

where g is a quadratic form, impose simple conditions on the variables. Thus let $c=0$ and

$$g(x, y, z, w) = x^2 + y^2 + z^2 + w^2.$$

Then if $\alpha=2$, x, y, z, w are either all even or all odd. If $\alpha=3$, x, y, z, w are all even.

We consider the equation

$$(3) \quad z^2 = (a_1x^2 + b_1y^2)(a_2x^2 + b_2y^2)(a_3x^2 + b_3y^2),$$

where the a and the b are integers. We suppose that either all the a and b are positive, or that in one pair, a and b have opposite signs. This means that all the three factors in (3) are positive.

THEOREM. *The equation (3) has no integer solutions except $(0, 0, 0)$ if all the following conditions are satisfied,*

- (i) $a_1 + a_2 + a_3 \equiv -1 \pmod{4}$, $b_1 + b_2 + b_3 \equiv 0 \pmod{4}$,
- (ii) *only one b is even,*

Received by the editors June 6, 1968.

(iii) *none of the sets a_1, a_2, a_3 or $a_1+b_1, a_2+b_2, a_3+b_3$ are $\equiv 1, 1, 1 \pmod{4}$; or to a permutation of $(0, 1, 2)$,*

(iv) *$a_2b_3-a_3b_2, a_3b_1-a_1b_3, a_1b_2-a_2b_1$ have no common divisor, and all their odd factors are $\equiv 1 \pmod{4}$.*

The equations so found are of special interest since (3) may be everywhere locally solvable. There is no difficulty in finding any number of instances.

We may suppose that $(x, y) = 1$. Write

$$\begin{aligned}d_1 &= (a_2x^2 + b_2y^2, a_3x^2 + b_3y^2), \\d_2 &= (a_3x^2 + b_3y^2, a_1x^2 + b_1y^2), \\d_3 &= (a_1x^2 + b_1y^2, a_2x^2 + b_2y^2).\end{aligned}$$

Then $d_1 \mid (a_2b_3 - a_3b_2)$ etc. Also d_1 and d_2 are relatively prime since a common factor must also divide all of $a_2b_3 - a_3b_2$ etc. Hence from (3), if we assume $z \neq 0$, a condition which the method of proof shows is satisfied, then

$$a_1x^2 + b_1y^2 = d_2d_3f_1, \quad a_2x^2 + b_2y^2 = d_3d_1f_2, \quad a_3x^2 + b_3y^2 = d_1d_2f_3.$$

Since $(f_1, f_2) = 1$, we have $f_1 = z_1^2, f_2 = z_2^2, f_3 = z_3^2$, where the z are integers.

Two cases arise according as all the d are odd, or one only is even. The first case gives

$$\begin{aligned}(4) \quad z_1^2 &\equiv a_1x^2 + b_1y^2, \\z_2^2 &\equiv a_2x^2 + b_2y^2 \pmod{4} \\z_3^2 &\equiv a_3x^2 + b_3y^2.\end{aligned}$$

By addition,

$$z_1^2 + z_2^2 + z_3^2 + x^2 \equiv 0 \pmod{4}.$$

Then either

$$z_1 \equiv z_2 \equiv z_3 \equiv x \equiv 0 \pmod{2},$$

and since at least one b is odd, $y \equiv 0 \pmod{2}$ and then $(x, y) \neq 1$; or

$$z_1 \equiv z_2 \equiv z_3 \equiv x \equiv 1 \pmod{2}.$$

Then according as y is odd or even

$$a_1 + b_1 \equiv a_2 + b_2 \equiv a_3 + b_3 \equiv 1 \pmod{4},$$

or

$$a_1 \equiv a_2 \equiv a_3 \equiv 1 \pmod{4},$$

and these have been excluded by (iii).

Suppose next that one of the d is even, say, d_3 . Since a factor 4 can be absorbed in z_1^2, z_2^2 , we may suppose that $\frac{1}{2}d_3$ is odd. Now we have

$$(5) \quad \begin{aligned} 2z_1^2 &\equiv a_1x^2 + b_1y^2, \\ 2z_2^2 &\equiv a_2x^2 + b_2y^2, \pmod{4} \\ z_3^2 &\equiv a_3x^2 + b_3y^2. \end{aligned}$$

By addition,

$$(z_1 + z_2)^2 + (z_1 - z_2)^2 + z_3^2 + x^2 \equiv 0 \pmod{4}.$$

Two cases arise. Firstly,

$$z_1 \equiv 1, \quad z_2 \equiv 0, \quad z_3 \equiv 1, \quad x \equiv 1 \pmod{2}.$$

According as y is odd or even, we have the two cases excluded by (iii),

$$a_1 + b_1 \equiv 2, \quad a_2 + b_2 \equiv 0, \quad a_3 + b_3 \equiv 1 \pmod{4}$$

or

$$a_1 \equiv 2, \quad a_2 \equiv 0, \quad a_3 \equiv 1.$$

Secondly, either

$$z_1 \equiv 1, \quad z_2 \equiv 1, \quad z_3 \equiv 0, \quad x \equiv 0 \pmod{2},$$

and then

$$b_1y^2 \equiv 2, \quad b_2y^2 \equiv 2, \quad b_3y^2 \equiv 0 \pmod{4}.$$

Clearly y is not even, and since by (ii) at least one b is odd, y cannot be odd; or

$$z_1 \equiv z_2 \equiv z_3 \equiv x \equiv 0 \pmod{2},$$

and since $y \not\equiv 0 \pmod{2}$, $b_1 \equiv b_2 \equiv b_3 \equiv 0 \pmod{2}$ contrary to (ii).

We give some numerical illustrations. Take

$$\begin{aligned} (a_1, a_2, a_3) &= (4a + 1, 3, 4b + 3) \equiv (1, 3, 3) \pmod{4}, \\ (b_1, b_2, b_3) &= (2, 1, 1). \end{aligned}$$

Then from the enunciation of the theorem, the only condition to be satisfied is that the odd factors of $5 - 4a$, b , $8b - 4a + 5$ should be $\equiv 1 \pmod{4}$. Three instances are given by

$$(6) \quad a = 0, \quad b = 1, \quad z^2 = (x^2 + 2y^2)(3x^2 + y^2)(7x^2 + y^2),$$

$$(7) \quad a = 1, \quad b = 2, \quad z^2 = (5x^2 + 2y^2)(3x^2 + y^2)(11x^2 + y^2),$$

$$(8) \quad a = -2, \quad b = 2, \quad z^2 = (-7x^2 + 2y^2)(3x^2 + y^2)(11x^2 + y^2).$$

We show that these equations are everywhere locally solvable.

On giving x or y a fixed nonzero value, the equations are of genus two. It is known that an estimate for N , the number of solutions of the sextic congruence

$$Y^2 \equiv a_0 X^6 + \dots + a_6 \pmod{p},$$

p a prime, satisfies the inequality $N > p - (a_0/p) - 4\sqrt{p}$, where (a_0/p) is the Legendre symbol. Hence $N > 0$ if $p - 1 - 4\sqrt{p} > 0$, i.e. the congruences resulting from (6), (7), (8), are solvable if $p > 17$. However when $p = 17$, the corresponding congruences (7), (8) with $y = 1$ have $(a_0/p) = -1$, and then $N > 0$ if $p > 13$. It is then obvious that the equations taken as congruences are solvable for $z \pmod{p^a}$. We need only note that if $z \equiv 0 \pmod{p}$, we can find a solution where, say, z/p^a is a quadratic residue $\pmod{p}$.

The primes $p = 2, 3, 5, 7, 11, 13, 17$ must be considered separately. Solvability is obvious for these from the details now given.

For (6). $x = 1, y = 3, z^2/64 \equiv 1 \pmod{8}$,
 $x = 4, y = 1, z^2/9 \equiv 1 \pmod{3}$,
 $x = 1, y = 0, z^2 \equiv 1 \pmod{5}$,
 $x = 0, y = 1, z^2 \equiv 2 \pmod{7}$,
 $x = 1, y = -31, z^2/121 \equiv 9 \pmod{11}$,
 $x = 1, y = 2, z^2 \equiv 4 \pmod{13}$,
 $x = 2, y = 1, z^2 \equiv 1 \pmod{17}$.

For (7). $x = 1, y = 3, z^2/16 \equiv 1 \pmod{8}$,
 $x = 1, y = 5, z^2/9 \equiv 1 \pmod{3}$,
 $x = 3, y = 2, z^2 \equiv 4 \pmod{5}$,
 $x = 0, y = 1, z^2 \equiv 2 \pmod{7}$,
 $x = 1, y = 2, z^2 \equiv 1 \pmod{11}$,
 $x = 3, y = 1, z^2 \equiv 1 \pmod{13}$.

For (8). $x = 1, y = 0, z^2 \equiv 1 \pmod{8}$,
 $x = 1, y = 5, z^2/36 \equiv 1 \pmod{3}$,
 $x = 1, y = 0, z^2 \equiv -1 \pmod{5}$,
 $x = 0, y = 1, z^2 \equiv 2 \pmod{7}$,
 $x = 1, y = 5, z^2 \equiv 5 \pmod{11}$,
 $x = 1, y = 2, z^2 \equiv 1 \pmod{13}$.