ON A CUBIC CONGRUENCE IN THREE VARIABLES. II[1]

L. J. MORDELL

Let p be a prime and let $f(x, y, z)$ be a cubic polynomial whose coefficients are integers not all $\equiv 0 \pmod{p}$, and so are elements of the Galois field $G(p)$. We have the

CONJECTURE. *Suppose that $f(x, y, z)$ cannot be expressed as a cubic polynomial in two independent variables, and that $f(x, y, z)$ is irreducible in any algebraic extension of $G(p)$. Then the number N of solutions of the congruence*

$$f(x, y, z) \equiv 0 \pmod{p} \tag{1}$$

for large p satisfies

$$N = p^2 + O(p), \tag{2}$$

where the constant implied in O is independent of the coefficients of $f(x, y, z)$ and of p.

A well-known case when (2) holds is[2]

$$ax^3 + by^3 + cz^3 + d \equiv 0, \qquad abcd \not\equiv 0. \tag{3}$$

Another nontrivial instance is given by [1]

$$z^2 \equiv f(x, y) + k, \tag{4}$$

where

$$f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$$

is not a multiple of a perfect cube.

It is not without interest to find other instances for which (2) holds. When I communicated (4) to Professor Davenport, he wrote (October 27, 1961) that (2) also holds for

$$f(x, y, z) \equiv k, \tag{4a}$$

where $f(x, y, z)$ is the general ternary cubic form.

I prove now the

THEOREM. *The result* (2) *holds for the congruence*

$$z^2 \equiv f(x, y) + lx + my, \tag{5}$$

Presented to the Society, November 17, 1962; received by the editors April 20, 1962.

[1] This work was supported in part by the National Science Foundation, Washington, D. C.

[2] We omit mod p, hereafter in congruences.

where

$$f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3 \not\equiv g(lx + my)^3.$$

Proofs of such results are of two kinds. One is at a completely elementary level, but the other makes use of Weil's theorem on the number of solutions of a polynomial congruence mod p. My proof of (4) was elementary. Professor Davenport in his letter gave a nonelementary proof of (4) and (4a). I give two proofs of the theorem. They both use Weil's results, but the second one, though shorter than the first, requires perhaps more detailed knowledge than the first.

A linear transformation shows that we can replace (5) by

$$z^2 \equiv f(x, y) + kx. \tag{6}$$

We note that when $p \equiv 3 \pmod 4$, $N = p^2$.
For clearly

$$N = \sum_{x,y} \left(1 + \left(\frac{f(x, y) + kx}{p}\right)\right),$$

where the inner bracket denotes the quadratic character (mod p). This changes sign when x, y are replaced by $-x$, $-y$, and so the result follows.

Suppose, hereafter, that $p \equiv 1 \pmod 4$. We first dispose of the trivial case when $f(x, y) = jx(gx+hy)^2$. On replacing $gx+hy$ by y, (6) becomes $z^2 \equiv jxy^2+kx$. This congruence has obviously $p^2+O(p)$ solutions.

Denote by $N(k)$ the number of solutions of (6). Then $N(k) = N(kt^4)$ where $t \not\equiv 0$ is any integer. For on putting $t^2x \equiv X$, $t^2y \equiv Y$, $t^3z \equiv Z$, in (6),

$$Z^2 \equiv f(X, Y) + kt^4X.$$

Hence $N(k)$ depends only on the biquadratic character of k (mod p), and so as k takes all values, $0 \leqq k < p$, $N(k)$ assumes five values, one N_0, corresponding to $k = 0$, and four others, say N_1, N_2, N_3, N_4. In (6), the number of solutions with $x \equiv 0$ is p, and so we enumerate hereafter only solutions with $x \not\equiv 0$. Consider now (6) as a congruence in four variables $x \not\equiv 0$, y, z, k. Then we have

$$N_0 + \frac{p-1}{4}(N_1 + N_2 + N_3 + N_4) = p^2(p-1). \tag{7}$$

The left-hand side is the number of solutions corresponding to $k = 0, 1, \cdots, p-1$. The right-hand side is the number when we take values of $x \not\equiv 0$, y, z, since these define k uniquely. Next

$$N_0^2 + \frac{p-1}{4}(N_1^2 + N_2^2 + N_3^2 + N_4^2) = p^5 + E, \tag{8}$$

where p^5+E is the number of solutions of

$$\frac{z^2 - f(x, y)}{x} \equiv \frac{z_1^2 - f(x_1, y_1)}{x_1} \tag{9}$$

in x, y, z, x_1, y_1, z_1 where $xx_1 \not\equiv 0$.

We show that each side of (8) represents the number of solutions of

$$z^2 \equiv f(x, y) + kx, \qquad z_1^2 \equiv f(x_1, y_1) + kx_1.$$

The left-hand side gives the number for $k=0, 1, 2, \cdots, p-1$, and the right-hand side the number obtained by equating the two values of k. From (7) and (8), since

$$1 + \frac{p-1}{4}(1 + 1 + 1 + 1) = p,$$

we have

$$(N_0 - p^2)^2 + \frac{p-1}{4}\{(N_1 - p^2)^2 + \cdots + (N_4 - p^2)^2\} = E + 2p^4.$$

We shall prove that $E+2p^4=O(p^3)$, and then

$$N_1 - p^2 = O(p),$$

etc., the required results.

We write (9) as

$$\frac{z^2}{x} - \frac{z_1^2}{x_1} \equiv \frac{f(x, y)}{x} - \frac{f(x_1, y_1)}{x_1}. \tag{10}$$

The number of solutions of

$$Az^2 + Bz_1^2 \equiv C, \qquad ABC \not\equiv 0,$$

is given by

$$p - \left(-\frac{AB}{P}\right)$$

If, however, $C\equiv 0$ and $AB\not\equiv 0$, the number is given by

$$p + (p-1)\left(\frac{-AB}{p}\right).$$

The bracket denotes the quadratic character.

Hence the number $E+p^5$ of solutions of (10) is S_1+S_2, where

$$S_1 = \sum_{x,x_1,y,y_1} \left(p - \left(\frac{xx_1}{p}\right)\right) = p^3(p-1)^2, \tag{11}$$

and

$$S_2 = p\sum\left(\frac{xx_1}{p}\right)$$

extended over the solutions of

$$\frac{f(x,y)}{x} - \frac{f(x_1,y_1)}{x_1} \equiv 0.$$

On noting (11), it suffices to prove that $S_2=O(p^3)$.

On putting $y\equiv vx$, $y_1\equiv v_1x_1$,

$$S_2 = p\sum\left(\frac{xx_1}{p}\right)$$

taken over $x^2f(1,v)\equiv x_1^2f(1,v_1)$.

Now put $x_1\equiv tx$. Then,

$$S_2 = p(p-1)\sum\left(\frac{t}{p}\right) \tag{12}$$

taken over the solutions of

$$f(1,v) \equiv t^2f(1,v_1). \tag{13}$$

In (12), we consider separately the parts arising according as t is a quadratic residue or nonquadratic residue. We put $t=lu^2$ where $l=1$ when t is a quadratic residue, and $l=n$ any fixed nonquadratic residue when t is a nonquadratic residue. We have

$$S_2 = p(p-1)(N_1' - N_2'), \tag{14}$$

where N_1', N_2' are the number of solutions in u, v, v_1 of

$$f(1,v) \equiv l^2u^4f(1,v_1) \tag{15}$$

for $l=1$, n respectively. We shall prove that

$$N_1' = p^2 + O(p), \qquad N_2' = p^2 + O(p),$$

and so $S_2=O(p^3)$.

The values of v_1 for which $f(1,v_1)\equiv 0$ give at most $O(p)$ solutions,

so we need not consider these v_1 any further. The number of solutions in u of $u^4 \equiv s \pmod{p}$ can be written as

$$1 + \chi(s) + \chi^2(s) + \chi^3(s), \tag{16}$$

where χ is an obvious biquadratic character (mod p). Hence the number of solutions of (15) is given by

$$\sum_{v,v_1} (1 + \chi(s) + \chi^2(s) + \chi^3(s)), \qquad s = f(1, v)/l^2 f(1, v_1).$$

The first term contributes $p^2+O(p)$ to N_1' and N_2'. The second term contributes a sum

$$\tilde{\chi}(l^2) \sum_{v} \chi(f(1, v)) \sum_{v_1} \tilde{\chi}(f(1, v_1))$$

where $\tilde{\chi}$ is the character conjugate to χ.

By Weil's theorem, the congruence $w^4 \equiv f(1, v)$ has $p+O(\sqrt{p})$ solutions since we have excluded the case when $f(1, v) = j(g+hv)^2$. It easily follows, as is already known, and follows from an application of Weil's theorem to a result of Davenport [2], that

$$\sum_{v} \chi(f(1, v)) = O(\sqrt{p}),$$

for any nonprincipal biquadratic character. Hence the number of solutions of (15) is equal to $p^2+O(p)$. This finishes the proof.

We now give another proof of the theorem. We have seen that

$$\begin{aligned} N &= \sum_{x,y} \left(1 + \left(\frac{f(x, y) + kx}{p}\right)\right) \\ &= p^2 - p + S, \end{aligned}$$

where on putting $y = vx$,

$$S = \sum_{x,v} \left(\frac{x^3 f(1, v) + kx}{p}\right).$$

We prove that $S = O(p)$.

We can omit the $O(1)$ values of v for which $f(1, v) \equiv 0$ since the sum in x is then zero. Replace x by $x/f(1, v)$. Then

$$S = \sum_{x,v} \left(\frac{x^2 + kf(1, v)}{p}\right)\left(\frac{x}{p}\right).$$

Write

$$S_A = \sum_{x} \left(\frac{x^2 + A}{p}\right)\left(\frac{x}{p}\right).$$

Let r, n be a fixed quadratic residue and nonquadratic residue mod p. We have then $A = tA_1^2$ where $t = r$ or n. On replacing x by $A_1 x$, and denoting S_r, S_n by R, N respectively,

$$S_A = \left(\frac{A_1}{p}\right) S_t = \frac{1}{2}\left(\frac{A_1}{p}\right)\left(\left(1 + \left(\frac{t}{p}\right)\right) R + \left(1 - \left(\frac{t}{p}\right)\right) N\right),$$

$$2S_A = \left(\frac{A_1}{p}\right)(R + N) + \left(\frac{A_1 t}{p}\right)(R - N).$$

It is known that $|R| \leqq 2\sqrt{p}$, $N \leqq 2\sqrt{p}$; in fact, it is easily proved, as is known, that $R^2 + N^2 = 4p$.

We show now that when $tA_1^2 \equiv kf(1, v)$, then $\sum_v (A_1/p) = O(\sqrt{p})$. On changing the notation slightly, it suffices to show that if $g(v)$ is a cubic in v which is not of the form $j(g+hv)^2$ and $u^2 \equiv g(v)$, then $\sum_v (u/p) = O(\sqrt{p})$.

Replace u by ru^2, nu^2 respectively according as u is a quadratic or nonquadratic residue of p. Since the number of solutions of $tu^4 \equiv g(v)$ is $p + O(\sqrt{p})$,

$$\sum_v \left(\frac{u}{p}\right) = p + O(\sqrt{p}) - p - O(\sqrt{p}) = O(\sqrt{p}).$$

This finishes the proof.

Bibliography

1. L. J. Mordell, *On a cubic congruence in three variables*, Acta Arith. 8 (1962–1963), 1–9.

2. H. Davenport, *On character sums in finite fields*, Acta Math. 71 (1939), 99–121.

University of Arizona and
St. John's College