On a cubic congruence in three variables

by

L. J. MORDELL (Cambridge)

Let p be a large prime, and let $f(x, y)$ be a cubic polynomial in x, y with coefficients in $G(p)$, i.e., the field of residues $\bmod p$. Suppose also that $f(x, y)$ is irreducible in $G(p)$ or any algebraic extension of $G(p)$. Let N be the number of solutions of the congruence

$$(1) \qquad f(x, y) \equiv 0 \,(\mathrm{mod}\, p)\,,$$

where we suppose that the curve $f(x, y) = 0$ is of genus one. Then there is Hasse's well known very deep result that

$$(2) \qquad |N - p| < 2\sqrt{p} + 1\,,$$

where $\sqrt{p}$ is the best possible power of p.

Suppose next that $f(x, y, z)$ is a cubic polynomial in x, y, z with coefficients in $G(p)$ which is not a function of only two independent variables. Suppose also that $f(x, y, z)$ is irreducible in $G(p)$ or any algebraic extension of $G(p)$. Let now N denote the number of solutions of the congruence [1]

$$(3) \qquad f(x, y, z) \equiv 0 \,(\mathrm{mod}\, p)\,.$$

It is quite easy to show that

$$(4) \qquad |N - p^2| = O(p^\gamma)\,, \qquad \gamma = 3/2,$$

where the constants implied in O here and throughout the paper are absolute constants independent of the coefficients of $f(x, y, z)$. From (1), this is easily proved to be the best possible result when $f(x, y, z)$ is homogeneous and the curve $f(x, y, 1) = 0$ is of genus one. In general, the best possible value of γ is unknown. In some instances to be dealt with, we can take $\gamma = 1$. I put this forward as a conjecture in the general case excluding, of course, the particular homogeneous case noted above.

Trivial cases when $\gamma = 1$ are given by

$$z f_2(x, y) + f_3(x, y) \equiv 0\,,$$

[1] We omit modulus hereafter since we use only $\bmod p$.

where f_2 and f_3 are polynomials of degrees 2 and 3 respectively and, by

$$z^2 \equiv g_2(x, y) + g_3(x, y),$$

where g_2, g_3 are homogeneous of degrees 2 and 3 respectively. Here the complete solution can be expressed by means of two parameters e.g. $x \equiv \xi y,\ z \equiv \zeta y$.

A more interesting case is the well-known congruence

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

where $\gamma = 1$.

It is now not without interest to prove the

THEOREM. *Let p be a large prime and let*

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

where we suppose that

$$f(x, y) \not\equiv \nu(\lambda x + \mu y)^3,$$

where λ, μ, ν are rational.

Then $N = N(k)$, the number of solutions of the congruence

$$(5) \qquad z^2 \equiv f(x, y) + k$$

satisfies the inequality

$$(6) \qquad |N - p^2| = O(p).$$

The result is trivial when $p \equiv 2 \pmod 3$. For if $x \equiv 0$, the crudest argument gives at most $2p$ solutions for y, z. If $x \not\equiv 0$, we can put $y \equiv vx$. Then
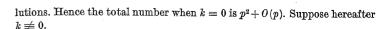
$$z^2 \equiv (a + 3bv + 3cv^2 + dv^3)x^3 + k.$$

Suppose first that $a + 3bv + 3cv^2 + dv^3 \equiv 0$. This gives $\delta = 0, 1, 2$ or 3 values of v. Then x can be taken arbitrarily and then there are at most two values for z, and this gives at most $6p$ solutions.

Suppose next that $a + 3bv + 3cv^2 + dv^3 \not\equiv 0$. Then arbitrary z gives one value for x, and so this gives $p(p - \delta)$ solutions. Hence there are $p^2 + O(p)$ solution for (5).

We consider next the case when $p \equiv 1 \pmod 3$. We first of all dispose of the special case when $k \equiv 0$. Suppose first that $x \equiv 0$ and so $z^2 \equiv dy^3$. If $d \equiv 0$, y is arbitrary. If $d \not\equiv 0$, we have a solution $x \equiv 0$, $y \equiv 0$, and $p - 1$ solutions when $z \not\equiv 0$, given by putting $y \equiv uz$ where $1 \equiv du^3z$. Hence there are $O(p)$ solutions with $x \equiv 0$. Suppose next that $x \not\equiv 0$, so that we can put $y \equiv xv$, $z \equiv xw$. Then

$$w^2 \equiv (a + 3bv + 3cv^2 + dv^3)x.$$

For the δ values of v above, x is arbitrary and this gives δp solutions. We have next $p - \delta$ values for v and p values for w giving $p(p - \delta)$ so-

lutions. Hence the total number when $k \equiv 0$ is $p^2 + O(p)$. Suppose hereafter $k \not\equiv 0$.

We require in the next section a result which we state as

LEMMA 1[2]. *The number of solutions in x, y of*

$$AX^2 + BY^2 \equiv C, \qquad ABC \not\equiv 0,$$

is $p - \left(\dfrac{-AB}{p} \right)$ where the symbol ( ) is the Legendre symbol.

We consider first the special case when $f(x, y)$ is reducible $\bmod p$, and so $f(x, y)$ has a linear factor $\bmod p$. By means of a linear substitution, we may suppose $a \equiv 0$ and so we consider

$$(7) \qquad z^2 \equiv 3bx^2y + 3cxy^2 + dy^3 + k.$$

Suppose first that $b \equiv 0$, and so $c \not\equiv 0$. If $y \equiv 0$, x is arbitrary and there are at most two values for z, i.e., this gives $O(p)$ solutions. If $y \not\equiv 0$, z is arbitrary and x is uniquely determined giving $p^2 - p$ solutions. Hence the total number is $p^2 - O(p)$.

Suppose next that $b \not\equiv 0$. If $y \equiv 0$, we have at most $2p$ solutions for x and z. Suppose then $y \not\equiv 0$. Then [3]

$$(8) \qquad 3byz^2 \equiv (3bxy + \tfrac{3}{2}cy^2)^2 + (3bd - \tfrac{9}{4}c^2)y^4 + 3bky.$$

Suppose first that $4bd - 3c^2 \equiv 0$. Then

$$(9) \qquad z^2 \equiv 3by\left(x + \frac{cy}{2b}\right)^2 + k.$$

By Lemma 1, (9) has $\displaystyle\sum_{y=1}^{p-1} \left(p - \left(\frac{-3by}{p} \right) \right) = p^2 - p$ solutions. We have then $p^2 + O(p)$ solutions when $b \not\equiv 0$, and $4bd - 3c^2 \equiv 0$.

Suppose next that $b(4bd - 3c^2) \not\equiv 0$. Since $y \not\equiv 0$, there are at most three values of y for which $(3bd - \tfrac{9}{4}c^2)y^4 + 3bky \equiv 0$. Since each value of x gives at most two values of z, at most $6p$ solutions arise in this way. If we exclude these three possible values of y and $y \equiv 0$, (8) has

$$\sum_{\nu} \left(p - \left(\frac{-3by}{p} \right) \right) = p^2 + O(p)$$

---

[2] A proof is given in Bachmann's *Arithmetik der quadratisches Formen*, Bd. 1, page 491. Another proof is also easily found by proving the existence of at least one solution X_0, Y_0 in the usual way, and then putting $Y - Y_0 = t(X - X_0)$ where t is a rational parameter.

[3] We understand throughout by a fraction $1/v$, $v \not\equiv 0 \pmod p$ the integer $\bar{v}$ where $v\bar{v} \equiv 1 \pmod p$ (when appropriate).

solutions. Hence we have also $p^2 + O(p)$ solutions of (7) when $f(x, y)$ is reducible $(\bmod p)$. We suppose hereafter that $p \equiv 1 \,(\bmod 3)$, and that $f(x, y)$ is irreducible $(\bmod p)$.

This sixth power residues of the numbers $k = 0, 1, \ldots, p-1$ can be arranged in seven sets. The first consists of the single number $k = 0$, and the other six consist each of $\frac{1}{6}(p-1)$ numbers. The number of solutions of (5) is the same for two numbers k', k in the same set. For then with appropriate v, $k' \equiv kv^6$, and the congruence

$$z^2 \equiv ax^3 + 3bx^2y + 3cxy^2 + dy^3 + kv^6$$

is replaced by (5) on putting $x \equiv v^2 X$, $y \equiv v^2 Y$, $z \equiv v^3 Z$.

We denote by $N(k_0), N(k_1), \ldots, N(k_6)$ the number of solutions of (5) corresponding to the sets in which the k may lie. Then

$$(10) \qquad \sum_{k=0}^{p-1} N(k) = N(k_0) + \tfrac{1}{6}(p-1)\big(N(k_1) + \ldots + N(k_6)\big) = p^3 \,,$$

since the left-hand side is the number of solutions of (5) in the four variables x, y, z, k. Next

$$(11) \qquad \sum_{k=0}^{p-1} N^2(k) = N^2(k_0) + \tfrac{1}{6}(p-1)\big(N^2(k_1) + \ldots + N^2(k_6)\big) = N^{(1)} \,,$$

where $N^{(1)}$ is the number of solutions in x, y, z, x_1, y_1, z_1 of

$$(12) \qquad z_1^2 - z^2 \equiv f(x_1, y_1) - f(x, y) \,.$$

Denote by $N^{(2)}$ the number of solutions of

$$(13) \qquad f(x_1, y_1) - f(x, y) \equiv 0 \,.$$

These will contribute to (12), $(2p-1)N^{(2)}$ solutions. When (13) is not satisfied, we have $(p-1)(p^4 - N^{(2)})$ solutions of (12) since we can take $z_1 - z = v$, $v = 1, 2, \ldots, p-1$. Hence

$$N^{(1)} = (p-1)(p^4 - N^{(2)}) + (2p-1)N^{(2)} \,,$$
$$= p^5 - p^4 + pN^{(2)} \,.$$

Combining (10) and (11) with $\sum_{k=0}^{p-1} 1 = p$, we have

$$\big(N(k_0) - p^2\big)^2 + \tfrac{1}{6}(p-1)\Big[\big(N(k_1) - p^2\big)^2 + \ldots + \big(N(k_6) - p^2\big)^2\Big] = pN^{(2)} - p^4 \,.$$

We shall prove below that $N^{(2)} = p^3 + O(p^2)$. Then if $k \not\equiv 0$,

$$\tfrac{1}{6}(p-1)\big(N(k) - p^2\big)^2 = O(p^3) \,,$$

and so $N(k) - p^2 = O(p)$, the required result (6).

To find $N^{(2)}$, we put $x_1 \equiv x + \xi$, $y_1 \equiv y + \eta$. Then

$$(14) \qquad f(\xi, \eta) + x\frac{\partial f}{\partial \xi} + y\frac{\partial f}{\partial \eta} + \frac{1}{2}\left(x^2 \frac{\partial^2 f}{\partial \xi^2} + 2xy \frac{\partial^2 f}{\partial \xi \partial \eta} + y^2 \frac{\partial^2 f}{\partial \eta^2}\right) \equiv 0 \,,$$

and we require the number of solutions in x, y, ξ, η. We write this as

$$(15) \qquad Ax^2 + 2Hxy + By^2 + 2Fy + 2Gx + C \equiv 0 \,,$$

and we now find the number of solutions in x, y for given ξ, η.

We state the result as

LEMMA 2. *The number $N^{(3)}$ of solutions in x, y of (15) when no one of*

$$A \equiv 0, \qquad H^2 - AB \equiv 0, \qquad \varDelta = ABC + 2FGH - AF^2 - BG^2 - CH^2 \equiv 0$$

is satisfied, is given by

$$N^{(3)} = p - \left(\frac{H^2 - AB}{p}\right).$$

For we can write (15) in turn as

$$(Ax + Hy + G)^2 + (AB - H^2)y^2 + 2(AF - GH)y + AC - G^2 \equiv 0 \,,$$
$$(AB - H^2)(Ax + Hy + G)^2 + \big((AB - H^2)y + AF - GH\big)^2 + A\varDelta \equiv 0 \,.$$

The result is now obvious from Lemma 1.

There are some cases of (15) requiring special consideration and it will convenient to deal with these first.

We show that we cannot have both $ac - b^2 \equiv 0$, $db - c^2 \equiv 0$ except when both $b \equiv 0$, $c \equiv 0$, each of these latter implying the other since $ad \not\equiv 0$. For then

$$f(x, y) \equiv \frac{b^2}{c} x^3 + 3bx^2y + 3cxy^2 + \frac{c^2}{b} y^3$$
$$\equiv (bx + cy)^3 / bc \,,$$

and this has been excluded. We may suppose then that $ac - b^2 \not\equiv 0$ unless $b \equiv c \equiv 0$.

The special cases referred to are when any of $A \equiv 0$, $AB - H^2 \equiv 0$ and $\varDelta \equiv 0$.

Suppose first that $A \equiv 0$, i.e., $\frac{\partial^2 f}{\partial \xi^2} \equiv 0$ or $a\xi + b\eta \equiv 0$. This will not be identically satisfied in ξ, η since we cannot have both $a \equiv 0$, $b \equiv 0$. Hence $\frac{\partial^2 f}{\partial \xi^2} \equiv 0$ is satisfied by p sets of values for ξ, η. We can deal at once with the case $\xi \equiv 0$, $\eta \equiv 0$. Then in (14), x, y are arbitrary and we have p^2 solutions of (14). We now exclude the case $\xi \equiv 0$, $\eta \equiv 0$. Then $\frac{\partial^2 f}{\partial \xi \partial \eta} \not\equiv 0$, since $a\xi + b\eta \equiv 0$, $b\xi + c\eta \equiv 0$ require $ac - b^2 \equiv 0$. This has been excluded unless $b \equiv c \equiv 0$ and this we deal with in a moment.

Hence excluding $\xi \equiv \eta \equiv 0$, there are $p-1$ values of y for which $\frac{\partial f}{\partial \xi} + y \frac{\partial^2 f}{\partial \xi \partial \eta} \not\equiv 0$. Each of these determines x uniquely and so $O(p^2)$ sets of solutions arise for ξ, η, x, y. Suppose next that y satisfies $\frac{\partial f}{\partial \xi} + y \frac{\partial^2 f}{\partial \xi \partial \eta} \equiv 0$. Then x is arbitrary and so we have again $O(p^2)$ sets of solutions for ξ, η, x, y.

Suppose next $b \equiv c \equiv 0$. Then (14) takes the shape

$$(16) \qquad a\xi^3 + d\eta^3 + 3a\xi^2 x + 3d\eta^2 y + 3(a\xi x^2 + d\eta y^2) \equiv 0 ,$$

and $A \equiv 0$ gives $\xi \equiv 0$. Then

$$\eta(d\eta^2 + 3d\eta y + 3dy^2) \equiv 0 .$$

Hence either $\eta \equiv 0$ and there are p^2 solutions for x, y, or $\eta \equiv 1, 2, ..., p-1$. For each value of η, there are at most 2 values for y since $d \not\equiv 0$ and x is arbitrary. We have here again $O(p^2)$ solutions.

Suppose next that $H^2 - AB \equiv 0$, i.e.,

$$(17) \qquad \frac{\partial^2 f}{\partial \xi^2} \frac{\partial^2 f}{\partial \eta^2} - \left(\frac{\partial^2 f}{\partial \xi \partial \eta}\right)^2 \equiv P\xi^2 + 2Q\xi\eta + R\eta^2 \equiv 0 ,$$

say. This is not identically congruent to zero if $b \equiv c \equiv 0$, or if $ac - b^2 \not\equiv 0$. Hence (17) gives $O(p)$ sets of values for ξ, η. Also (14) takes the shape

$$(18) \qquad f(\xi, \eta) + x\frac{\partial f}{\partial \xi} + y\frac{\partial f}{\partial \eta} + \nu(\lambda x + \mu y)^2 \equiv 0 ,$$

say. We cannot have both $\lambda \equiv 0$, $\mu \equiv 0$ unless both $\xi \equiv 0$, $\eta \equiv 0$. For $\frac{\partial^2 f}{\partial \xi^2} \equiv 0$, $\frac{\partial^2 f}{\partial \eta^2} \equiv 0$ gives $\frac{\partial^2 f}{\partial \xi \partial \eta} \equiv 0$, and so

$$a\xi + b\eta \equiv 0 , \qquad c\xi + d\eta \equiv 0 , \qquad b\xi + c\eta \equiv 0 .$$

Then $b^2 - ac \equiv 0$ which has been excluded unless $b \equiv c \equiv 0$. We note $b \equiv c \equiv 0$ would give $\xi \equiv \eta \equiv 0$. Hence putting $\lambda x + \mu y = X$, there are at most $O(p)$ values for x, y and again $O(p^2)$ sets of solutions in x, y, ξ, η.

Suppose finally that

$$\varDelta = ABC + 2FGH - AF^2 - BG^2 - CH^2 \equiv 0 ,$$

so that $\varDelta$ is a quintic binary form in ξ, η. We prove that $\varDelta$ is not identically congruent to zero. The leading ξ terms $A', B', ...$ in $A, B, ...$ are

$$A' = 3a\xi , \qquad B' = 3c\xi , \qquad C' = a\xi^3 ,$$

$$F' = \frac{3b}{2}\xi^2 , \qquad G' = \frac{3a}{2}\xi^2 , \qquad H' = 3b\xi .$$

Hence the coefficient of ξ^5 in $\varDelta$ is

$$9a^2c + \tfrac{27}{2}ab^2 - \tfrac{27}{4}ab^2 - \tfrac{27}{4}a^2c - 9ab^2 = \tfrac{9}{4}(a^2c - ab^2) .$$

Since $a \not\equiv 0$, this requires $b^2 \equiv ac$. Similarly $c^2 \equiv db$. Hence if $bc \not\equiv 0$,

$$f(\xi, \eta) \equiv \frac{b^2}{c}\xi^3 + 3b\xi^2\eta + 3c\xi\eta^2 + \frac{c^2}{b}\eta^3 ,$$

and so $f(\xi, \eta)$ would be a cube except for a factor $1/bc$.

If, however, $b \equiv 0$, then $c \equiv 0$, and

$$f(\xi, \eta) \equiv a\xi^3 + d\eta^3 .$$

Now

$$A = 3a\xi , \quad B = 3d\eta , \quad C = a\xi^3 + d\eta^3 , \quad 2F = 3d\eta^2 , \quad 2G = 3a\xi^2 , \quad H = 0 ,$$

Then

$$\varDelta = 9ad\,\xi\eta(a\xi^3 + d\eta^3) - \tfrac{27}{4}ad^2\xi\eta^4 - \tfrac{27}{4}da^2\eta\xi^4 \not\equiv 0$$

identically.

Hence $\varDelta \equiv 0$ gives at most $O(p)$ sets of values of ξ, η. Since then (14) splits into two linear factors in x, y we have at most $O(p)$ sets of values for x, y. Hence at most $O(p^2)$ solutions arise when $\varDelta \equiv 0$.

Since there are $O(p^2)$ solutions in ξ, η, x, y when any of $A \equiv 0$, $H^2 - AB \equiv 0$, $\varDelta \equiv 0$, we have

$$N^{(2)} = \sum_{\xi, \eta}\left(p + \left(\frac{H^2 - AB}{p}\right)\right) + O(p^2) ,$$

where the summation is taken over all the values of ξ, η except the excluded sets $O(p)$ in number when $A \equiv 0$ etc. Hence

$$(19) \qquad N^{(2)} = p^3 + O(p^2) .$$

This finishes the proof.

It seems as if the same method might apply to the congruence $z^3 \equiv f(x, y) + k$.

The ideas just developed make it quite easy to deal with N, the number of solutions of the congruence

$$f(x, y) = ax^3 + 3bx^2y + 3cxy^2 + dy^3 \equiv 1 , \qquad \text{where} \qquad f(x, y) \not\equiv \nu(\lambda x + \mu y)^3 .$$

When $p \equiv 2 \pmod 3$, we have trivially

$$|N - p| = O(1)$$

on putting $y \equiv vx$.

We prove that when $p \equiv 1 \pmod 3$, we have

$$|N - p| = O(\sqrt{p}) .$$

We now consider the number $N(k)$ of solutions for $k = 0, 1, \ldots, p-1$ of

$$f(x, y) \equiv k \, .$$

The numbers k can be arranged in four classes. The first contains only $k = 0$ and the other three each contain $\frac{1}{3}(p-1)$ numbers, namely one class of cubic residues and two of non-cubic residues. Denote by $N(k_0)$, $N(k_1)$, $N(k_2)$, $N(k_3)$ the number of solutions of the corresponding congruences. Then we find easily

$$N(k_0) + \tfrac{1}{3}(p-1)\big(N(k_1) + N(k_2) + N(k_3)\big) = p^2 \, ,$$

$$N^2(k_0) + \tfrac{1}{3}(p-1)\big(N^2(k_1) + N^2(k_2) + N^2(k_3)\big) = N^{(2)} = p^3 + O(p^2)$$

where $N^{(2)}$, the number of solutions of $f(x, y) = f(x_1, y_1)$ is given in (19). Hence

$$\big(N(k_0) - p\big)^2 + \tfrac{1}{3}(p-1)\big(\big(N(k_1) - p\big)^2 + \big(N(k_2) - p\big)^2 + \big(N(k_3) - p\big)^2\big) = O(p^2) \, ,$$

and so

$$N(k) - p = O(\sqrt{p}) \, , \qquad k \not\equiv 0 \, .$$

The result is of course included in (2), but the elementary proof seems of interest.

The same idea leads to a result on cubic exponential sums given by the

THEOREM. *Suppose that*

$$f(x, y) = ax^3 + 3bx^2y + 3cxy^2 + dy^3 \not\equiv \nu(\lambda x + \mu y)^3 \, .$$

Then

$$\sum_{x,y=0}^{p-1} e^{\frac{2\pi i}{p} f(x,y)} = O(p) \, .$$

When $p \equiv 2 \pmod 3$, the result is trivial on putting $y = vx$. Suppose then $p \equiv 1 \pmod 3$, and unite

$$S(k) = \sum_{x,y=0}^{p-1} e^{\frac{2\pi i k}{p} f(x,y)} \, .$$

Then there are obviously four different sums $S(0) = p^2$ and $S(k_1)$, $S(k_2)$, $S(k_3)$ arising from the cubic character of k.

Hence

$$S^2(0) + \tfrac{1}{3}(p-1)\big(S^2(k_1) + S^2(k_2) + S^2(k_3)\big) = \sum e^{\frac{2\pi i k}{p}(f(x,y) - f(x_1,y_1))}$$
$$= pN^{(2)} = p^4 + O(p^3) \, ,$$

the summation being taken over $0 \leqslant k, x, y, x_1, y_1 < p$, since the sum in k is zero unless $f(x, y) \equiv f(x_1, y_1)$. Hence

$$S(k) = O(p) \quad \text{if} \quad k \not\equiv 0 \, ,$$

It may be noted that when $f(x, y)$ is the general polynomial of the third degree, it has been conjectured that

$$S = \sum_{x,y=0}^{p-1} e^{\frac{2\pi i}{p} f(x,y)} = O(p^\gamma) \, ,$$

and that $\gamma = 1$ is best possible. I conjecture that $|S| \leqslant 4p$. Professor Davenport informs me that he has proved the result with $\gamma = \frac{5}{4}$. The conjecture is true when

$$g(x, y) = f(x, y) + mx + ny$$

in the case when $\left(\dfrac{-D}{p}\right) = 1$, where

$$D = -a^2d^2 + 6abcd - 4ac^3 - 4bd^3 + 3b^2c^2$$

is the discriminant of $f(x, y)$. For then, the factors of the Hessian of $f(x, y)$ have integer coefficients, and so by a linear substitution with integer coefficients and determinant prime to p, we can write

$$S = \sum_{Y,X} e^{\frac{2\pi i}{p}(AX^3 + BY^3 + CX + DY)} \, ,$$

where A, B, C, D are integers. From a known deep result,

$$\left| \sum_X e^{\frac{2\pi i}{p}(AX^3 + CX)} \right| \leqslant 2\sqrt{p} \, ,$$

and so $|S| \leqslant 4p$.

I should like to thank Dr Mohindoa S. Cheema for his comments on my manuscript.

UNIVERSITY OF COLORADO, BOULDER, COLORADO U.S.A.
UNIVERSITY OF ARIZONA, TUCSON, ARIZONA U.S.A.
ST. JOHNS COLLEGE, CAMBRIDGE, ENGLAND